MI Professional Bulletin
April - June 2016
PB 34-16-2

Multinational Operations and Other Intelligence Challenges

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

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

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.

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
1613301

From the Editor

I will be retiring in September; it's been a very rewarding job due in great part to the many contributors to the Bulletin. I want to thank all the writers and others who have made this Bulletin happen.

The following themes and deadlines are established for:

October-December 2016, *Leveraging DCGS-A: Our Primary Weapons System*, deadline for submissions is 12 July 2016.

January-March 2017, *Intelligence Training Management,* deadline for submissions is 29 September 2016.

April-June 2017, *BCT S2 Ops*, deadline for submissions is 30 December 2016.

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

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

Sterilla Smith
Editor

MI Professional Bulletin
April - June 2016
PB 34-16-2
Volume 42 Number 2

8

27

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 supercede information in any other Army publication.

DEPARTMENTS

Always Out Front

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

Unified action across Army, joint, and multinational forces synchronized with the activities of other government agencies, nongovernmental and intergovernmental organizations, and the private sector is critical. The warrior spirit of our unified action partners has been tested across countless battlefields and domains and they have demonstrated the ability to confront the enemies of freedom and respond to other types of crisis. As our strategic interests have drawn us together, we have also strengthened the military ties with our partners. We are unifying operationally across domains to collaborate in providing humanitarian assistance, disaster relief, maritime security, and maritime domain awareness.

In future operations, our military leaders will face a wide array of complex challenges. Advances in technologies, rapid proliferation of effective weapons systems, and emergence of new sophisticated threats are just a few of the potential dangers our military forces will face. Friendly forces must be capable of operating in a complex environment while simultaneously defeating numerous threats. Additionally, our forces must be able to effectively operate in the most demanding environments such as jungles, mountains, deserts, and megacities. To meet this daunting challenge, we must be skilled at operating with our unified action partners. As stated by Winston Churchill, "The only thing worse than fighting with allies is fighting without them."

The Army Operating Concept addresses a number of solutions to these challenges. Two of the solutions are properly trained and equipped Army formations and the need to execute realistic combined arms and joint training. To implement these solutions, the U.S. Army Intelligence Center of Excellence (USAICoE) is investing in Army Military Intelligence leaders by developing cognitive programs and strategies to enhance integration with our multinational partners.

Currently, there is no institutional training platform that provides instruction on the planning, execution, and integration of coalition intelligence operations. To fill this training gap, USAICoE, in conjunction with various Intelligence Community stakeholders, is developing the Coalition Intelligence Course for our "Five Eye" partner nations. The three to four week course, estimated to be implemented in Fiscal Year 2017, will be held semi-annually at Fort Huachuca. The course will train and assess individuals and staffs on coalition intelligence operations in subjects such as intelligence systems capabilities, coalition collection management, coalition intelligence planning, and coalition intelligence support to mission command.

Another way USAICoE is helping to prepare the Army for future unified action is the many activities of the U.S. Army Training and Doctrine Command's (TRADOC) Culture Center (TCC). Today's TCC is "chest deep" preparing Soldiers and leaders to operate with our unified action partners as units execute our Army's Regionally Aligned Forces focus. Staging from its home base at USAICoE, TCC conducts culture, regional expertise, and language (CREL) pre-deployment education and training, satisfying Forces Command's pre-deployment training requirements. This training is designed to help Soldiers and leaders better understand complex operational environments, build rapport with their unified action partners, and interact with the host nation population to accomplish their assigned mission. The TCC has recently begun to team with the Defense Language Institute Foreign Language Center, capitalizing on the synergy of their world-class programs and bringing more CREL assets to bear in support of our operational force.

Given there is a nexus between leader development and cross-cultural competency, the TCC plays an active role in building the Army's bench of future strategic leaders and regional experts. This education begins with U.S. Army Cadet Command's Cadet Overseas Training Missions. Each summer, more than 1,000 cadets travel to over 30 countries as part of a cultural immersion and military-to-military exchange with our multinational partners. TCC instructors play a key role, deploying with the cadets, serving as cultural advisors, and actively coaching and mentoring tomorrow's commissioned officers as part of this unique leader development program.

Working with our multinational partners with shared purpose and direction is a critical part of building the readiness and capability required to meet the challenges of a complex world. I have mentioned only a few of the initiatives we are implementing. USAICoE is committed to improving command arrangements, interoperability, intelligence sharing, and cultural understanding during future multinational operations. Together, the Army, joint forces, and our partners are, and will continue to be, ready to implement the Army's strategic framework of prevent, shape, and win to meet our national objectives.

"Always Out Front and Army Strong!"

CSM FORUM

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

Intelligence Challenge of Multinational Operations

To "Win in a Complex World" our Army needs to continue to operate in a Joint, Interagency, Intergovernmental Multinational (JIIM) environment. The operations we support now and in the future will continue to involve sister services, partnered agencies, and multinational partners to achieve mission success. All intelligence professionals need to be thinking about how we conduct our operations with our multinational partners. Whether you are assigned to a National Agency, a Combatant Command, a Military Intelligence (MI) brigade, a Forces Command formation, or special operations unit, the best way to support JIIM operations is to write for release.

We need your intelligence products to reach all of our mission partners to support operational success, especially in named operations with coalition forces such as Operations Resolute Support or Inherent Resolve. MI professionals need to be flexible and adjust based on the needs of the mission when supporting coalition forces and ensure reports are clearly understood by all customers. At one point during my tour at Bagram we had Czechoslovakian, Georgian, Jordanian, Polish, and several other countries and various agencies working with Army, Marines, Air Force, and Navy units and personnel defending the battle space. It took concerted efforts by all the intelligence assets supporting the coalition forces to ensure every patrol and guard force had updated and actionable intelligence to ensure mission accomplishment. That would not have been possible without skilled intelligence professionals working with their coalition partners, and writing for release.

Developing the skills and ability to share intelligence needs to become routine cannot wait until we are in a conflict. Regionally aligned forces (RAF) need to build relationships with the multinational partner(s) during exercises in support of possible future operations. These relationships need to be maintained not only by the command and operations staff, but also by the intelligence staff at Corps, division, and brigade. In order to rapidly integrate expeditionary forces with regional partners we need to maintain those relationships built during exercises through continued reach back and sharing of intelligence on projected adversaries supporting the RAF mission.

To make the most out of exercises and exchanges with our multinational partners, go beyond the exercise parameters and learn from your partners to build relationships. What are their capabilities for collection (equipment), analysis (personnel), and production and dissemination (communications)? We may be relying on the intelligence capabilities of our partners in RAF situations to support operations, especially when initially entering an area of operation under coalition forces control. Intelligence support of multinational operations is a multi-lane street, do not assume coming in that your information is more accurate or up to date. Incorporate information from all available assets and weigh it appropriately when developing situational understanding for your Commander. Think about it, who has the most extensive Human Intelligence assets in place. It is the host country you are deploying to in support of a RAF mission or the team just hitting the ground.

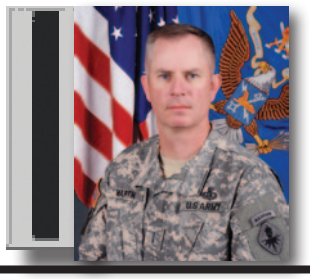
Intelligence efforts supporting host nation joint intelligence operations such as those in Korea and Japan often are bilateral in nature, serving the shared interests of the U.S. and the host nation. Sometimes though these relationships may expand to multinational efforts to share information against specific threats such as the North Korea. Keep in mind when you write your intelligence products for release that you need to continuously protect sources, capabilities, and tactics, techniques, and procedures. This is still a responsibility for all intelligence professionals even as you push your intelligence to the lowest level of command.

Keep up the great work and keep striving to increase our processing, exploitation, and dissemination to support all of our current and future JIIM operations at the tactical, operational, and strategic levels.

"Always Out Front and Army Strong!"

Technical Perspective

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



The Army Operating Concept "Win in a Complex World" defines complex "as an environment that is not only unknown, but unknowable and constantly changing." This is particularly true for the Army's Intelligence Warfighting Function (IWfF), which despite increased technological collection capabilities remains challenged to predict our nations next adversary in an increasingly unpredictable world. This uncertainty requires the IWfF to remain postured to operate globally in support of the Army's regionally aligned forces (RAF).

The demand for the world's premiere land force component to integrate and operate within a joint, interagency, and multinational (JIM) environment is greater than ever. The IWfF must be prepared to deploy and fully integrate as part of a joint/coalition team with multiple partners across multiple domains as demonstrated by the Army's many ongoing RAF missions. RAFs are deployed on a rotational basis, executing bilateral and multilateral exercises and engagements with interorganizational agencies, nongovernmental agencies (NGOs), foreign militaries, and joint partners. Hundreds of intelligence Soldiers are currently deployed in areas outside of the Middle East and Central Asia in support of a myriad of operations and exercises such as Operation Atlantic Resolve, Pacific Pathways and, African Horizons. These exercises combined with other contingency operations are examples of an enduring effort to build partnerships, demonstrate force projection, and execute strategic deterrence with our JIM partners.

For the IWfF to successfully operate within the JIM environment it must be able to seamlessly exchange time sensitive intelligence reporting and analysis to ensure mission command maintains situational awareness. While technology and advanced processes have enabled the IWfF to better share intelligence, agile and adaptive intelligence professionals, who seek innovative solutions to complex problems, remain the key to successfully operating in a JIM environment.

In October, 2014 the 101st Airborne Division deployed to Liberia and established Joint Forces Command-United Assistance to address the emerging Ebola epidemic in West Africa. The Screaming Eagles partnered with the U.S. Agency for International Development, the U.S. Public Health Service Commissioned Corps, and the Liberian Government as the Department of Defense effort to build capacity and rapidly contain the epidemic. The 101st G2 was charged with developing a common intelligence picture that would be integrated into an unclassified common operating picture (COP) using Google Earth. Chief Warrant Officer Three Tyson Van Patten and his team in the 101st G2 determined that the COP could be updated through a modification of the Distributed Common Ground Station-Army (DCGS-A) Tactical Entity Database, displaying near real-time changes in the environment. To facilitate the effort, his team loaded a portable Google-Earth Server onto an Intelligence Fusion Server stack. This not only allowed the COP to be displayed, but provided access to all members of the Operation United Assistance staff, to include the NGOs and the Liberian Government via All Partners Access Network. The creative efforts of the 101st illustrates that DCGS-A is an adaptable family of systems that can be modified to provide intelligence support in a JIM environment.

The U.S. Army Intelligence Center of Excellence (USAICoE) has expended a great deal of effort in training functional interoperability within the JIM environment to posture our formations to better operate in a complex environment. For Military Intelligence warrant officers this means training to support JIM operations is resident in all of our courses but it is particularly emphasized in the recently developed MI phases of Warrant Officer Intermediate Level Education and Warrant Officer Senior Service Education. In the future, USAICoE looks to expand multinational partnerships with the introduction of a Five Eyes (FVEY) intelligence course that will foster collaborative relationships and situational understanding.

We will continue to explore opportunities to establish trust through partnerships that expand beyond the uniformed services and the confines of our U.S. territories. It's through these relationships that we will protect our national interests.

Always Out Front! Army Strong!

The MI Brigade (Theater) as an Intelligence Anchor Point for Regionally Aligned and Global Response Forces

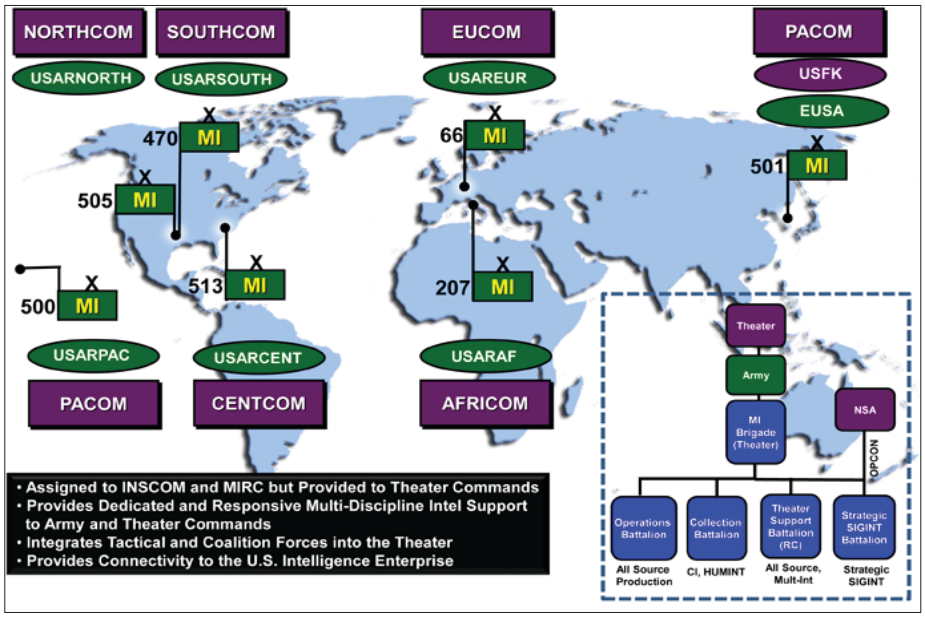
by Thomas Stokowski, U.S. Army INSCOM G3 Plans
Contributors: Robert Coon, Jimmy (Stan) Hinton,
and INSCOM G3 Operations and Training Staff Members

Army Operating Concept Mission Requirement: Expeditionary Operations Integrated with the Theater Intelligence Structure

The Army Operating Concept requires Army forces to be both expeditionary and interoperable with Joint, interagency, and multinational (JIM) partners. Attaining and sustaining readiness to execute regionally aligned forces (RAF) and global response forces (GRF) missions under these conditions compels integration with the Geographic Combatant Command (GCC)/Army Service Component Command's (ASCC) theater intelligence structure beginning with the mission alignment order and lasting through the duration of the force generation cycle.

Central Idea: The MI Brigade (Theater) (MIB(T)) Directly Supports RAF and GRF to Rapidly Integrate into the Theater

Faced with expeditionary mission readiness demands, the Army's MI leaders have committed to establishing the U.S. Army Intelligence and Security Command (INSCOM) and the MI Readiness Command (MIRC) MIB(T)s–under the direction of the Theater Army/ASCC and in turn, the GCCs–as the theater intelligence "Anchor Point" to partner with Army force provider commands (FORSCOM, USAREUR, USARPAC) and RAF and GRF units at all echelons to help "set the theater" and to provide enabling services for all ground forces deploying to, operating in, or otherwise supporting each theater.



MI Brigades (Theater).

Anchor Point Concept: Based on the MIB(T)'s Role as the GCC's Ground Intelligence Organization

The Anchor Point concept builds on the MIB(T)'s central role as the theater's permanently assigned ground intelligence organization, where it has always had the responsibility to support Army forces based in, and deploying to its theater. The MIB(T) is deeply rooted in the theater's operational environment with some MIB(T)s having JIM ties spanning decades. The MIB(T)'s Forward Collection Battalion and Operations Battalion, reinforced by a U.S. Army Reserve Theater Support Battalion, are continuously engaged in meeting the GCC/ASCC's daily operational requirements and conduct intelligence operations under the authorities vested in the GCC.

MIB(T) Anchor Point Provides Core Services: Analytics, Systems, Synchronization/Collaboration, and Training

Through coordination with the ASCC G2/G3 and MIB(T) S3, RAF/GRF units can leverage the MIB(T)'s ongoing in-theater collection and analytical production efforts and corresponding operating authorities to train and prepare for their own RAF/GRF missions. The MIB(T) can support home station reach/overwatch operations and meet the expeditionary mission command challenges of operating on the move (en route to, and in the theater). Additionally, the MIB(T) can offer RAF units intelligence discipline-specific expertise (GEOINT, CI, HUMINT, SIGINT, MASINT, OSINT, TECHINT), informed by in-theater experience and lessons learned.

- **Analytics.** Each MIB(T) maintains the theater-specific Tactical Entity Database that aggregates the Distributed Common Ground System-Army (DCGS-A) populated data, including JIM sources. The MIB(T) will work with RAF/GRF units to establish connectivity so that this data is available to mission command centers in theater and via reach to home station. RAF/GRF intelligence data requirements will vary based on echelon and mission sets. A brigade combat team will need more narrowly tailored data sets than a GRF unit or a RAF division headquarters interested in global or area of responsibility-wide data sets. The MIB(T), which provides the ASCC its Theater Analysis and Control Element, can assist RAF/GRF units in determining what data is needed and where the data is available and can recommend how to access, ingest, and manage that data.
- **Systems.** The MIB(T) is an integrated element of the theater's intelligence structure, which includes the support that the GCC receives from Joint and National capabilities. This enables the MIB(T) to convey access to these capabilities to RAF units via the DCGS-A as they prepare for, and execute operations in support of the GCC. Additionally, the MIB(T), working through the INSCOM staff, can leverage INSCOM's unique relationships with Defense and National Intelligence Community organizations (e.g., National Security Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency) to coordinate Intelligence Enterprise systems support to tactical-level operations.
- **Synchronization/Collaboration.** Under the operational control of the ASCC, the MIB(T) synchronizes and coordinates intelligence activities in the GCC area of operations to support the unity of effort and coherence of the Intelligence Warfighting Function. This includes a role in the coordination of intelligence sharing and interoperability with allies and partner nations. The MIB(T) also extends to the theater-level intelligence-connected functions that INSCOM delivers to the Army as a whole. The MIB(T) can leverage the capacity of INSCOM's functional subordinate commands and organizations, as well as the intelligence community, in support of RAF, GRF, and Prepare to Deploy Order missions. This support can include assistance with intelligence and electronic warfare equipment maintenance, Joint Worldwide Intelligence Communications System issues, Quick Reaction Capabilities fielding/training, and intelligence-specific logistics and contracting. The types of intelligence support with the corresponding INSCOM organizations that provide or facilitate it are displayed below.

Aerial ISR and PED* –116th MI Bde (Aerial Intel)
*(*Processing, Exploitation, & Dissemination)*

HUMINT–Army Ops Grp (AOG), INSCOM G-2X (IG2X)

OSINT–Army OSINT Office, Intel Information Services (IIS)

Analysis & TECHINT–National Ground Intel Center (NGIC)

SIGINT–Army Cryptologic Ops (ACO), 704th MI Bde, 706th MI Grp
Meade Ops Center (MOC), European Cryptologic Center (ECC)

Counterintelligence–902nd MI Grp, IG2X

GEOINT–Army GEOINT Bn, Army GEOINT Office (AGO)

Intel IT & Knowledge Management–Ground Intel Support Activity (GISA), IIS, NGIC

Intel Support to Cyber Operations–780th MI Bde

Contract Linguist Support–Contract Linguist & Intel Programs Support Office (CLIPSO)

Intel Community Support (NSA, NGA, DIA, NRO, CIA, FBI, State)–INSCOM HQ, ACO, 704th MI Bde, 706th MI Grp, AGO, IG2X, NGIC, AOG, 902nd MI Grp, Army Field Support Center (AFSC)

- **Training.** INSCOM provides the following training support to RAF and GRF units:

–*Foundry program-funded live environment training (LET)*. RAF Soldiers, through TDY funded by Foundry, embed in an MIB(T) element to gain experience and expertise with live collection and analysis on the same region and adversaries against which their RAF unit is aligned. A complete listing of LETs is in the Foundry Catalog at https://www.us.army.mil/suite/doc/45681127 [Catalog access is controlled/limited to official DoD users.]

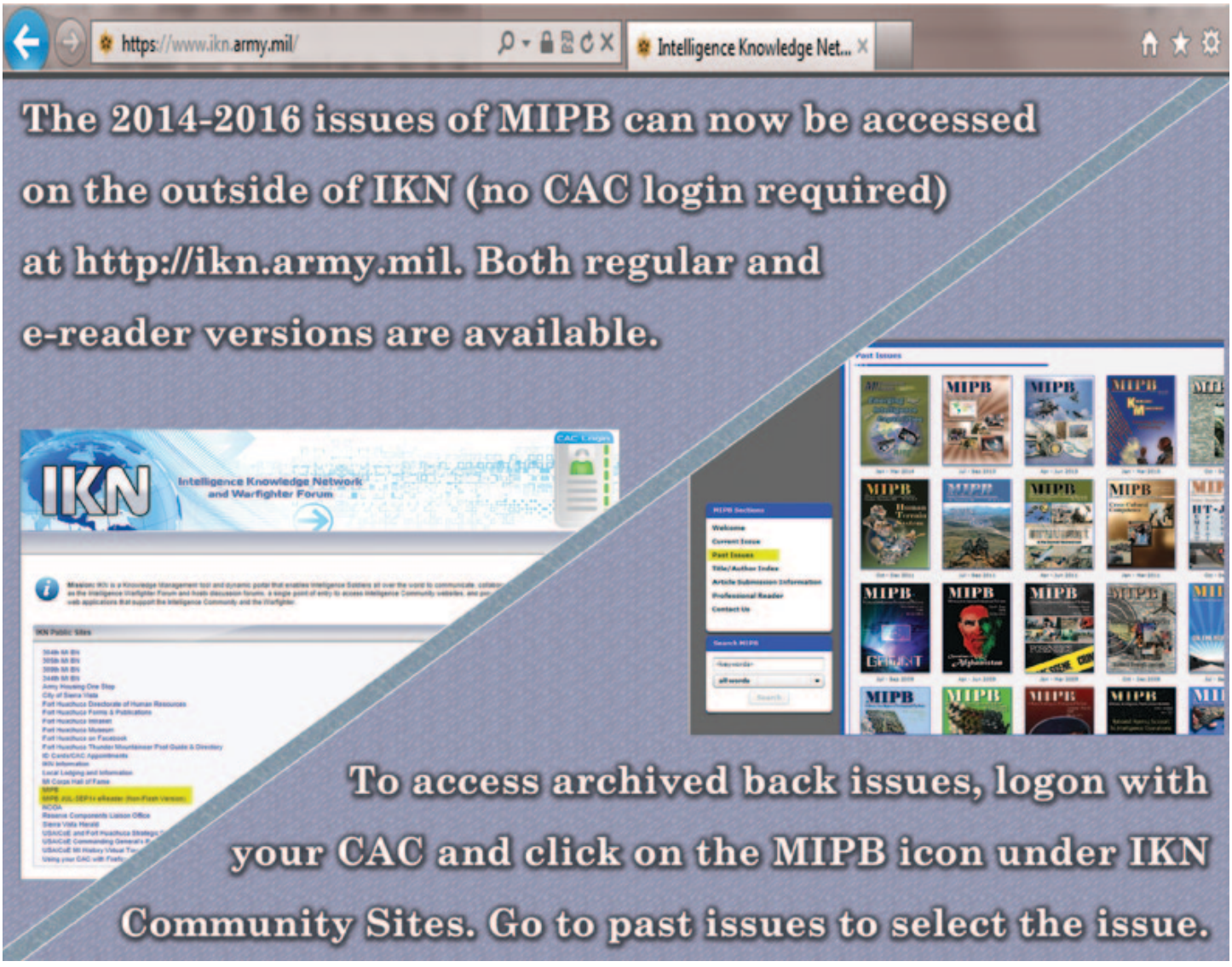
–*Mobile training teams (MTT).* From the Foundry catalog, RAF units can select MIB(T) MTT-delivered course material to receive theater-specific training that would not otherwise be available at their home-station.

–*Home station exercise support.* For Mission Command Training Program Warfighter and mission rehearsal exercises, the MIB(T) can work with RAF units to deliver reach support to home station that, within the context of exercise scenario, replicates architecture, processes, and data flow the unit will encounter when deployed.

–Combat training center (CTC) support. To ensure that units train and certify against a realistic expeditionary operating environment, MIB(T)s will reinforce existing Foundry personnel at the CTCs to portray theater-level intelligence support (architecture, processes, data flow).

Conclusion: The Intelligence Anchor Point Supports RAF/GRF Readiness for Expeditionary Missions

The MIB(T), reinforced by INSCOM's functional brigades, supports RAF/GRF at all levels to assist with integration into the theater enterprise before, during, and after deployment. Through the MIB(T) Anchor Points and functional brigades, INSCOM, along with the MIRC, brings the full capabilities of the National Intelligence Enterprise to supported operational and tactical level commands to ensure they have the necessary intelligence to conduct expeditionary operations, which contributes to the Chief of Staff of the Army's #1 priority–remaining ready to win in the "unforgiving crucible of ground combat."



Operationalizing the Army Total Force Policy: USFK's Model for AC/RC Integration

by Colonel Kris A. Arnold, 501st MI Brigade Commander, Lieutenant Colonel Jens Hansen, 368th MI Battalion (RC) Commander, and Lieutenant Colonel David Hazelton, 501st MI Brigade S3

"Much of America's Army's capacity is resident in the Reserve Components, and we must rely more heavily on them to meet the demands of a complex global environment."

–General Mark A. Milley, Chief of Staff of the Army, 22 March 2016

"ISR remains my top readiness challenge and resourcing priority as CFC/USFK requires increased, multi-discipline, persistent ISR capabilities to maintain situational awareness."

–General Curtis Scaparrotti, USFK Commander, Testimony to the Senate Armed Services Committee on 23 February 2016

Introduction

Two years ago the Secretary of the Army signed the Implementation of the Army Total Force Policy to increase the integration of the Active and Reserve Components (AC/RC). Effecting implementation of this policy is increasingly important as resources become more constrained. Within the intelligence enterprise, operating with constrained or limited resources is a constant–there is never enough intelligence, surveillance, and reconnaissance to meet the demand. This persistent condition spurs Military Intelligence (MI) leaders to continually identify ways to maximize efficiency and leverage all available resources.

For the 501st MI Brigade, which is responsible for providing U.S. Forces Korea critical Indications and Warning, this challenge has translated into leveraging the regionally aligned 368th MI Battalion (RC) to the fullest extent possible. Through four lines of effort (LOEs), *resourcing, training, integrating, and command emphasis*, the 501st MI Brigade has achieved great success in operationalizing the Army's Total Force Concept. How the Brigade (BDE) and Battalion (BN) leveraged these LOEs are discussed here.

Resourcing

The saying "vision without resources is hallucination" is apropos. Resources are one of the key factors to enabling integration, especially those that are foundational–communication equipment, architecture, and systems. For our Theater Aligned Intelligence Reserve Battalion, a key resource is the Distributed Common Ground System–Army (DCGS-A). The 368th MI BN has not yet fielded this key MI "weapon system," driving the 501st MI BDE to temporarily hand receipt DCGS-A systems to the 368th at home station to support a full array of operational capabilities. As 368th capabilities increase, the 501st has concurrently assisted in developing the supporting architecture.

The 501st goal for the BN is to grow the capability to replicate all core missions to some capacity, allowing federation and surge capacity during a crises. One of the 501st high profile missions that the 368th MI BN fills is the Deployable Intelligence Support Element (DISE). In the event of a crisis or war, the theater demand for a DISE would be instantly realized. Accordingly, the 501st has acquired the DISE equipment set in Korea (prepositioned), while the 368th provides the personnel on a rapidly deployable basis. Deploying the a small number of Soldiers from the 368th MI BN with only their personal gear would preclude the CONUS organization from having to compete with other units in the airload process, resulting in a reduced timeline to realize full operational capability.

Training

Resources are foundational, but Soldiers also must be trained on how to use those resources to make them effective. This training is more challenging for the RC than

the AC, given limited time during Battle Assemblies/Annual Training. To tackle this training challenge, the 501st MI BDE has routinely sent experienced AC Soldiers on temporary duty to participate in and lead the 368th's Battle Assembly training. This training integration is to ensure Reserve Soldiers understand the Korea-specific operational environment, which is focused on conventional warfare and battle damage assessment tracking.

To maximize integration, training standards for both the AC and RC must be the same. The standard operating procedures and mission essential task lists focus between the two Components must completely mirror one another. Timing is also essential. Training focuses on preparing reserve Soldiers prior to major exercises to ensure those teams can fully integrate immediately. Additionally, the BDE developed a process of evaluating 368th training holistically throughout the year, culminating with Key Collective Task validation during its support to a major theater exercise. Training utilized two important training principles: train while operating and train as you fight.

Integrating

Historically, Reserve integration has been problematic due to the challenges of assuming a full AC mission set in a timely manner. The tenuous security environment within Korea cannot accommodate a multi-week ramp-up; the BDE requires the BN to assume mission during crises in a matter of days or even hours. To make this rapid assumption of mission feasible, the 501st has focused the 368th on specific mission sets such as the DISE. Constant and robust communication between units is therefore paramount. Both units have invested in liaison officers at one another's locations with full-time officers, as well as a steady flow of rotating Reserve lieutenants for short-term assignments in Korea. The "3rd shift" mission of the 368th MI BN has moved from mere integration to interdependence. During Korean nights, a team of 368th analysts in California continues the intelligence cycle and ensures 501st Soldiers report to duty with an informed handoff.

In addition, an often under-recognized yet significant attribute of the relationship is the enduring continuity that the 368th MI BN brings to the fight. Most 501st Soldiers rotate out of Korea after just one year, while many of the Reserve Soldiers remain in the 368th for over a decade. The level of expertise that the Reserve Soldiers attain over this extended time frame turns them into the experts, possessing a level of understanding rare among rotational AC Soldiers. This interdependence fosters a trust between units that solidifies the value that each brings to the fight.

Command Emphasis

Command teams must expend the requisite time, energy, and attention to emphasize activities that are of the highest priority. This is not missed in the 501st/368th relationship. The 501st BDE Commander attends each 368th Battle Assembly via VTC to address the formation. Topics range from training focus, to exercise planning, to military professional development. Unit cohesion is another essential point of command emphasis. The 368th recognizes this intangible LOE through events including Hail and Farewells, OPDs/NCOPDs, holiday family events, and unit competitions. These seemingly minor activities strengthen cohesion within and between units.

At the other end of the spectrum, the Brigade and Battalion Commanders collectively develop multi-year training plans that ensure training is logical, cumulative, and properly resourced. This coordinated planning is essential because the inevitable leadership churn in both the 501st BDE (Korea) and 368th BN (California) creates the risk of a sporadic approach to long-term mission requirements. Both units have consciously chosen to focus Reserve efforts toward becoming experts in a narrow set of mission sets, instead of becoming the proverbial "jack of all trades, master of none." This mission focus requires active prevention of "good ideas" from detracting from the core mission tasks agreed upon by the two Commanders.

Conclusion

The 501st MI Brigade (Theater) (MIB (T)) and 368th MI Battalion (RC) have pioneered a mutually beneficial model for AC/RC integration in the face of a critical intelligence mission set: Indications and Warnings of North Korean aggression. This dynamic threat presents a mission set that can never be fully exploited, making the integration of a theater-aligned Reserve battalion's capacity a critical enabler to success. Through the additional resources provided by an integrated Reserve battalion, a coherent training regime that endures the test of time, a deliberate approach to integration, and command emphasis to bring it all together the 501st MIB(T) and 368th MI Battalion have proven that AC/RC integration can–and does–work even when tested by a challenging operational environment. This integration has filled collection gaps, drastically increased capabilities, raised morale, and allowed for collective mission accomplishment at a level greater than either Component could ever achieve apart. In light of GEN Milley's challenge to "rely more heavily on them (RC) to meet the demands of a complex global environment," Korea's MIB(T) and Theater-Aligned Reserve Battalion have found a way to make this work–even thrive–in uncertain times.

Multinational Interoperability Challenges in Information Collection

by Captain Peyton Hurley

Introduction

Since the fall of the Berlin Wall and the end of the Cold War, the North Atlantic Treaty Organization (NATO) Alliance has welcomed many new allies, shifted priorities, and revised operating concepts. This makes today's NATO, which is conducting operations in Afghanistan and simultaneously confronting a resurgent Russia, very different from NATO of twenty-five years ago. One of the biggest changes besides the introduction of new allied nations is the operational scope of multinational operations and the challenges of interoperability at the tactical level.

Under the previous NATO architecture, member nations only integrated at the division and above level. Today NATO multinational operations occur at the brigade level and below. Since NATO doctrine focuses on facilitating operations at the division-level and above, multinational brigades and battalions struggle to integrate information collection (IC) into their operations. Large disparities in capacity and capabilities among member nations further exacerbate this lack of NATO doctrine, standardization agreements (STANAGs), and standard operating procedures (SOPs) at the tactical level.

While these challenges will likely persist, they are not insurmountable, and there are several things battalions and brigades participating in multinational operations can do now to alleviate many of these challenges. This article seeks to frame the current problem within multinational information collection and provide recommendations for solutions and refinement. The observations provided herein are Observer-Coach/Trainer (OC/T) observations of battalion-level task forces in three different Joint Multinational Readiness Center (JMRC) training exercises

While very different in both rotational construct and participating units, these rotations provide many useful insights into information collection practices. The article begins with a brief discussion of U.S. Army IC doctrine, other allied nations' IC doctrine and capabilities, and then presents examples from JMRC rotations to highlight interoperability challenges. The article closes with recommendations for additions to NATO doctrine, for allies participating in multinational operations, and for U.S. units serving as multinational brigade headquarters or as battalions subordinate to a brigade task force under the command of an ally.

U.S. Information Collection Doctrine

New IC capabilities have emerged over the previous fifteen years of conflict in Iraq and Afghanistan, and the Army has updated its IC doctrine to allow for proper planning and synchronization of information collection and ensure the primacy of commander's critical information requirements (CCIR). "I*nformation collection*[1] is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as processing, exploitation, and dissemination systems in direct support of current and future operations."[2]

Information collection involves three tasks each with different proponents: the S2/G2 plans requirements and assesses collection; the S3/G3 tasks and directs collection; and the reconnaissance, surveillance and military intelligence units and Soldiers execute collection.[3] Some key features will illuminate elements of allied doctrine as well as recommendations for units participating in multinational operations.

Information collection is a collaborative intelligence and operations process that is integrated between echelons, adjacent units, and unified action partners to answer CCIR so the commander can make decisions. Various allied nations have somewhat different concepts of the purpose of information collection and very different capabilities to collect information, leading to potential conflicts during multinational operations.

Observations of Allied Doctrine

NATO nations each have different doctrine at the brigade-level and below. These differences seem to have increased in the last decades as different nations have adopted different solutions to modern conflicts and increased IC capabilities. These differences are greatest between the U.S. and Western European, and Eastern European doctrines. There are generally two reasons for such a wide divergence: different expectations and organizational cultures with respect to

the purpose of information collection, and different capabilities and the derivative staff capacity to integrate information collection capabilities.

While U.S. doctrine focuses IC assets and resources on collecting information to answer CCIR or for target acquisition, other nations often use collection platforms in the close fight as a security force, usually to screen, even during offensive operations. Reconnaissance and surveillance assets deploy in front of the forward-line-of-own-troops in order to report composition and disposition of enemy forces to the main body. This defensive employment of collection assets is essentially a screen mission, not dedicated information collection to answer priority intelligence requirements (PIR). While the brigade or battalion may task the screening element to observe and report on enemy locations, they rarely provide specific intelligence requirements. Additionally, units rarely tie CCIR to decision points with a decision support template or matrix. Failure to link collection assets to PIRs and decision points limits the commander's ability to make tactical decisions.

Lastly, some NATO armies, particularly in Eastern Europe, assign the responsibility to manage the collection process exclusively to the intelligence staff. The S2 plans the intelligence requirements, tasks the units to collect information, then conducts the production and dissemination of intelligence from the collected information. This is significantly different from U.S. and Western European doctrine, where collection is a collaborative process between the S2 and the S3. This leaves open the possibility that the IC plan will not support the maneuver plan or other aspects of the operational plan.

Soldiers from the 74th Czech Battalion plan for offensive operations in Operation Allied Spirit II in August 2015. (Photo courtesy of JMRC/Released.)

Allied Information Collection Capabilities: Collection Assets, Resources, and Staff Capacity

The U.S. military has invested significantly in collection platforms in the past decade, an area many other NATO militaries have not matched. As a result, many allied armies are not accustomed to operating with and integrating many IC assets and resources to support their overall IC plan. Unfamiliarity with increased collection assets has led to a gap in allied IC doctrine. Many allied nations also lack the staff capacity to plan for the integration of these assets into the overall plan. Lastly, while U.S. doctrine encourages and rewards units that request and successfully utilize higher echelon IC assets, many allied nations do not take advantage of these resources. Asking for additional collection resources, according to their organizational culture, tacitly admits they cannot accomplish the mission on their own.

Observations on the Impacts of Doctrinal Differences

Differences in U.S. and allied partners' IC doctrine, capabilities, and capacity are not so divergent that multinational task forces are unable to interoperate successfully. Rather, the nuanced differences lead to an underutilization of IC assets from allies, particularly under a U.S. brigade headquarters. Not once during three rotations at JMRC did the observed battalion headquarters request additional collection resources from brigade or echelons above brigade. Technical barriers to successful integration of collection platforms (e.g., no One System Remote Video Terminal) certainly exist, but are manageable. Rather, organizational culture that prevents requesting additional support, coupled with unfamiliarity of collection platforms and a lack of staff capacity to integrate these resources, causes underutilization of available assets. During JMRC rotations, the lack of

U.S. Soldiers of Brigade HHC, 1st ABCT, 3rd ID and a Dutch soldier (center) of 43rd Mechanized Brigade conduct an IC plan brief during exercise Combined Resolve V at the JMRC, October 2015. (U.S. Army photo by SSG Carol A. Lehman/Released)

collection assets dedicated to multinational battalion task forces often caused the intelligence staff to develop a flawed intelligence picture within the battalion, which skewed brigade situational understanding. This hindered the utilization of the brigade's decision support matrix and inevitably caused the brigade commander to make uninformed decisions. Brigade-level collection cannot substitute for such poor situational understanding from subordinate battalion task forces.

Additionally, allied armies' utilization of the reconnaissance assets as screening forces decreases those assets' effectiveness. As noted, the collection of information to answer PIR that drive decisions becomes a secondary task of many allied nations' collection assets. When higher headquarters allocates collection assets during an operation, they are unable to integrate these resources as anything other than security forces because utilizing IC assets as security forces does not require detailed collection planning from the staff. Much of that planning responsibility shifts to the security force. Without the underlying staff products that drive the collection process (good PIRs, event template, named area of interest overlay, IC plan, etc.), it is impossible to integrate additional collection resources that answer PIR and drive decisions, particularly in the battalion deep fight. While U.S. units often struggle to produce all of these products with sufficient detail as well, they tend to be more familiar with integrating collection assets and resources to answer CCIR.

Key personnel from the Romanian 191st IN BN, a multinational task force with soldiers from Romania, Bulgaria, Albania and Georgia, participate in a Combined Arms Rehearsal during Operation Combined Resolve V in October 2015. (Photo courtesy of JMRC/Released.)

Lastly, since many NATO armies assign the responsibility of managing the collection process to the intelligence staff, the collection plan and the maneuver plan become de-synchronized. As the operation proceeds, information collection becomes less relevant to the commander's decisionmaking. While this phenomenon is certainly attributable to the intelligence staff's exclusive responsibility for information collection, the staff could overcome this obstacle by ensuring the intelligence staff has a very good understanding of the maneuver plan and the commander's decision points. Unfortunately three products or processes–a decision support template and matrix, wargaming, and a rehearsal that incorporates the IC plan–are either not completed or lack sufficient detail.

Recommended Changes to NATO Doctrine

Current NATO doctrine for information collection, Allied Joint Publication-2.7 *Reconnaissance and Surveillance* and Allied Tactical Publication-77 *NATO Guidance for ISTAR in Land Operations*, focuses on echelons above brigade. As the paradigm for multinational operations has shifted since the end of the Cold War, with multinational units interoperating at the brigade and battalion level, it is imperative to develop doctrine and STANAGS applicable to brigades and below. Different allied armies will have their own internal processes for developing requirements and planning for the utilization of collection assets and resources. SOPs can overcome many of these differences. NATO doctrine, however, must address two areas: staff proponency for information collection, and the primacy of answering CCIRs throughout the IC process.

Recommendations for Allied Armies

While NATO doctrine does not specifically address information collection at the brigade level and below and allied armies do not have a doctrinal imperative to align IC processes, allied nations can begin to align doctrine on their own. While addressing the aspects of staff proponency and CCIR primacy are certainly a start, allied armies should also begin to build the staff capacity to integrate collection resources from higher echelons that they are not accustomed to controlling. Again, some technical barriers exist, but the underlying staff functions that allow an allied nation to develop requirements and plan information collection are not technical. Home station training exercises that incorporate the full suite of collection platforms that are available while operating in a multinational operation with U.S. units would familiarize allied nations with the capabilities of these collection resources and accelerate the development of the staff capacity to integrate them.

Recommendations for U.S. Units Participating in Multinational Operations

U.S. Army units typically contribute most of the collection assets in a multinational operation, so most of the salient recommendations to improve interoperability in information collection are for U.S. units, particularly brigade

headquarters. These recommendations fall into three areas: understanding subordinate units' IC doctrine and processes; IC SOPs for multinational operations; and the use of liaison officers (LNOs).

The most important action a U.S. brigade headquarters should undertake to increase the effectiveness of information collection prior to a multinational operation is to understand their subordinate units' processes for developing requirements and planning information collection. The brigade staff must also understand their subordinate units' capacity to integrate collection resources into the battalion collection plan. This requires robust coordination between intelligence staffs at different echelons prior to the start of multinational operations. Additionally, U.S. units must understand that allied armies' organizational cultures might lead to a reluctance to admit unfamiliarity with information collection or to request additional collection resources. While this is difficult to ascertain during the initial formation of a multinational task force, U.S. units should use IC rehearsals and intelligence synchronization meetings to gauge familiarity with, capacity to use, and willingness to request collection resources. When in doubt, the brigade staff should not wait for a battalion to request collection resources. Allocating assets early in the planning process, according to the priority of information collection, will allow the battalion staff to better integrate them into their plan, rather than wait to recognize a requirement and request the resource.

While U.S. units often have SOPs for information collection, they rarely have SOPs specific to multinational operations. SOPs help reduce or eliminate some of the technical barriers to information collection such as reporting procedures and dissemination methods. Predetermined reporting formats and robust contingency plans for all types of information allow brigade and battalion task forces to focus on the procedural challenges within multinational information collection.

Lastly, the success of information collection in multinational operations often hinges on the strength of the LNOs. JMRC OC/Ts consistently observe that the brigades best able to overcome interoperability challenges within information collection have been those that send the strongest LNOs to subordinate battalions. As an example, during a recent rotation, the U.S. brigade headquarters sent an intelligence captain to serve as the S2 LNO to a multinational battalion. This LNO was able to facilitate communication and coordination between the brigade and multinational battalion intelligence staff. As with all liaison operations, LNOs must have a clear understanding of their duties and responsibilities as well as the resources available to accomplish the mission. If the allied staff is not familiar with collection assets or request procedures, the brigade S2 should consider tasking the S2 LNO to serve as an *ad hoc* collection manager. This allows the S2 LNO to remain in constant communication with the brigade, with a clear understanding of the battalion's operations, while alleviating potential procedural information collection limitations.

173rd LNO relaying 74th Czech Battalion operational plans to his headquarters. Competent LNOs proved essential to success during Operation Allied Spirit II in August 2015. (Photo courtesy of JMRC/Released.)

Conclusion

New NATO operating concepts have challenged multinational task forces at the brigade level and below as they attempt to resolve interoperability challenges. While optimal use of information collection during multinational opera-

A Soldier from B Co, 10th BEB, 1st ABCT, 3rd ID launches a RQ-20A Puma UAS while attending a training course during Exercise Combined Resolve V at the JMRC, October 2015. Exercise Combined Resolve V trains the U.S. Army's regionally aligned force to the U.S. European Command area of responsibility with multinational training at all echelons. Approximately 4,600 participants from 13 NATO and European partner nations will participate. The exercise involves around 2,000 U.S. troops and 2,600 NATO and Partnership for Peace nations. This is a preplanned exercise that does not fall under Operation Atlantic Resolve and trains participants to function together in a joint, multinational, and integrated environment. (U.S. Army photo by SGT Brian Chaney/Released)

tions is difficult, it is not impossible, and it is vitally important that multinational units get it right during future conflicts. While this article presents some specific recommendations for U.S. and allied units, it is important to realize that multinational units can overcome most procedural interoperability challenges through constant dialogue, which facilitates shared understanding. Shared understanding includes our ability to see ourselves and our allies to leverage strengths, mitigate weaknesses, and accomplish the mission.

Endnotes

1. Information collection and intelligence, surveillance, and reconnaissance (ISR) have the same definitions as defined in FM 3-55 and JP 2-01, respectively. Information collection is distinct from ISR in that IC focuses on answering CCIR while ISR is a joint and more inclusive term that includes intelligence, surveillance, or reconnaissance operations not directly tied to answering CCIR. This article uses information collection or IC exclusively to maintain consistency. A reader from a sister service or an allied army could use the terms interchangeably.

2. FM 3-55 Information Collection, May 2013, 1-1

3. FM 3-55, 1-1 and ATP 2-01 Plan Requirements and Assess Collection, August 2014, 1-1

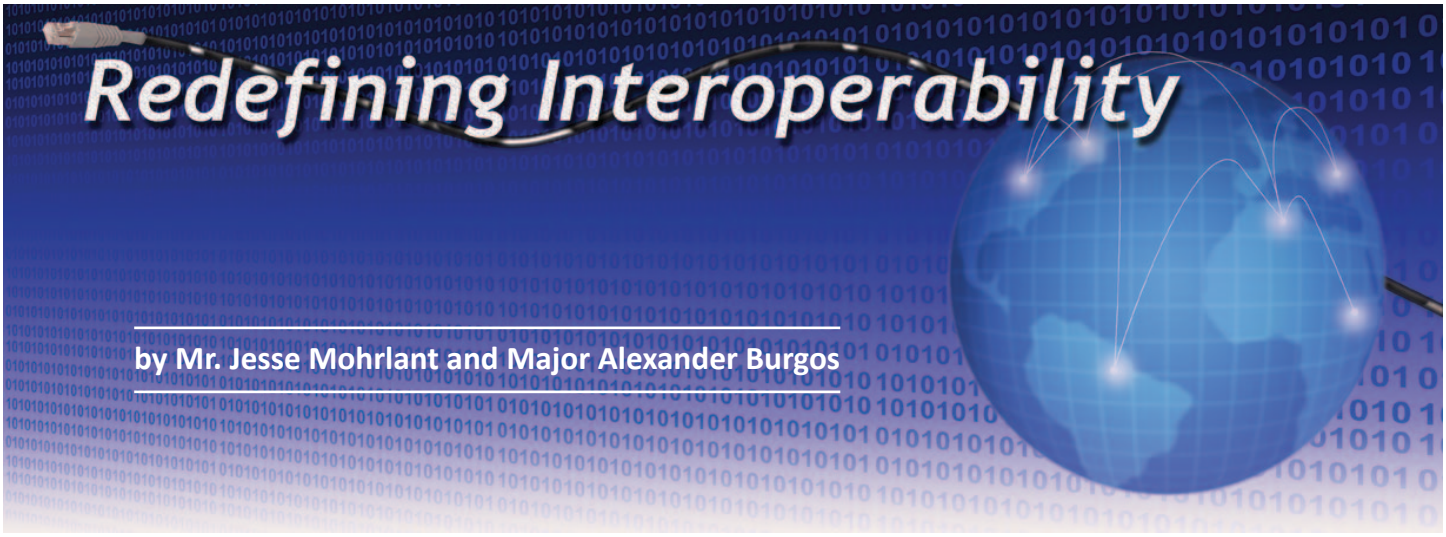
References

Joint Publication 2-01 Joint and National Intelligence to Military Operations, January 2012.

Allied Joint Publication-2.7 Allied Joint Doctrine for Reconnaissance and Surveillance, July 2009

Allied Tactical Publication-77, NATO Guidance for ISTAR in Land Operations, May 2013

CPT Hurley is currently assigned as a BN Intelligence OC/T at JMRC. He previously served as a battalion S2 and company commander at Fort Drum, New York and as a rifle platoon leader, company executive officer, and battalion S4 at Joint Base Lewis-McChord, Washington. He deployed twice to Afghanistan in support of Operation Enduring Freedom as both an infantry and military intelligence officer. He holds a BS in Economics from the U.S. Military Academy.



Redefining Interoperability

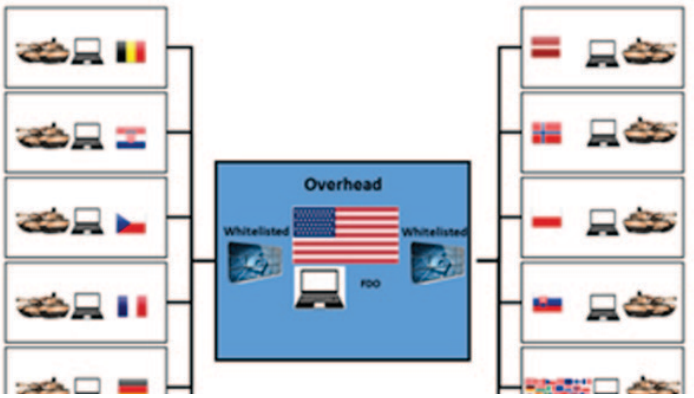
by Mr. Jesse Mohrlant and Major Alexander Burgos

The Problem: Lack of Architecture to Support Interoperability

Combatant commanders (CCDR) and Army Service Component Command (ASCC) commanders around the globe are faced with the same problem in every theater: transmitting need-to-share, high-veracity, structured and unstructured actionable data in near-real time. The challenge is that we often over-engineer a solution that ultimately limits us to only being able to pass data at the combined joint task force (CJTF) headquarters (or higher); creating an illusion that interoperability has been established when it truly has not. The danger in not having true interoperability, is that we cannot action it at all operational levels on the coalition systems. To complicate things further, there is often so much disparity between our systems, that even if we could pass structured data, our coalition partners wouldn't be able to convert our message formats into their program of record (POR) for tracking, analysis, and ultimately targeting where required.

Current Data Sharing Model

Interoperability has created a paradigm in our current operating environments that has pushed the preponderance of overhead away from data management to network management. The network management approach to the problem will always preclude us from making the data both available and actionable in real time because there is no direct access to their networks. It can be further convoluted with unilateral, bilateral, and multilateral agreements, and the ability to share data across multiple domains simultaneously. Our current model requires multiple layers of networks, encryption devices, and services management and does not allow for a rapid, tailorable, cost-effective expansion into unknown environments that are constantly changing. An event today can very quickly change information sharing agreements that were previously non-existent or hampered. If we can change our focus from network structure to data structure, we can rapidly change access as required.



Author: Jesse Mohrlant

Figure 1. Simple example demonstrating network overhead requirements in a current Multi-National Intelligence Architecture.

Interoperability Approaches: What Works?

Combatant Commands' theater Systems Integration Officers have seen three primary approaches to this problem framed by the existing data structure. The first is typically placing a Multi-National Intelligence Readiness Operations Capability (MN-IROC) into a CJTF headquarters. This approach allows for releasable data to be shared in hard copy (and sometimes on the computer screen) with our coalition partners once approved by the Foreign Disclosure Officer (FDO). This process is often very inefficient in that it requires an FDO to approve it prior to being placed into a repository accessed by the MN-IROC, and once again when presented to the coalition partner.

There is also a requirement to "air gap" the data (moving the data either by a removable device, by copying from one screen to another, or by transposing data manually from a hard copy). This makes the information less actionable/timely, risks compromise of data/network integrity through

the removable device, and introduces the human factor that could potentially transpose information, grid coordinates, etc.

This also frequently requires additional security measures for the available networks, operational areas, and permissions to allow coalition partners to access the U.S. systems. U.S. intelligence organizations have inherited the overhead required to extend and manage the network that precludes intelligence production in an environment that is already heavily resource constrained. A positive side effect of this process is that we have learned how to move the transport layer into these headquarters, which could still allow a U.S.-only presence (where required) in support of the CJTF.

The second approach, is a modified MN-IROC approach, where we work on, or with, a coalition network that is typically promulgated again only to the CJTF headquarters. This approach is typically very costly to the coalition partner (and us) as it requires the purchase, maintenance, and accreditation of additional equipment. The introduction of our POR systems into their formation, encryption devices to allow passing of data between us and them, not to mention redundant circuits to the same location (U.S., coalition, and their organic network at a minimum) all comes at a cost. Despite our best efforts, it still requires an "air gap" to their POR, multiple FDOs (in depth), and a tremendous amount of overhead that is not resourced in either formation.

Recently, U.S. Army Europe requested the Program Executive Office, Command Control Communications–Tactical's assistance with developing a solution. One of their recommendations was to issue a third Mission Command System Stack to the ASCC. If this course of action is pursued, a decision point will have to be made to convert existing U.S. Army Battlefield Command Systems baselines (to include the Distributed Common Ground System-Army (DCGS-A)) to the coalition approved software release for their network, or an Operational Needs Statement would have to be submitted to the Department of the Army to source additional systems. At the end of the day, we are still incapable of actioning data on the coalition system and we are potentially expecting them to purchase and learn a new baseline that is arguably moribund within our own formations. Both of these approaches push the overhead for networking, encryption devices, FDOs, etc. towards the network, and not at the veracity of the data.

The third approach, is leveraging "Whitelisting" web services to coalition partners. This technology was first developed around 2009 in an attempt to apply heuristics to email messages to reduce spam. The technology was later refined

Figure 2: Simple example of potential reinvestment of network overhead into data management of a Multi-National Intelligence Whitelisted Architecture.

to Domain Name Service (DNS) whitelisting, which limited certain websites from sending/accessing data. In its current form, the Defense Information Systems Agency has a capability that allows a series of guards (one on the U.S. side and one on the coalition side), to allow access to a specific web based service from a very specific IP Address. The service uses a series of authentication protocols to verify that the user accessing the coalition side from a specific IP with the correct credentials, is authorized to access the U.S. web service and its releasable data.

This approach reduces overhead because it now allows more analysts to focus on the veracity of the data and less on all of the security levels, as you have now centralized the risk to the point of access. This approach allows coalition partners to access the data from their organic systems, which also allows them to target, add, modify, delete (or whatever permissions we give them) to the data. The FDO now only has to allow which fields within a relational database are truly releasable (typically the icon is always unclassified and the remarks are nearly always releasable). The data that cannot or should not be released, (i.e., source) would not be available to the individual/organization accessing the data.

DNS Whitelisting Advantages/Disadvantages

The advantages to this approach are broad. We no longer need security services in depth (multiple FDOs, security guards, additional crypto and networking for every coalition partner, etc.) The coalition doesn't have to purchase additional hardware. The coalition and U.S. are no longer co-dependent for life cycle replacements, etc. We could upgrade the entire system from DCGS-A to any follow-on system or service as long as the data is available in a SQL or Oracle da-

tabase, it would be transparent to the end users across all forces.

This approach is not a simple one. It assumes much risk for the ASCC and CCMD from an accreditation standpoint, especially for the Designated Approving Authority. This would have to be mitigated by the coalition's ability to meet our accreditation standards, by validating their Body of Evidence (BOE) as they request permission to access the data services. This BOE would have to be routinely updated to ensure that they remain in compliance with established security standards. This cost is still marginal compared to the aforementioned courses of action (they would use their own existing equipment, vice having to purchase ours), and it helps the coalition (as well as us) identify and implement industry standards to make both coalition and U.S. networks more secure and less susceptible to cyber network attacks.

It also requires the data to be structured in such a way that either certain fields can be released from the existing database (giving each field in a record its own security label), or the ability to export portions of the data in such a way that it is releasable to the coalition partner. Because the data is available via a web portal, it allows for a tailorable common operating picture (via Geo Fusion Viewer) as well as the ability to target and action data on their organic systems in near real time while eliminating dependencies on multiple networks.

Conclusion

As commanders are presented solutions to these complex problems, we cannot lose sight of the end state. Interoperability is not defined as "presence in the tactical operations center," it is defined by providing high veracity data that is actionable on our own organic systems (U.S. and coalition). When combined with waning resources, and potentially increasing numbers of vulnerabilities through multiple networks, cost benefit analysis leads us to a solution with less points of failure, while simultaneously increasing all coalition partner's ability to secure their networks in the pursuit of defeating and/or deterring a common antagonist while operating with their own organic systems. This is the definition of true interoperability.

Mr. Mohrlant is currently the Intelligence Enterprise Manager for the 66th MI Brigade. During his career, he has served as a master analyst, field software engineer, intelligence integration officer, and knowledge manager in PACOM, EUCOM, and CENTCOM theaters.

MAJ Burgos is currently the 24th Military Intelligence Battalion Operations Officer within 66th MI Brigade, Wiesbaden, Germany. He has served as a BDE AS2 in both 1st and 2nd BDE, 1st Infantry Division, Fort Riley, Kansas. He was also the MI Company Commander for 1/1 BSTB, 1st BDE, 1st Infantry Division, Fort Riley, Kansas. He has deployed in support of Operations Iraqi Freedom and New Dawn. He holds a B.A. from Virginia Tech University and an MA from the National Intelligence University and University of Oklahoma.

Information Collection Failures that Lead to 'Discovery Learning'

by Captain Raymond A. Kuderka and Captain Andrew H. Eickbush

This article was first published in ARMOR, April-June 2015, Fort Benning, Georgia.

Introduction

"Before I can develop the ground maneuver plan I need to know what the enemy is doing." It's a sentence echoed by operations officers during every scenario conducted at our Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany.

Intelligence preparation of the battlefield is the intelligence officer's primary task during mission analysis and serves as the catalyst, synchronizing information collection (IC) with a ground maneuver plan throughout the duration of the military decision making process. The IC process at face value seems simple enough: staff provides analysis in the form of the commander's critical information requirements (CCIR), thus enabling the commander to make informed operational decisions. But we have noticed that in most decisive action training environment (DATE) rotations at JMRC, regardless of unit type–whether light, heavy or motorized–or nation of origin, units fail to plan and execute an IC plan that supports the commander's decision making process.

Why? Though not all encompassing, most shortcomings of IC planning/execution can be attributed to the following failures:

- ✦ Not defining the operational framework.
- ✦ Producing convoluted IC overlays.
- ✦ Not understanding organic IC capabilities.
- ✦ Not prioritizing assets.
- ✦ Executing inadequate staff coordination.

The result of these inefficiencies often leads to unnecessary discovery learning as the unit crosses the line of departure with little situational understanding of the immediate fight. The following five problem sets describe established patterns we regularly see during rotations at JMRC. Each provides a starting point for discussion. The intent is for each unit to acknowledge these common shortcomings and provide a unit-tailored solution based on composition, disposition, and mission to set the conditions for success.

Problem Set 1: Defining the Operational Framework

Army doctrine on unified land operations states that "Army leaders are responsible for articulating their visualization of operations in time, space, purpose, and resources."[1] This is accomplished through the development of a standardized operational framework that is consistent throughout all echelons. There is a direct connection between defined framework and its application to the development and execution of an IC Plan. Most units' intelligence sections analyze the mission in a framework that most closely resembles the "Deep-Close-Security" framework. According to this framework, "areas of operation can be divided into three distinct parts: support area, close area, and deep area."[2] Throughout the remainder of the article we will use this framework to discuss observed trends.

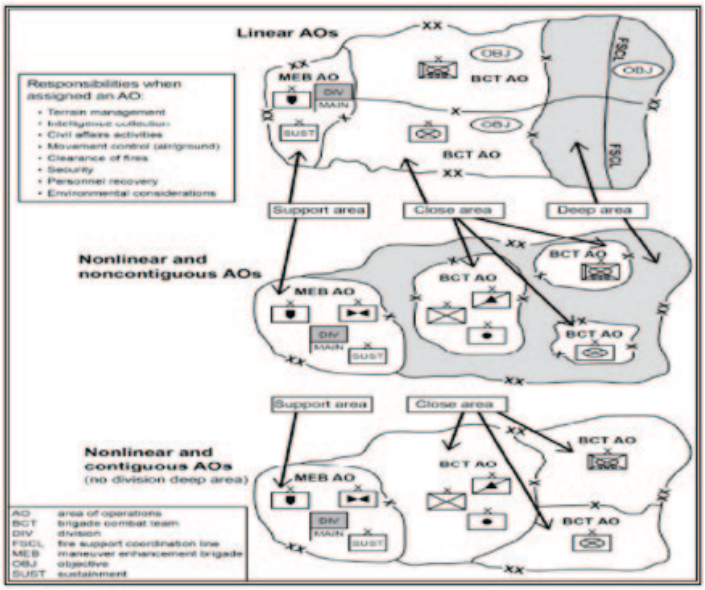


Figure 1. Example of Deep-Close-Security Operational Framework (ADRP 3-0).

Most units view their assigned area of operation (AO) in a homogenous manner resulting in little to no delineation between the deep and close fight. This view cripples the ability of IC planners to visualize the battlefield. Ultimately, without a clear understanding of the operational framework, units inevitably develop and execute an IC plan with three seams that the enemy exploits to gain a marked advantage. *Seam 1: The Battalion "Close Area."* At the battalion level, the primary friction point lies in the belief that all critical information requirements (IRs) are located within their deep area. In addition, units assume that subordinate elements will execute counter reconnaissance patrols without direct tasking. This leads to all organic IC efforts focused too far forward, to the furthest extent of the brigade's close area. Consequently, the battalion fails to both develop and task organic IC assets/capabilities to collect on close proximity named areas of interest (NAI), with a specific focus on enemy reconnaissance elements. These actions create "Seam 1" as depicted in Figure 2. The result is the enemy has complete freedom of movement around the unit's main body, with unrestricted surveillance and observation of indirect fires.

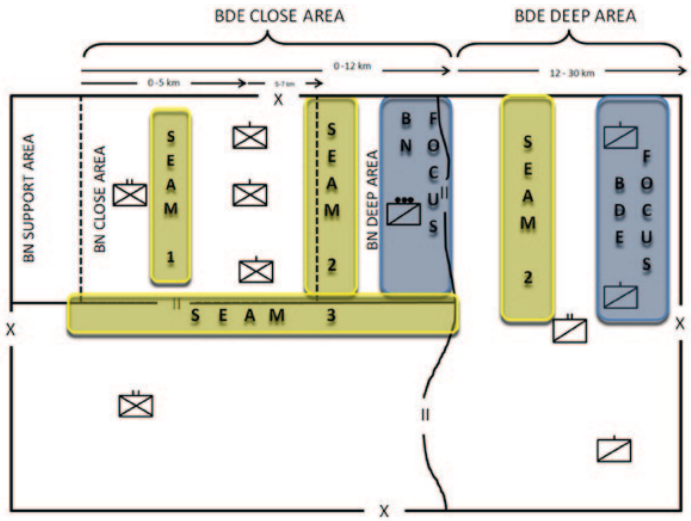


Figure 2. Brigade Linear Battlefield with Defined Deep and Close Areas.

Seam 2: The Battalion "Deep Area" vs. the Brigade "Close Area." Brigades and battalions struggle to define their individual roles and responsibilities for collection between their respective close and deep areas. This is the basis for Seam 2 depicted in Figure 2. Battalion and brigade operations and intelligence personnel rarely synchronize IC efforts. This lack of coordination often results in a combination of three outcomes:

1. Duplicated efforts. Brigade and battalion establish NAIs and task organic elements to collect information at the same geographic location. Often this is represented by a battalion tasking organic reconnaissance assets to observe the same area that brigade is covering with an aerial IC platform.
2. Echelon prioritization. IC overlays are developed and executed at both the brigade and battalion level without discussion, understanding, or rehearsals. Consequently, neither echelon comprehends the prioritization of NAIs, but merely assumes that templated NAIs will receive coverage. Unfortunately, rarely does NAI prioritization at the brigade and battalion match. As a result the brigade does not collect on a critical (event driven) NAI from the battalion perspective.
3. The deep focus. Units tend to position their reconnaissance assets to the furthest extent of their deep area. Additionally, units do not have sufficient reconnaissance efforts to cover in both width and depth. The result is Seam 2, a gap in coverage between the rearmost elements of the unit's reconnaissance effort and the forward edge of the unit's main body. Depending on the depth, it may constitute a gap in both time and space. For example, an enemy echelon may pass through deep brigade or echelon above brigade reconnaissance assets and, because it is not handed off to battalion scouts or other assets, it essentially disappears in the seam and is not observed again until it arrives in the battalion's forward edge of the battle area hours later. Worse, the enemy may appear again only in our rear or flanks (Seam 1), having taken advantage of the third seam.

Seam 3: Adjacent Unit Coordination. Successful operations include adjacent unit coordination. IC planning is no different. Units often state the need to synchronize their movements, fire plans, and sustainment requirements but rarely share CCIR, IC overlays, or current enemy assessments. Instead, they rely on their higher headquarters and digital platforms like Blue Force Tracker, Command Post of the Future, and the Distributed Common Ground System-A to create common understanding. Absent from the process is direct verbal or face-to-face interaction. Most intelligence sections routinely fail to establish effective primary, alternate, contingency, and emergency communications plans leaving each subordinate organization operating as an isolated unit. This issue is amplified when working within multinational task forces that operate on varying mission command and communications systems as witnessed at JMRC. This lack of direct synchronization creates Seam 3 which runs parallel along unit boundaries. The enemy anticipates this failure, seeks to identify the seam, and then exploits it by committing its main attack on this axis.

The Nonlinear Environment

Defining the operational framework within a nonlinear environment is conceptually much harder for most organizations. The frustration is often multiplied as the brigade and battalion focus of reconnaissance is overlaid over most of the same terrain. As depicted in Figure 3, it becomes clear how multiple aerial assets become layered within the same geographic footprint.

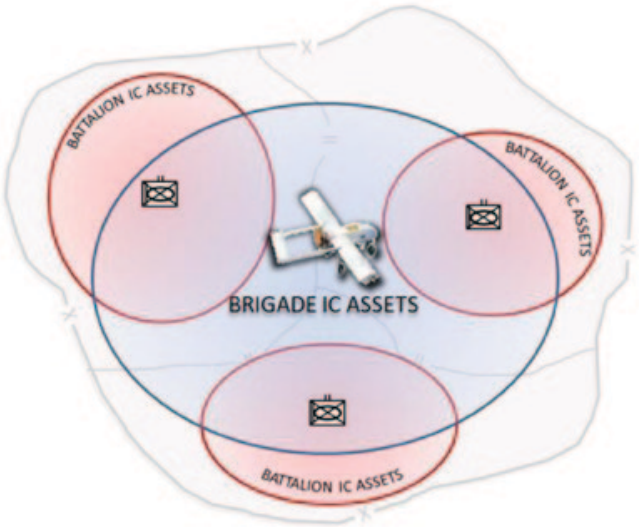


Figure 3. Brigade and Battalion IC assets within a nonlinear framework.

The Army's experiences during Operations Enduring Freedom and Iraqi Freedom (OEF/OIF) are mostly built on a nonlinear operational framework. This nonlinear and static environment forced units to use IC assets to look internally on their AO. This enabled subordinate units to first accept, and second expect, an abundance of nonorganic aerial IC platforms. Indirectly, this led to brigade assets collecting on multiple battalion and brigade NAIs from the same airspace at near-simultaneous time.

These experiences built a perception that IC platforms could answer multiple IRs within multiple areas during a single flight with minimal coordination. This caused a paradigm shift toward a substantial decrease in IC tasks directed at organic maneuver elements to include battalion scouts. The Army has yet to transition back toward recognizing the finite aerial resources and their placement in the brigade and battalion reconnaissance efforts.

Ultimately, the Army will continue to fight wars in both a linear and nonlinear operational framework. Each provides opportunities and limitations. Units must recognize how these frameworks affect their tasking of IC platforms.

Problem Set 2: IC Overlay Inadequacies

"The tasking and directing of information collection assets is fundamentally linked to the development of the IC overlay."[3] In DATE, intelligence sections routinely produce IC overlays that are not tied to satisfying CCIR, convoluted and lack focus, and not phased over time.

The foundation of an effective IC plan starts with a coordinated effort between the staff and commander to develop CCIR. Establishing priority intelligence requirements (PIRs) allows the collection manager to focus efforts on finding information that will ultimately drive a decision. However, commanders rarely take ownership of this process, resulting in the adoption of a higher echelon's CCIR or intelligence officers (S2) creating their own. The residual effect is felt in the IC overlay as NAIs are chosen based on terrain analysis and templated enemy locations rather than critical events that drive decisions.

An efficient IC overlay is clear, concise, and easily understood. In most rotations units struggle to adhere to these principles. The most identifiable shortcoming is the inability to delineate IC overlays between echelons. Often these products have countless NAIs that lack a specific focus, exceed IC collection capabilities, and are not tied to the specific units plan (brigade NAIs on a battalion IC overlay). In plain sense, the entire AO becomes an NAI. Consequently, units are overwhelmed and do not prioritize resulting in a failure to task collection assets on critical NAIs.

The initial IC overlay developed to support an operation needs to adapt as conditions change. However, units fail to develop IC overlays that are phased over time as their operational focus changes (defense, offense, wide area security). The common practice involves the application of NAIs across the depth of the AO based off assumptions from initial mission analysis. This results in units creating "enduring" or "legacy" NAIs with the belief that their relevance is applicable to all phases of the operation. Ultimately, if the IC plan is not updated, it is no longer relevant after the first day of the operation.

Problem Set 3: Missed Opportunities with Organic and Multinational Capabilities

Units often fail to effectively utilize their organic IC assets. This is predicated on deployed experiences which have conditioned units to use aerial platforms rather than ground elements. Indirectly, operations officers are focused with planning and lose sight how and to whom specific IRs were tasked.

Organizations often have a myriad of units with specific capabilities that have been attached or reside within their organic footprint that could support the reconnaissance effort. These elements range from Air Force Joint Tactical Air Controllers (JTAC) to forward observers to the basic Infantryman. Each of these carries its own capabilities that

can be applied to specific IRs within the IC Synchronization Matrix. What units often fail to realize is that more than one unit is capable of answering CCIR. More importantly, we fail to disseminate CCIR effectively and efficiently to those myriad assets that could provide the answers. A common example often observed at JMRC is described below.

The battalion S2 develops a specific information requirement with an accompanying indicator of 3 or more BMPs traveling through a mobility corridor within a valley. This information will answer a PIR that determines what avenue of approach the enemy main body will use for its attack. In addition, the PIR will also drive a decision by the battalion commander in regards to his counter attack plan. In the execution of the battalion IC plan, this PIR is often tasked to the forward most element–the battalion scouts.

In most circumstances, Air Force JTACs are employed within the battalion scout element in an effort to streamline the prosecution of targets through type I or type II close air support (CAS) control during force-on-force engagements. The attached JTACs are very capable of answering this same mission critical PIR. However, rarely are the JTACs tasked to collect on, or are aware of, the unit's PIRs. This lack of awareness results in JTACs that do not understand the battalion's critical IRs. Information gathered is ultimately conveyed as a situation report (SITREP) rather than an answered PIR. This method relies on the training of the radiotelephone operator's to extract relevant information and inform unit leadership.

Another significant oversight is the incorporation of multinational partners. Often units arrive at JMRC with a predisposed list of limitations for their multinational partners. U.S. units must not focus on their multinational partners' constraints but rather their capabilities. An example of this is when U.S. units focus on their multinational partners' limited night vision devices, which hamper movement at night, as an excuse to relegate their role to insignificant tasks. Instead leaders should consider how to leverage their counterpart's strengths wherein they are viewed as contributors rather than inhibitors.

Lastly, units rarely establish a system that efficiently utilizes the individual Soldier as an IC asset. CCIR is only known by leaders with the expectation that they will receive reports from subordinates, decipher the information, and transmit the appropriate answer to designated PIRs. In practice leaders rarely have the capability to track all of the PIRs and filter reports from subordinates to answer them. Soldiers that understand PIR can become the filters and report answers rather than SITREPS. This will prevent excess traffic on the radio and enable company leadership to focus where required.

Problem Set 4: Asset Prioritization and Retasking

Leaders continue to rely on their counterinsurgency experiences as the Army transitions to DATE scenarios at JMRC. Most previously deployed leaders have a shared experience relating IC assets to a false sense of ownership or tasking ability. This understanding is built upon the surplus of theater IC assets that were present during OIF and OEF. Contingent to this experience is the execution of most immediate reconnaissance operations by "pulling" IC assets rather than using organic elements. Pulling IC assets was accomplished by applying the immediate CAS request to IC platforms–establishing the immediate IC request. Inevitably units had success at receiving support for scantily planned reconnaissance efforts due to an abundance of IC assets.

The net result of this process was subordinate units that do not develop a distinct, focused IC plan utilizing organic IC assets. Additionally, units lack the ability to forecast and request higher level capabilities to satisfy IRs that cannot be met using organic platforms. JMRC observers/controllers/trainers (O/C/Ts) have observed units that plan under the assumption that if they find a brigade priority target they will receive higher level organic asset(s) (Shadow) to continue to develop the intelligence. Ultimately they believe, "If we find it, they will come."

The failure of headquarters units to provide the required prioritization and oversight for IC is the reverse result to the immediate IC request. Just as a battalion was able to "pull assets," brigade now had the means to re-task. This ability has a detrimental impact to the development of the IC Synchronization Matrix. Organizations no longer feel the need to designate assets by time to prioritized NAIs. IC fundamentals such as cueing, mixing, and redundancy are not incorporated into asset management. Instead the IC Synch Matrix resembles more of an asset request template due to the fact that allocated platforms rarely collect on the NAIs in which they were requested. These assets are almost always re-tasked as soon as they arrive on station.

Ultimately units must understand that assets, to include IC platforms, are a finite resource. Battalions and brigades must clearly prioritize NAIs that satisfy CCIR. The dissemination of prioritization, both higher and lower, is vital to preventing IC assets from being "re-tasked." An absence of prioritization prior to the fight will continue to increase higher units' appetites to "pull" IC platforms to fill immediate needs as they arise during the fight.

Problem Set 5: The Need for Staff Collaboration

"The operations officer, based on recommendations from the operations staff, tasks and directs the information col-

lection assets."[4] The concept that IC is a collaborative process involving the entire staff is codified in doctrine and should be accepted by all leaders. However, most battalions continue to struggle with the practical application of cohesive IC development leaving the battalion S2 as the sole proprietor of the task. The compounding effects of this decision result in the absence of NAI prioritization in accordance with the ground maneuver plan, limited organizational understanding of the IRs tied to each NAI and, most importantly, subordinate organizations that are not specifically tasked to collect on critical NAIs that drive operational decisions by the battalion commander.

Conclusion

The phrase "intelligence drives operations" is commonly accepted throughout the Army. Information collection is critical in making this phrase a reality. Throughout this article we have identified five major shortcomings that prevent organizations from internalizing this mantra. Leaders need to acknowledge these common pitfalls to drive unit tailored solutions. The success of the mission depends on it.

Endnotes

1. ADRP 3-0 Unified Land Operations, 19.

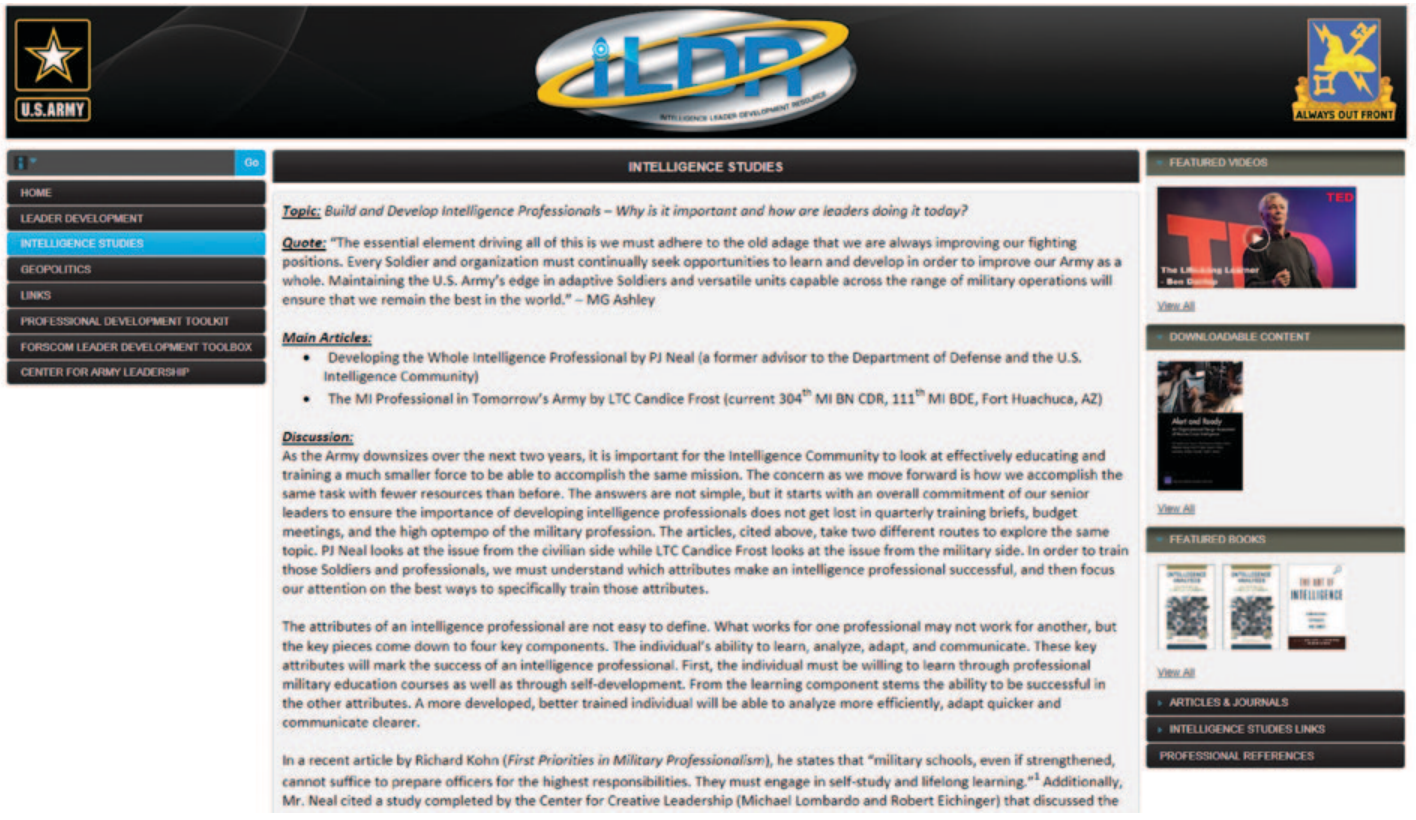
2. Ibid., 20.

3. FM 3-55, Information Collection, 39-42.

4. Ibid., 1-2.

CPT Kuderka is currently an MI Captains Career Course instructor at Fort Huachuca, Arizona. His past duty assignments include Intelligence O/C/T at JMRC, MICO Commander, 3/1 Brigade Special Troops Battalion, 1st Infantry Division, Fort Knox, Kentucky; Battalion AS2, 1st Ranger Battalion, Hunter Army Air Field, Georgia; and Battalion IC Coordinator, 2-27 Infantry Regiment, 3rd Infantry BCT, 25th Infantry Division, Schofield Barracks, Hawaii. His military education includes North Atlantic Treaty Organization Staff Officer Course, MI Captains Career Course, and MI Basic Officer Leadership Course. CPT Kuderka holds a BA in Criminal Justice from The Citadel.

CPT Eickbush is an O/C/T with JMRC. His past duty assignments include Commander, Headquarters and Headquarters Battery, 4-25 Field Artillery, 3/10th Mountain, Fort Drum, New York and AS3, 4-25th Field Artillery. His military education includes NATO 101, Joint Firepower Course, Field Artillery Captains Career Course and Field Artillery Basic Officer Leadership Course. CPT Eickbush holds a BS in Industrial Engineering from the South Dakota School of Mines and Technology.



BCT Multifunctional Teams in a DATE Exercise

by First Lieutenant Lauren Kobor and Chief Warrant Officer Two Dane Rosenkrans

Bottom Line up Front: A brigade multifunctional team (MFT) platoon must continue to provide tactical Signals Intelligence (SIGINT) and Human Intelligence (HUMINT) operations with the option of time-sensitive MFT exploitation as missions dictate. The key to successful collection operations, however, is the ability to communicate from the team level directly to the battalion and brigade S2 shop.

Introduction

In September 2014, the Military Intelligence Company (MICO), 3rd Infantry (Light) Brigade Combat Team, 25th Infantry Division (3-25 IBCT), received hard news–make a new "Multifunctional Platoon." With a few PowerPoint slides, our manning structure changed and our entire platoon mission became a giant question mark. At the time, our understanding of the MFT concept was that of the rank- and experience-heavy targeting and rapid exploitation teams of Afghanistan. How were we going to balance the traditional collection needs of a light infantry brigade with the time-sensitive targeting capability of the Afghanistan MFTs? This is an account of where we came from, the decisions we made, and the implementation of our newly refined capabilities in Decisive Action Training Environment (DATE) exercises.

Transition

Prior to September 2014, our HUMINT and SIGINT Soldiers were in two different platoons: the Intelligence, Surveillance, and Reconnaissance Platoon, with All-Source and geospatial intelligence analysts, and the Major Systems Ground Platoon (tactical SIGINT Platoon), with linguists and SIGINT analysts. With a cancelled deployment, the Brigade had been conducting emergency deployment readiness exercises and command post exercises (CPX), leaving few opportunities for HUMINT and SIGINT to work together in a field environment. And then we were hit, like every other BCT, with the MFT manning change. We looked at each other and quickly realized that nobody had the answers.

So we got book smart, reading the MFT Team Leader's handbook, Draft ATP 2-19.5, as well as multiple tactical standard operating procedures and capabilities briefs from the battlefield surveillance brigades. But all of this led to one conclusion: MFT was not right for this light infantry brigade. This problem was exacerbated by the need to keep ourselves ready for any near-peer threat that might arise in the U.S. Pacific Command area. If all of our collectors were to be assigned to three MFT squads, we saw the new mission as stripping us of our core capabilities–low level voice intercept (LLVI), Prophet Enhanced, and HUMINT Collection Team (HCT) operations–and forcing us to exclusively conduct time sensitive targeting and site exploitation. We kept trying to fit what we saw as a square peg into a circular hole.

After exhausting our efforts, we reached out to the MI Warrant Officer Proponent for answers. She explained:

> ***"The only thing that has remained constant throughout the history of this (35M) MOS is that HUMINT conducts HUMINT. The size, shape, and rank configuration of the teams have constantly evolved. Call the team Bob or Jim or MFT or GHOST or whatever, the mission of the trained and certified HUMINT collector on the team is still to conduct interrogations, full-spectrum military source operations, and support to document and media exploitation."***

She explained from the HUMINT side how we came from IPWs to tactical HUMINT teams to HCTs and now, the next step in our evolution, an MFT. Our ability to conduct tactical, time-sensitive exploitation did not replace our HCT and LLVI capabilities, but *added* to them.

Training

With this understanding, we laid out our training glide path to be ready for the Joint Readiness Training Center (JRTC) in May 2015. However, manning issues quickly surfaced. Between advanced schooling, professional military education, leave, projected moves, borrowed military manpower, physical profiles, company responsibilities, and taskings from outside the company, we were barely able to man two 5 to 6 person MFTs. This was continuously one of our greatest challenges. Ultimately, we decided that every Soldier and every noncommissioned officer needed to be trained to fall into multiple team configurations as missions dictated. We compensated for diminished team continuity with mission flexibility.

For our first major training event, we conducted an MFT squad validation. In October, we spent a week in the field covering the crawl and walk phases for two MFTs. During this validation, we (legally) cross-trained MOS 35Ms to use the AR8200 police scanner and understand the fundamentals of direction finding. We trained the MOS 35Ps (Cryptologic Linguists) to conduct tactical questioning and to understand the fundamentals of Military Source Operations (MSO). Finally, we trained all MFT Soldiers on field expedient document exploitation and tactical site exploitation (TSE), having received a Site Exploitation class from a mobile training team several weeks prior. The exercise culmi-

nated in both MFTs attaching to an infantry platoon during a platoon raid. The infantry platoon secured the site and gave the MFT leaders a time limit, during which the MFTs had to complete TSE, a direction-finding mission, and a battlefield interrogation. After action reports with the infantry platoon showed that we had come a long way, but still had a long road ahead.

After evaluating our capabilities, we got on the calendars for each of the maneuver units and briefed their staffs and company/troop commanders on our new capabilities. In hindsight, we oversold our capabilities, especially with regard to signal terminal guidance–we did not have the proper equipment. We also would have curbed the language to move away from multifunction "teams" and towards multifunction "capabilities." We did not properly manage the expectations of the maneuver units, which would hurt us down the road when battalions would ambiguously request "MFT," when what they really needed was "LLVI" or "HUMINT screening ops."

After our validation, we seized several more opportunities to exercise our skills. We injected HUMINT, SIGINT, and TSE training objectives into infantry field training exercises. Working with the battalion S2s allowed us to add depth to training without derailing the maneuver element's training objectives; and second, allowed us to build relationships with the battalions that would work to our collective advantage during Brigade level exercises.

Decisive Action and JRTC

Our training validation occurred in two Brigade exercises: the 25th ID-led Brigade Evaluation Exercise Lightning Forge in Hawaii and the May 2015 Decisive Action rotation at JRTC. We were then able to test the Operational Management Team (OMT) and Cryptologic Support Element (CSE) as management teams for HCT and SIGINT operations while also working within the Brigade S2, and focus on influencing Brigade operations with our single-source reporting. Our greatest takeaways were the following: get teams to the (right) battalions as quickly as possible during staging; ruthlessly demand a daily or twice-daily activity report directly between the teams and the Platoon leadership (in addition to the tactical intelligence reporting chain); ensure that the teams have a robust and effective PACE (communications) plan directly to the OMT or CSE and, as implied, that every Soldier knows how to use all available communications equipment.

The preparation phase proved to be the most critical and most time consuming for the MFT Platoon as a platoon. We had to be a full planning cycle ahead of the Brigade. With Platoon leadership participating directly in the Brigade military decision making process (MDMP), we initiated each exercise with HCTs and LLVI teams attached to maneuver battalions as necessary. We pushed hard to be the first on the ground for preparation. An advance team of MOS 35T MI System Maintainer/Integrators and Prophet Enhanced operators were the first in the Brigade to occupy the initial staging area. Arriving and preparing early allowed us to attach our teams to their supported units as the battalions were conducting MDMP and troop leading procedures, meaning that our team leaders were intimately involved in company-level planning.

Platoon leadership balanced receiving equipment and preparing the teams, participating in Brigade MDMP and all supported battalion MDMP timelines. The Platoon Leader and warrant officers conducted in-person coordination at every supported battalion. The Platoon Leader attempted to attend every supported battalion operations order with the team leaders. While we were adept at communicating with the battalion S2s, we would later find that a good working relationship, or lack thereof, with the battalion S3s had significant impact on the effectiveness of our collection teams.

We should have done a better job preparing the team leaders on how to ingest information at a battalion operations order and what personnel to seek out within a maneuver battalion staff. We also needed to bolster the confidence in our young team leaders to approach the right people (an infantry major executive officer is not used to seeing a specialist contact him as a direct support enabler). Our teams were most successful when given a direct line to the Company Commander and First Sergeant with whom they would be attached, no matter the rank of the team leader. The least successful teams found themselves as just one in the mix of enabler teams in a headquarters company with no tactical contacts. The assistant intelligence officer was not the appropriate tactical chain of contact for a collection team. While familiar with the intelligence requirements, staff officers will not be intimately familiar with company operations and communication. Overall, participating directly in Brigade and battalion MDMP cycles as early as possible, getting ahead of the battalion planning process, and physically placing the teams with their supported units with a clear tactical chain of command were critical to initiating operations successfully.

For the exercise rotations, our teams operated in approximately 72-hour cycles of Joint Forcible Entry (JFE), to include defense and offense with sprinklings of stability, noncombatant evacuation, and counterinsurgency opera-

tions. Throughout both exercises, our teams remained in HCTs, LLVI teams, and Prophet Enhanced teams. For one mission, we combined an HCT and an LLVI team as an MFT for a time-sensitive high value individual capture/kill raid. While we were prepared to morph our SIGINT teams between LLVI and Prophet Enhanced teams, we never needed to do so. For the JFE, we divided HCTs, LLVI teams, and Prophet Enhanced Mobile teams among the battalions according to mission sets, meaning that one battalion received three collection teams while others received none. We attempted to keep all teams mounted in vehicles for maneuverability, equipment management, and access to communications, but several teams did participate in a battalion air assault infiltration. Throughout operations, while prepared to switch teams and team composition around as necessary (flexibility was the name of our game), the teams maintained their original collection missions throughout, even if the supported unit, battlespace, or specific mission changed. We never changed an LLVI team into a Prophet team, or an HCT into an MFT.

During the defense, LLVI teams focused on screening operations and providing tippers and threat warnings to ground commanders, while HCTs conducted tactical questioning, screenings and MSO, especially at refugee camps and population centers. During the offense, we attempted to co-locate two LLVI teams for targeting operations, but a breakdown in communication between Brigade and battalions kept the teams in separate screening missions. HCTs, however, focused more on MSO and interrogations at the detainee holding area (DHA) as time passed and the kinetic fight intensified. We also pushed a Prophet Mobile team to a battalion tactical operations center (TOC), and then with the Brigade forward TOC (TAC) as the forward-line-of-troops moved rapidly forward. Our final battlefield array had our two LLVI teams with the cavalry scouts, a Prophet Mobile with the Brigade TAC, a Prophet Dismount at the Brigade TOC, and HCTs at the main urban center, the DHA, and the Brigade TOC.

During operations, the Platoon headquarters element staged at the MICO Post directly outside of the Brigade S2 cell at the Brigade TOC. The Platoon Leader coordinated with the Brigade Collection Manager and S2 Plans to build the missions of the collection teams for each phase, assisted in writing Annex L, Information Collection, for each order, and coordinated with the MICO Commander, who was working with the S3 Plans. The Platoon Sergeant worked with the MICO First Sergeant and Executive Officer at the Brigade TOC to facilitate equipment readiness and manning cycles. This was an especially important role to the company as the Collection Platoon Sergeant took more of a technical role in the S2 shop. The warrant officers assumed their critical roles within the OMT and CSE while still coordinating with the Brigade Collection Manager and Platoon Leader to push daily Collection Emphasis messages to the teams based on mission planning. Additionally, each team was required to submit a Daily Activity Report (DAR) directly to the Platoon chain-of-command outside of any technical or intelligence reporting.

The DAR, a digital or 5-line radio report, served several functions:

- It established and maintained a communications link between the MICO and the teams.
- It allowed the Platoon leadership to track location, readiness, maintenance, etc.
- It allowed the Platoon leadership to assess if the teams were being properly and effectively used at the ground level.

This allowed the MICO to ensure that no one fell through the cracks and provided feedback for the next cycle of mission planning. If the teams and Platoon could not communicate directly, then we would go through the battalions. While the Platoon headquarters did not spend significant time doing battlefield circulation, their centralization contributed to in-depth planning and an emphasis on integration in the Brigade intelligence cycle.

Lessons Learned

The most valuable lesson we learned from these exercises was the need to be experts in communication. So many different factors impeded our ability to communicate with the teams forward and the Brigade elements in the rear. We quickly identified that the use of Joint Capabilities Release-Blue Force Tracker was critical to mission success. The most important task of an intelligence collector, according to our observer/coach/trainer (O/C/T), was to report. An inability to communicate is an inability to report.

Over the better part of 2014-2015, we have been training, evaluating, and learning. We have boiled our experiences down to four key lessons:

1. *Clearly communicate the capabilities of BCT organic collection to battalion and Brigade commanders and staff.* First and foremost, the level of understanding with regards to the MFT Platoon needs to be increased and maintained. This is a struggle. There are so many misconceptions about what we can provide. We should have provided a menu of capabilities (LLVI, SIGINT collection, MSO, screening, interrogations), as opposed to teams (one MFT please) to the

maneuver elements. Then, MICO, S2, and S3 leadership could determine the size and configuration of the teams. It is also important that the key staff players understand this as well. The Brigade and battalion S3s shops are often overlooked in this process, despite the fact that they play the most important role in task organization. The MICO Commander, S2 Plans, and Collection Manager also need to be well versed in MFT capabilities.

2. *MFT Platoon leadership (PL, PSG, Warrant Officers, NCOICs) are involved in Brigade MDMP*. We need to play an active role in MDMP. On Brigade staff, the OMT/S2X and CSE need to inject their input after mission analysis and before the task org is set. The single-source subject matter experts should be drafting the language that appears in the Brigade operations order with respect to HUMINT/SIGINT. Task, purpose, command and support relationships, sustainability, transportation, security, and specific intelligence requirements should be dictated in the operations order. Also, the maneuver elements need to understand the difference between general and direct support relationships. It does not matter what appears in an operations order if nobody else understands what it actually means.

3. *Balance training in MOS and MFT skill sets.* Training needs to be balanced. This is extremely difficult, and every unit will have to find their own way to get it done. Our goal over a calendar year is to conduct one MFT exercise, three HUMINT and three SIGINT exercises, and provide support (either HUMINT/SIGINT or multifunction) to each maneuver company. And, of course, this needs to be balanced with professional military education, language requirements, advanced schooling, battalion/brigade taskings, CPXs, Red Cycles, etc., for the individual Soldiers and NCOs.

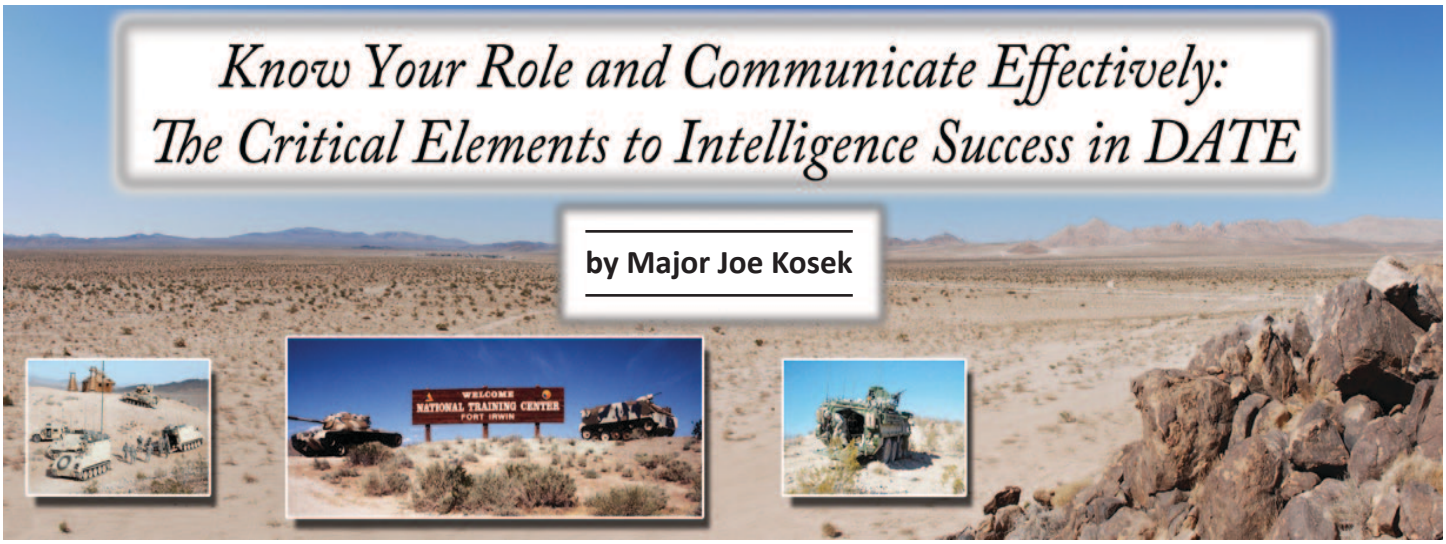
4. *Eight individual sets of communications equipment for eight individual team elements.* Finally, and we think most importantly, a realistic, flexible PACE plan needs to be established between the teams and the Platoon at Brigade. This cannot be overstated. Failure to do so will end in mission failure. Every single member of the multifunctional Platoon needs to have the communication skills of an infantry radiotelephone operator and the technical skills of an MOS 25-series Soldier. It needs to be reinforced in every training exercise that is conducted. We, as a profession, have failed to maintain these skills. During JRTC, the O/C/Ts told us that if we could tell them "in the first 72 hours of the fight who on [our] teams was dead or alive, that is a success." Surely we should not have such low expectations. We trained consistently on our PACE plan and were even supplemented with more communication channels during JRTC, but we were still only able to speak to our teams an average of once a day. The bottom line is that as long as someone at Brigade (PL/PSG, OMT, CSE) can talk to the teams, all other problems can be fixed.

Conclusion

In conclusion, although a difficult transition from separate SIGINT and HUMINT sections into a Multifunctional Platoon, we were able to focus on tactical intelligence collection operations as opposed to only analytical operations inside of a TOC. We trained in a way that made each Soldier familiar with several collection skill sets–HUMINT, SIGINT, and TSE. We offered capabilities to our Brigade and maneuver battalion leaders and maintained the flexibility to fill a variety of mission requirements. We culminated our year as one of the first BCT Multifunctional Platoons to execute a Decisive Action rotation at a combat training center. Flexibility and communication, both staff and tactical, were key. What we sacrificed in depth of MOS training, we gained in adaptability on the battlefield.

1LT Kobor served as the Platoon Leader for the MFT Platoon, Delta Co, 29th BEB, 3rd IBCT, 25th ID, from June 2014 to August 2015, including JRTC rotation 15-07. She is currently attending the MI Captains Career Course with a following assignment to 3rd ABCT, 1st Cavalry Division. She graduated with honors from the U.S. Military Academy in 2012 with a BS in International Relations.

CW2 Rosenkrans served as the sole HUMINT Technician for 3rd IBCT, 25th ID, during JRTC rotation 15-07 and is currently assigned to A Co, 202nd MI Battalion, 513th MI Brigade in Fort Gordon, Georgia. He earned an Associate of Applied Science Degree in Intelligence Operations in 2009, and is a graduate of various HUMINT schools, to include Source Operations Course, Defense Strategic Debriefer Course, and Operational Management (G/J2X) Course.



Know Your Role and Communicate Effectively: The Critical Elements to Intelligence Success in DATE

by Major Joe Kosek

Introduction

The National Training Center (NTC) at Fort Irwin, California is the premier training center for Army brigade combat teams (BCTs) to practice executing unified land operations (ULO) in preparation for real world missions. No other combined arms training center has the economic resources and maneuver space available to allow a BCT to simultaneously practice its ULO core competencies of combined arms maneuver and wide area security while significantly dispersed over complex terrain, fighting a near-peer, thinking enemy with the ability to illustrate what occurs over the course of a mock battle using instrumentation.

In preparing BCTs to execute ULO, the NTC also prepares BCT Intelligence (S2) Sections and Military Intelligence (MI) Companies (MICOs) to execute tactical-level intelligence operations in support of the BCT. The NTC began focusing on conducting ULO in the Decisive Action Training Environment (DATE) in March 2012.[1] Despite four years of practicing ULO in the DATE, BCT S2 sections and MICOs continue to struggle when they come to the NTC. With a multi-year repository of rotational after action reviews (AARs) at their disposal and the ability to implement lessons learned during home station training, why do BCT S2s and MICOs experience significant challenges during DATE rotations at the NTC, and what can be done to reverse this trend?

The BCT Intelligence Enterprise Structure

There are three primary reasons why BCT S2 sections and MICOs struggle at the NTC. First, intelligence analysts across the entirety of the intelligence enterprise of the BCT, also referred to as the Intelligence Warfighting Function (IWfF), do not understand their duties and responsibilities, to include reporting requirements and deliverables. Second, BCT S2s and MICO Commanders (CDRs) do not design and validate a communications plan that facilitates consistent communication across the IWfF prior to their rotation, resulting in significant communication challenges during the rotation. Finally, as a consequence of not understanding duties and responsibilities and not being able to communicate effectively, the IWfF is unable to generate and maintain a common intelligence picture (CIP), or the intelligence portion of the common operational picture (COP) at echelon.[2]

The lack of a CIP typically results in the BCT CDR and subordinate commanders not having a shared understanding of where the enemy is located on the battlefield. The enemy, who possesses a thorough understanding of the terrain through home-field advantage along with a developed and rehearsed communications plan, does not experience the same loss of situational awareness. Not knowing where the enemy is coming from and when they are coming typically results in the BCT sustaining a staggering number of combat losses against a numerically inferior force. The question that remains is: What can be done to counter each of these contributing factors to poor performance across the IWfF and improve NTC rotational performance?

To understand why intelligence analysts do not understand their duties and responsibilities along with their reporting requirements, one must first understand the structure of the IWfF in the BCT. The number and type of intelligence personnel in a BCT stems from the unit's modified table of organization and equipment (MTOE). Based upon the typical BCT MTOE, the highest concentration of all-source intelligence analysts reside in two areas: the BCT S2 Section and the MICO Analysis Platoon.[3] In a deployed environment, these two entities typically merge together to form the Brigade Intelligence Support Element (BISE).[4]

However, in the garrison environment, the Analysis Platoon is owned by the MICO, which falls under the Brigade Engineer Battalion (BEB) and reports to the BEB CDR. The

BCT S2 Section, which comprises the other portion of the BISE, is owned by the BCT S2 and reports directly to the BCT CDR. Thus, the BCT MTOE facilitates a condition in which the two sections that represent the principle element for all source analysis and production in the BCT do not work together on a day to day basis in the garrison environment.[5]

ATP 2-19.4 acknowledges this deficiency by stating that the relationship between the S2, the MICO, and other staff is critical because "in garrison these individuals seldom interact, yet in a tactical environment, they must collaborate on matters concerning intelligence support to BCT operations."[6] Typically, only when the BCT CDR organizes staff elements in command post cells by warfighting function will the BCT S2 Section and the Analysis Platoon come together to form the BISE.[7] Because the BCT S2 Section and the Analysis Platoon do not have a habitual working relationship in garrison, intelligence analysts from these two entities do not understand their duties and responsibilities within the BISE. When faced with a situation where analysts do not know what to do, they should first turn to current doctrine to find a solution to the problem.

Intelligence Doctrine Baselines

Fundamental Army Intelligence doctrine, such as FM 2-0 Intelligence Operations and ATP 2-19.4 Brigade Combat Team Intelligence Techniques outline the general functions of the BISE and overall duties and responsibilities of key leaders of the IWfF, such as the BCT S2, BISE Chief, and the MICO CDR. While these manuals provide the general blueprint for developing the BCT intelligence architecture, they do not go into significant detail on the art of executing intelligence operations at the BCT level and below. Therefore, only by establishing habitual working relationships and conducting routine, simulated intelligence training events can BISE analysts and other intelligence analysts across the BCT develop an understanding of how they contribute to the larger BCT intelligence picture.

Additionally, analysts do not understand their reporting requirements and deliverables because there is no textbook answer–reporting requirements and deliverables vary from unit to unit depending on the needs of both the BCT CDR and the higher headquarters. Thus, the critical takeaway for BCT CDRs and S2s should be if intelligence analysts from different parts of the BCT do not work together habitually in garrison, they cannot be expected to review doctrine, organize quickly, and generate a detailed threat picture.

Another significant problem contributing to BCT S2 and MICO struggles is the failure to develop an effective communication plan throughout the IWfF. FM 2-0 clearly lays out that "intelligence operations must be vertically and horizontally integrated and synchronized with joint, theater, lateral, and lower echelons."[8] While the BCT S2 and MICO CDR typically understand the intelligence enablers available within the BCT and at higher echelons, they usually do not develop a detailed and redundant plan for how they will communicate with these entities. This is contrary to FM 2-0, which states that staff members must know "enablers available at their echelon, as well as those at echelons above and below, and how to request and manage those assets."[9] Because of the natural dispersion of subordinate elements and the complexity of the terrain at Fort Irwin, the NTC Intelligence Observer/Coach/Trainers typically recommend that units develop a primary, alternate, contingency, and emergency (PACE) communication plan with each unit or enabler.

BCT S2 sections and MICOs typically arrive at the NTC with a planned, but un-validated PACE communication plan. By not validating the IWfF PACE communication plan over a significant distance prior to coming to the NTC, units quickly discover upon arrival that their communication plan will not work as designed. An ineffective IWfF PACE communication plan contributes to both intelligence enablers not being able to pass critical information to the BCT S2 section and the BCT S2 section not being able to convey critical intelligence to all subordinate elements quickly. This ultimately leads to the BCT S2's inability to generate and maintain a CIP across the BCT. However, the question still remains: What can a BCT S2 or MICO CDR do to overcome these challenges at home station to prepare for a successful NTC DATE rotation?

Home Station Preparation

First, the BCT S2 should seek to flatten the network, streamline reporting channels, and establish a habitual working relationship among critical intelligence personnel in the garrison environment. Typically, this is accomplished by creating a memorandum of understanding (MOU) between the BCT S2 and the BEB CDR, which allows all-source warrant officers and other all source analysts from the MICO to report directly to, and work for, the BCT S2 in the garrison environment. BEB CDRs and MICO CDRs will undoubtedly be reluctant to agree to this relationship. Therefore, the BCT S2 must first develop a detailed training plan that clearly illustrates how these personnel will be used and what intelligence training events will take place and when. The IWfF training plan should be built in collaboration with the overall BCT training plan built by the BCT Operations Officer (S3) and approved by both the BCT and BEB CDRs. Developing a tangible plan in conjunction with the MICO CDR and reviewing the plan with the BEB CDR before seeking BCT CDR approval will go a long way toward facilitating the BEB CDR

signing an MOU and relinquishing control of these personnel on a daily basis.

Second, as part of the overall BCT training plan, the BCT S2 should develop a progressive IWfF training plan. Initial portions of the IWfF training plan will likely focus on individual training in garrison using BCT-internal intelligence noncommissioned officers, warrant officers, or Foundry personnel as the primary instructors. After completing individual-focused training, BCT S2s can move on to collective training and practical exercises using Foundry and BCT IWfF enablers to focus on sending and receiving reports, battle-tracking enablers, and maintaining a running estimate of the enemy.

BCT S2s can then build upon these exercises over time by conducting field-based practical exercises (potentially as part of a larger BCT event) focused on using MTOE equipment and enablers to practice developing the threat picture and establishing and maintaining a COP at echelon. During each exercise, intelligence leaders at every echelon should seek to codify roles and responsibilities in written intelligence standard operating procedures (SOPs). Additionally, intelligence leaders should seek to complement current doctrine by creating "job books" for each position within the IWfF. Job books should outline in great detail what is required by position to facilitate the overall success of the IWfF. Finally, BCT S2s and MICO CDRs should also attempt to codify and validate both duties and responsibilities, as well as the command-support relationships of MICO enablers task organized to maneuver task forces during BCT collective training exercises. In the event the BCT does not deploy to the NTC or another decisive action environment, BCT S2s should push to conduct an IWfF staff exercise every two months at home station to maintain proficiency.

Third, BCTs preparing to conduct operations in a decisive action environment should develop a clearly defined PACE communications plan with higher and subordinate echelons as well as organic intelligence enablers. MI Publication 2-01.2 Establishing the Intelligence Architecture, is a good reference to use when developing a PACE communications plan for the IWfF, as it shows the level of detail a BCT S2 section and MICO must think through to create a functional communications architecture. A solid PACE communications plan should include a balance of upper tactical infrastructure (TI) and lower TI communications, and it should take the BCT's MTOE into account. For example, many BCT S2 sections include tactical satellite (TACSAT) radio as part of their PACE communications plan; however, many BCT S2s do not check to ensure that the BCT actually has enough TACSAT radios and trained TACSAT radio operators on hand to make this a valid communications method.

BCT S2s must also take into account the access that subordinates have to contingency and emergency methods of communication if the BCT S2 needs to resort to those methods to communicate. For instance, many BCTs equipped with Force XXI Battle Command Brigade and Below (FBCB2)/Joint Capabilities Release (JCR) systems tend to use FBCB2/JCR as the primary means of communication for the IWfF when FM or upper TI communications are not available at the NTC. While most BCT S2s typically have their own FBCB2/JCR terminal, BCT S2s fail to understand that at subordinate echelons, battalion (BN) S2s typically do not have dedicated access to a FBCB2/JCR terminal based on the MTOE for the BN S2 section. This means that there may be significant lag time for a BN S2 to send or receive updated reporting.

Whenever possible, each element of the PACE should have a broadcast ability to enable multiple entities at echelon to communicate simultaneously. For example, FM communications allow the BCT S2 to communicate with multiple BN S2s simultaneously. Finally, the BCT S2 should attempt to validate the PACE communications plan over an extended distance at home station prior to coming to the NTC to ensure that the planned PACE will work. To be effective in the DATE, a good PACE communications plan should support echelons separated by up to 50 kilometers over complex terrain.

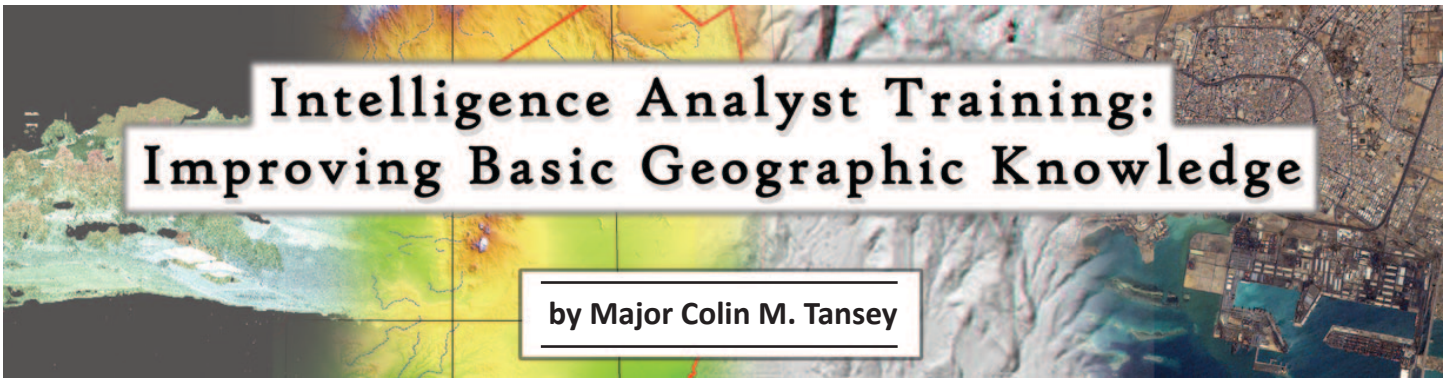
Conclusion

The job of the BCT S2 to prepare the BCT IWfF to fight and win in the DATE is an extremely complex one, which is why the BCT S2 position is widely regarded by senior intelligence officers today as the most difficult position an MI major can hold.

To quote Prussian Statesman Otto von Bismarck, "Only a fool learns from his own mistakes. The wise man learns from the mistakes of others."[10] Utilizing AARs and lessons learned from previous DATE rotations at the NTC, the wise and proactive BCT S2 will start training the IWfF early and train repetitively. First, seek to establish a habitual working relationship between critical intelligence personnel in the garrison environment. Second, using a progressive IWfF training plan, begin to clearly define duties and responsibilities for each member of the IWfF and codify these into written intelligence SOPs for the BCT. Finally, while expanding IWfF training exercises from garrison-based to field-based events, develop and validate a PACE communications plan at echelon that can overcome the tyranny of distance and support the BCT.

Implementing these lessons learned early and practicing them often will go a long way toward a successful rotation

(Continued on page 36)



Intelligence Analyst Training: Improving Basic Geographic Knowledge

by Major Colin M. Tansey

"Those who do not understand the conditions of mountains, forests, hazardous defiles, marshes and swamps, cannot conduct the march of an army."
–Sun Tzu, ca 500 BC

Introduction

Sun Tzu was right, commanders must understand the geographic conditions of the environment in which they operate. This has been understood for centuries, and as such, the U.S. Army teaches the military aspects of terrain and weather to every aspiring Military Intelligence (MI) analyst and lieutenant who enters the Intelligence Center of Excellence at Fort Huachuca. However, just learning the military aspects of terrain and weather are insufficient to provide commanders with an accurate understanding of the operational environment. I further suggest that the MI community needs to change how it teaches the importance of geography, and all that it entails, to future intelligence analysts.

Understanding geography is more than just knowing where one country is in relation to another or knowing the different classes of rocks and minerals. From a military perspective, it "concentrates on the influence of physical and cultural environments over political-military policies, plans, programs, and combat/support operations of all types in global, regional, and local contexts."[1] Some might contend that the Topographic Analysts/Terrain Teams are also geographers, but they only touch on physical geography, and not cultural geography. As we move towards a regionally aligned force structure and add climate change considerations to our operations, it is important for analysts, even down to the battalion level, to know more than just the military aspects of terrain and weather. They must know and understand the regional geography.

American Geographic Intelligence

Americans, in general, struggle with geography. In 2005-2006, the National Geographic Society commissioned a survey to evaluate the geographic knowledge of Americans. Their survey found that most young adults (ages 18 through 24) had a limited understanding of the world and lacked the basic geographic skills needed to improve their knowledge of the world around them. For instance, only 37 percent could find Iraq on a map, despite the U.S. troop presence. Approximately 20 percent thought that Sudan, Africa's largest country, was located in Asia. (How many today would even know that South Sudan seceded as an independent country in 2011?) Half of all respondents couldn't locate New York State on a map. It was not just their basic knowledge of geography that was lacking; their cultural knowledge was equally dismal with 48 percent believing that the majority of the population in India is Muslim (where approximately only 15 percent are Muslim).[2]

This trend has not improved. According to the Washington Post, a March 2014 poll of 2,066 Americans found that only 1 out of 6 could locate Ukraine on a map. Tied to this geographic illiteracy, the further away their guess was from Ukraine's actual location, the more they wanted U.S. military intervention. Interestingly enough, and possibly disturbing, military member households scored no better than non-military member households with only 16.1 percent correctly locating the country on a map. Education levels did not matter as 77 percent of college graduates failed to identify Ukraine properly.[3]

Clearly Americans have a geographic illiteracy problem and it is these same Americans who will become our future MI analysts. The only way to combat illiteracy is through education, but according to *U.S. News and World Report*, almost three-quarters of eighth graders tested below proficient on the 2014 National Assessment of Educational Progress. These results are almost identical to those from a 1994 survey. Clearly, our geographic education has not improved as only 17 states require a geography course in middle school and only 10 states require it for high school graduation.[4] Teaching analysts and MI officers just the military aspects of terrain and weather is not likely to close this geographical education gap.

In his 2013 remarks to the Brookings Institution, former Army Chief of Staff, General Raymond Odierno remarked "… you have to understand the world and its geography…Not

only the [physical] geography but then the cultural aspects, religious aspects, economic aspects, social aspects, because that all contributes to how you figure out what the right response is when you have a problem in a certain area."[5] A good analyst must have geographic knowledge that is more than a mile wide and an inch deep.

Geography and the Military

Geography is a very broad discipline. It touches upon a multitude of other disciplines as they all study the interaction between humans and the Earth. Generally speaking, geography includes the physical environment–soils, rocks, weather, clouds, topography (physical terrain), the people–culture, religion, demographics, development (cultural geography), and uses a wide array of technologies and techniques (geospatial information systems (GIS)), remote sensing, cartography) to gather, analyze, and visualize geographic data and information to understand these dynamics. Both the Engineer and MI Corps conduct terrain analysis, but only intelligence analysts are expected to understand and anticipate the effects of the physical geography (terrain and weather) on operations; understand the people, languages, and other civil characteristics (cultural geography); and create their intelligence products utilizing computers and other digital systems (GIS).

All this helps the intelligence analyst in examining, analyzing, and appreciating the physical and human landscape and its potential impacts on the mission. Knowing the military aspects of terrain and weather used to be enough, but as battalions and brigades are deploying around the world as part of the regionally aligned forces, even junior intelligence analysts must think in broader terms of geography, in military geography. This means both the physical and cultural factors and how they influence the tactics and movements of military forces. But how can they be proficient if they lack a basic understanding of geography in general?

Military history is replete with instances of geographic ignorance (willful or otherwise) leading to military defeat, none more famous or infamous than Napoleon or Nazi Germany's invasions of Russia. Harold Winter's seminal book, *Battling the Elements*, highlights the impact of weather and climate on military operations. In it, he describes Napoleon's march of the Grande Army of 600,000 into the Russia steppes during the summer of 1812 only to be forced to flee with about 20,000 survivors, most falling victim to the harsh Russian climate. In 1941/1942, that same harsh climate helped the Soviet Union to defeat the invading Germany Army. It isn't that the severity of the Eurasian climate was unknown, but it was the incorrect assumptions, of both Napoleon and Hitler, that quick victories would force Russia to surrender before the harshness of winter set in. When those expectations failed to materialize, both invaders proved inadequately prepared for the harsh winter climate. While the Russian people's grit and determination resulted in victory, the harsh climate was a key enabler. Tens of thousands fell victim to disease and the effects of the cold, brought on by a lack of proper winter equipment and gear.

At times, even the very vegetation can create environmental conditions that make military operations difficult. Vegetation covers most of the Earth's surface, with the exception of more austere environments such as the poles. As such it must be taken into consideration by intelligence analysts because it can affect mobility, counter-mobility, observation, and fields of fire. During the U.S. Civil War, the dense vegetation of the Wilderness disrupted both Union and Confederate operations. Dense forests and ground cover inhibited cavalry operations, delayed crucial troop movements, and concealed operations. Only those with intimate knowledge of the terrain were able to effectively maneuver along the often-concealed, trails, and mobility corridors. The vegetation's impact on Union forces during the first battle of the Wilderness was so great that General Hooker blamed it, not General Lee, for his inability to maneuver and eventual defeat.[6] The dense vegetation in Vietnam proved just as vexing to U.S. forces. The Vietnamese climate and biome is very different from that around Chancellorsville, Virginia, but in both cases the vegetation made military operations incredibly difficult and favored those most familiar with the environment.

These are just a few examples of why it is important to have a broad geographic knowledge. Analysts are often the only "experts" a commander has when planning at the operational or tactical level. As such, it is imperative that they have a base knowledge of geography (weather, climate, geomorphology, and culture) that enables their commanders to be successful in any environment. Since so many analysts lack this knowledge, the "so what" of terrain and weather analysis has largely disappeared from the Situation paragraph (Paragraph 1) of the Operations Order. If the elementary and secondary schools aren't teaching it, then it falls on the MI schoolhouse.

Military Intelligence Analysis and Geography

FM 6-0 Commander and Staff Organization and Operations, identifies the military aspects of terrain as: observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (OAKOC). The five military aspects of weather are: visibility, winds, precipitation, cloud cover, and temperature and humidity. Both the military as-

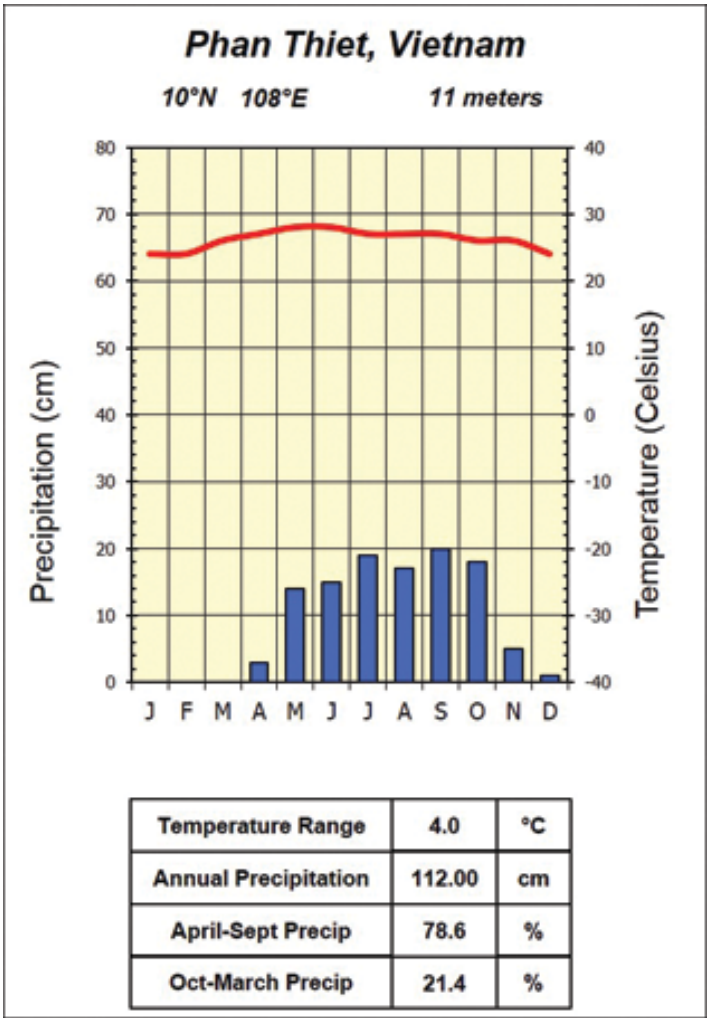
pects of terrain and weather are critical for the development of courses of action.[7] Commanders rely on the ability of their intelligence officers and analysts to understand both weather and terrain and determine their impact on friendly, neutral, and adversarial forces. But how much do they really know and why is it important?

Step 2 (Mission Analysis) of the military decision making process (MDMP) is primarily the responsibility of the unit's intelligence section (S2).[8] The S2 conducts intelligence preparation of battlefield/battlespace (IPB) with assistance from the other staff sections. This analysis includes defining the operational environment, describing the environmental effects on operations, evaluating the threat, and determining threat courses of action. This need to analyze the battlespace is exactly why the intelligence professional is the Army's geographer. Like geographers, intelligence analysts need to know "Who (or what) is where, and why."

While it may not seem like much to outsiders, the S2 is being asked to do a lot in a very limited amount of time. Everything that the S2 produces drives the follow-on steps of MDMP. That is why it is important that the S2 understands the military aspects of terrain and weather; so much is dependent on that knowledge. The problem is that most S2s, more than likely, have only a rudimentary knowledge of the military aspects of terrain and weather.

To complicate matters, in today's complex operational environments, the S2 is also expected to use analytical frameworks, such as areas, structures, capabilities, organizations, people and events (ASCOPE); sewage, water, electricity, academics, trash, medical, safety, and other considerations (SWEAT-MSO), and political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT), to analyze the geography of a particular region or place. All of these have linkages back to the basic climate, weather, geomorphology, and culture of a region. It is difficult to understand these complex interactions if one does not understand the basics of why things and people are where they are. Geography provides the larger framework in which ASCOPE, SWEAT-MSO, or PMESII-PT help guide the analytical effort.

Given the military's unique capabilities to respond to natural disasters and the establishment of regionally aligned forces it behooves MI planners to understand the natural forces, climatic and tectonic, that may influence a particular region. As resources are usually limited, especially time, it is important to focus on which environmental and physical considerations will most likely impact the operations. For example, understanding what conditions cause the summer and winter monsoons in Southeast Asia is important because the region experiences very different weather patterns depending on the time of year. Many people assume that the region always receives plenty of rainfall.



Temperature Range	4.0	°C
Annual Precipitation	112.00	cm
April-Sept Precip	78.6	%
Oct-March Precip	21.4	%

In fact, while the summer monsoons bring lots of moisture, the winter monsoon brings dry conditions and sometimes drought. Not understanding this can complicate operations in the region because it may result in units that are unprepared to deal with the extreme changes in climatic conditions. Climographs reveal a lot about the temperature and precipitation patterns in particular area. Analysts should understand how to interpret the data and be able to determine how their operations may be influenced.

The same goes for operating in mountainous regions. Mountains act as topographic barriers and affect more than just mobility. The weather and climate in mountains changes due to vertical zonation, meaning that different climates exist at different altitudes. The effect is similar to moving away from the equator and closer to the poles. Likewise, the windward side of the mountain is likely to be wetter and cooler than the leeward side due to the adiabatic warming and cooling of air as it moves over the mountain (as any-

one stationed at Fort Lewis and trained in Yakima can attest). This impact is seen quite frequently in the northern and eastern parts of Afghanistan. It also explains why the climates could vary, sometimes drastically, from one mountain valley to another.

Teaching Terrain

At Fort Huachuca, future intelligence officers are trained to "Conduct Intelligence Support to MDMP," with the intent that they can synchronize, coordinate, and produce IPB products while also integrating information collection, targeting, and intelligence analysis with ongoing and future operations. These officers are expected to identify the significant characteristics of the area of operations and area of interest based on the enemy, terrain, weather, and civil considerations. ATP 2-01.3 states that "Terrain and weather favor neither friendly nor enemy forces unless one is more familiar with–or better prepared to operate in–the physical environment."[9] This recognizes that terrain appreciation, an understanding of all aspects of terrain, is important for commanders to be successful.

The problem lies in the fact that the training in IPB focuses on broad overviews of surface features without a discussion of how they vary from one region to another. Terrain analysis in ATP 2-01.3 focuses on micro aspects of geography (OAKOC) without consideration of the broader geomorphology, climate, and biomes in the area of operations which may vary season to season. While adequate at the tactical level, this approach to physical geography does not prepare analysts for how these military aspects of terrain vary from region to region, let alone address the regional cultural concerns. It does not help prepare them to understand the complex regional geography and resultant geopolitical issues of the places they might be deployed. This is especially true when dealing with counterinsurgency. Analysts must evaluate geography as a whole, not in pieces.

Identifying avenues of approach and key terrain are important, but analysts and their commanders should understand how the geology and soils may affect operations in those avenues of approach or on the key terrain.[10] It is a very dry and technical subject, so most people do not want to study it. Yet soils and the underlying geology become important when considering cross-country mobility and trafficability. Different soils have different load-bearing capacities, traction, permeability and porosity, and stability, all of which can seriously impact the movement of personnel and materiel. Even weapon systems are impacted by soil conditions and rocks, as artillerymen learned in Vietnam. Artillery pieces sank into the wet ground when fired at or near maximum elevation causing them to malfunction.[11]

Recent experiences in Iraq and Afghanistan provide excellent examples and lessons why intelligence analysts must have a greater understanding of geography. Both countries are semi-arid deserts. This makes access to water an important concern for locals. Control of water resources, both surface and subsurface, has been a source of contention in the Middle East for centuries. The Government of Iraq and ISIS have been fighting for control of key dams across Iraq. In April 2014, ISIS forces captured the Fallujah Dam and immediately stopped the flow of the Euphrates downstream. This left towns like Karbala and Najaf without water while causing the reservoir behind the dam to overflow and flood about 500 square kilometers. Later, they reopened the dam and caused downstream flooding.[12] Thus water became a weapon of war.

In Iraq and Afghanistan, we quickly learned that drilling water wells was a quick and efficient way to "improve relations." No one thought about the second and third order effects of digging those wells. In areas where there are no large sources of surface water, groundwater becomes a key factor and remote villages and outposts often rely on local wells to provide their water. In arid and semi-arid environments, this groundwater becomes an important yet finite resource. More wells means more use and faster depletion.

Similarly, understanding the geologic structures of a region is important. Areas that have high concentrations of limestone and groundwater are likely to have large numbers of caves, sinkholes, and streams that can influence operations. Caves and depressions can hide units from most observation and significantly reduce the effectiveness of bombs and artillery. The karst topography, in and around former Yugoslavia, provided safe havens for partisans fighting the German army and provided refuge for hundreds of civilians. Mao Tse Tung sought refuge in caves following the Long March. Japanese soldiers, who used caves in the Pacific islands' hopping campaign, made the U.S. efforts to seize these areas extremely costly.[13] More recently, the Taliban used the caves in the Tora Bora region of eastern Afghanistan as a base of operations and to hide from Coalition Forces.

Conclusion

By default, intelligence analysts are the Army's geographers. They must have broader knowledge of geography than just the military aspects of terrain and weather. An analyst must be able to think about how the regional geography in an area will impact overall operations. They must understand the climatic and geomorphic differences that may impact the regional economic and military concerns. They must understand why a steel runway in a tropical en-

vironment may create issues with persistent fog, as happened to the Marines in Vietnam at Khe Sanh.[14] At the same time, they have to understand the science behind climate change if they are going to identify how and where it will lead to U.S. military involvement.

The only way to achieve these end-states is by increasing the basic geographic knowledge of our MI analysts. The goal is not to create geography experts, but aspiring analysts must understand simple things such as how the uneven heating of the Earth results in pressure differences, which creates the winds that move air masses around the globe. This results in the different climates and different biomes in which U.S. forces will operate. Similarly, they need to understand how the geomorphology of a region impacts development and economic activities. Differences in access to ports, natural resources, or infrastructure can create the conditions for conflict.

Incoming analysts are not learning the basics of geography in high school or college. Therefore, the responsibility for bridging this gap must fall on the intelligence community. Not every analyst needs a degree in geography or geology, but must understand the basics of how the physical environment works. It is hard to discuss the impact of weather or terrain on operations if you do not know what causes/creates them in the first place.

I recommend that the Intelligence Center for Excellence develop an introductory course that focuses on five key components: earth-sun relations; weather; climate; geomorphology; and culture. This is very similar to many basic introductory physical geography courses taught in colleges and universities. These five components build on and reinforce each other. It is not going to make instant geographical experts, but it will at least improve the basic geographical knowledge that I contend an MI analyst must know at the tactical, operational, or strategic levels to provide the best analysis possible to support the mission.

Endnotes

1. John M. Collins, *Military Geography for Military Professionals and the Public* (Washington, D.C: Potomac Books, Inc.), 3.

2. John Roach, "Young Americans Geographically Illiterate, Survey Suggests," *National Geographic News*, May 2, 2006. http://news.nationalgeographic.com/news/2006/05/0502_060502_geography_2.html. "Final Report: National Geographic-Roper Public Affairs 2006 Geographic Literacy Study," 6-8. At http://www.nationalgeographic.com/roper2006/findings.html.

3. Kyle Dropp, Joshua D. Kertzer, and Thomas Zeitzoff, "The Less Americans Know about Ukraine's Location, the More They Want U.S. to Intervene," *The Washington Post*, 7 April 2014. At https://www.washingtonpost.com/news/monkey-cage/wp/2014/04/07/the-less-americans-know-about-ukraines-location-the-more-they-want-u-s-to-intervene/.

4. Lauren Camera, "U.S. Students Are Really Bad at Geography," *U.S. News and World Report*, 16 October 2015. At http://www.usnews.com/news/articles/2015/10/16/us-students-are-terrible-at-geography.

5. General Ray Odierno, "*The Army of the Future*," The Brookings Institution, Washington, D.C., 15 February 2013, 37. At http://www.brookings.edu/~/media/events/2013/2/15%20odierno/20130215_odierno_army_transcript.pdf, 37.

6. Harold A. Winters, Gerald E. Galloway, William J. Reynolds, and David W. Rhyne, *Battling the Elements: Weather and Terrain in the Conduct of War* (Baltimore: Johns Hopkins University Press, 2003).

7. FM 6-0 Commander and Staff Organization and Operations, May 2014, 10-5.

8. FM 6-0, 9-3.

9. ATP 2-01.3 Intelligence Preparation of the Battlefield/Battlespace, 10 November 2014, 3-14.

10. Collins, 36.

11. Ibid.,38.

12. Fred Pearce, "Mideast Water Wars: In Iraq, A Battle for Control of Water," *Yale Environment* 360, 25 Aug 2014. At http://e360.yale.edu/feature/mideast_water_wars_in_iraq_a_battle_for_control_of_water/2796/.

13. Collins, 268-269.

14. Harold A. Winters, Gerald E. Galloway, William J. Reynolds, and David W. Rhyne, *Battling the Elements: Weather and Terrain in the Conduct of War* (Baltimore: Johns Hopkins University Press, 2003).

MAJ Tansey serves as the Assistant Course Director for Physical Geography in the Department of Geography and Environmental Engineering at the U.S. Military Academy, West Point. A career MI officer, he has served in a wide variety of assignments in the U.S, Europe, and the Middle East to include platoon leader, battalion and brigade intelligence officer, and collection manager. He most recently served as the Executive Officer for the 2nd MI Battalion (CI/HUMINT) in Wiesbaden, Germany. He holds a BA in Anthropology from California State University, San Bernardino, and an MA in Security Studies (Europe and Eurasia) from the Naval Postgraduate School.

MFLTS Providing Support to Army Expeditionary Warrior Experiment

by Patrick O'Malley and Tracy Blocker

The Machine Foreign Language Translation System (MFLTS) successfully demonstrated 2-way speech translation with foreign language speakers during the Army Expeditionary Warrior Experiment (AEWE) 2016 at Fort Benning, Georgia. MFLTS is a software product that provides a basic automated foreign speech and text translation capability. It will be integrated into Army Tactical Systems to augment and complement limited human linguistic resources across all Army echelons in all environments. The open systems architecture enables continuous integration of additional language components ("language packs") to meet the Army's prioritized language translation requirements, resulting in an ever expanding portfolio of language translation resources. The MFLTS Program is an incrementally deployed program that uses an evolutionary acquisition strategy to maximize the inherent advantages of product improvements and commercial best practices.

The AEWE is the U.S. Army Training and Doctrine Command's live prototype experimentation campaign. It examines concepts and capabilities for the current and future force across all warfighting functions. The AEWE focuses on the Soldier and small unit, examining concepts and capabilities for the current and future force across all warfighting functions and doctrine, organization, training, materiel, leadership and education, personnel and facilities (DOTMLPF) domains. The AEWE places technologies, like MFLTS, into the hands of Soldiers and is the Army's capstone event for investigation, experimentation, and assessment of dismounted technologies, tactics, techniques, and procedures, and emerging doctrinal concepts. AEWE informs on critical Army decisions (such as structure, basis of issue plans, and leader development for the technology-enabled Infantry Rifle Company and subordinate elements). AEWE provides capability developers, the science and technology community and industry a repeatable, credible, rigorous and validated operational experiment venue to support doctrine, organization, training, and leadership and education concepts and materiel development efforts.

During the experiment, noncommissioned officers (NCOs) used the MFLTS 2-Way Speech-to-Speech Translation Application for Iraqi Arabic on the Nett Warrior (NW) End User Device (EUD) to assess the performance of the integrated application and peripheral devices consisting of different microphones and speakers. Soldiers from the 52nd Translator/Interpreter Company at Fort Polk, Louisiana served as Iraqi role players in scenarios ranging from basic checkpoint and base security operations to tactical questioning. Both MOS 09L Translator/Interpreter Soldiers involved in the event, who recently returned from Iraq where they served as interpreters, believe that the MFLTS application would be of benefit to Soldiers involved in theater.

The NCOs used the MFLTS application to communicate with the foreign language role players to complete basic tasks or to gather information from the local population. A staff sergeant from the Exercise Force at Fort Benning stated, "In these tactical questioning scenarios, I understood what was needed. I liked having this application on NW, it was easy to use and effective. I felt that I could build rapport with the guy [foreign language speaker]."

"I see this app as ideal for basic communication and questioning when encountering the local population," said another staff sergeant from the Exercise Force. "I like that the logs are automatically recorded on the EUD for later reference." The local Exercise Force Commander echoed the teams' comments, "Even though the app is not 100 percent accurate, it enables communication and understanding."

SSG Steven Comeau of A Co, 1-29 IN engages with an Iraqi speaker using the MFLTS Speech-to-Speech Translation Application on the Nett Warrior (NW) End User Device (EUD) at the Army Expeditionary Warrior Experiment (AEWE) at FT Benning, GA. (Photograph from Tracy Blocker with permission to release photo for public use.)

One example scenario where Soldiers used MFLTS with good effect during AEWE was engagement with a non-Eng-

lish speaking truck driver who had information concerning the unit's area of operations. Supported by an NCO equipped with the MFLTS app on the NW EUD, the Exercise Force Commander learned that the truck driver had recently delivered his cargo and visited his family in an area controlled by insurgents. The man showed the commander on a map where trucks driven by insurgents have been delivering construction supplies (an old airstrip a few kilometers from the unit's position.) With this information, the Commander was able to more effectively plan for the next day's operation against the insurgents.

SSG Steven Comeau of A Co, 1-29 IN engages with an Iraqi speaker using the MFLTS Speech-to-Speech Translation Application on the Nett Warrior (NW) End User Device (EUD) at the Army Expeditionary Warrior Experiment (AEWE) at FT Benning, GA. (Photograph from Patrick O'Malley with permission to release photo for public use.)

Besides assessment of the actual MFLTS application on the NW EUD, Soldiers also used and evaluated three different peripheral microphone and speaker options. Soldiers assessed the peripherals on ease of use, microphone sensitivity, speaker volume, and overall combined performance with the software application. All of the peripheral options succeeded but with various pros and cons identified by the Soldiers, foreign language role players, and AEWE observers. After further analysis of the data points the Product Manager, Ground Soldier Systems (PdM, GSS) will make a determination on peripheral options for future fielding.

The AEWE has proven again to be an excellent venue for Soldier feedback based on Soldier experiences in an operational environment. With the knowledge gained at AEWE, MFLTS will confidently move forward with fielding of the MFLTS 2-way Speech Translation Application to NW in fall 2016. Likewise, PdM, GSS now has important data points to assist in the selection of microphone and speaker peripheral(s).

Patrick O'Malley, CGI Federal Contractor, is the MFLT Capability Developer at TRADOC Capability Manager for Biometrics, Forensics, and Machine Foreign Language Translation (TCM-BF&M), Fort Huachuca, Arizona. He is a retired Army Intelligence Officer.

Tracy Blocker, Scientific Research Corporation Contractor, is the MFLTS Product Office Representative at TCM-BF&M, Fort Huachuca. He is a retired Army Intelligence Officer.

Know Your Role and Communicate Effectively: The Critical Elements to Intelligence Success in DATE

(Continued from page 29)

at the NTC. Failure to incorporate these lessons during home station training will still result in the lessons being learned, as the school of hard knocks tends to instill the longest-lasting lessons. Unfortunately, they come at a great cost to the BCT.

Endnotes

1. "Today's Focus: Decisive Action Training Environment," *Stand To!* At Army.mil, 8 March 2012.

2. JP 2-0 Joint Intelligence 22 October 2013. iv-22.

3. ATP 2-19.4 Brigade Combat Team Intelligence Techniques, 10 February 2015, Section 2-42.

4. Ibid.

5. Ibid.

6. Ibid., para 2-8.

7. Ibid., para 2-4.

8. FM 2-0 Intelligence Operations 15 April 2014, para 1-30.

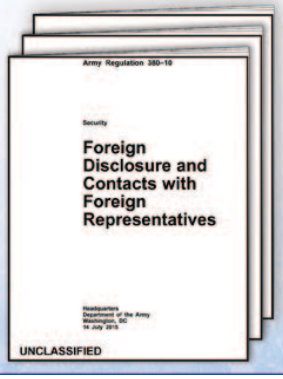
9. Ibid.

10. "Otto von Bismarck Quotes," *Goodreads*.

MAJ Kosek is the BCT Senior Intelligence Observer/Coach/Trainer at the NTC. He began his career in Armor and served as a Tank Platoon Leader, Scout Platoon Leader, and Headquarters Troop Executive Officer in Korea. In 2005, MAJ Kosek transitioned to MI and has since held a number of intelligence positions, including Infantry Battalion S2, MICO Commander, Armored BCT S2, and Division ACE Chief. He has deployed multiple times in support of Operation Enduring Freedom. MAJ Kosek's military education includes the Armor Officer Basic Course, the MI Captains Career Course, and Intermediate Level Education at Fort Leavenworth, Kansas. He holds a BBA and MBA from the University of Notre Dame and an MA in Security Studies from Kansas State University.

Institutionalizing and Operationalizing Foreign Disclosure

by Lieutenant Colonel (Ret.) Dave Grob



"There is only one thing worse than fighting with allies, and that is fighting without them!"

–Sir Winston Churchill, 1945

U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1 The U.S. Army Operating Concept: Win in a Complex World 2020-2040, articulates as a fundamental assumption for the Force that *"except for an immediate response to a national emergency, the Army will conduct operations as part of joint, interorganizational, and multinational teams."* This assumption is reflected doctrinally in ADP 3-0 Unified Land Operations, as that document was published to provide *"a common operational concept for a future in which Army forces must be prepared to operate across the range of military operations, integrating their actions with joint, interagency, and multinational partners as part of a larger effort."* Descending down through the Army's doctrinal taxonomy, ADRP 3-0 Unified Land Operations details the imperative of unified action and defines unified action partners as including *"joint forces and components, multinational forces, and U.S. government agencies and departments."*

ADP 1-01 Doctrine Primer states that field manuals (FMs) *"describe how the Army and its organizations conduct and train for operations"* and that they (FMs) also describe *"how the Army executes operations described in Army doctrinal publications."* Lastly, one additional purpose of an FM is to "fully integrate and comply with doctrine in Army doctrine publications and Army doctrine reference publications." With the clear focus and emphasis on multinational interoperability, it is not surprising that the Army has promulgated FM 3-16 The Army in Multinational Operations, FM 3-07 Stability, and FM 3-22 Army Support to Security Cooperation.

What is surprising and equally problematic is that Army doctrine lacks all but the most scant and tangential references as to how we should plan for, and conduct, the sharing of military information with multinational forces. When these rare doctrinal references do occur, they deal almost exclusively with the sharing of military intelligence. Successful unified land operations require the sharing of information sets from all the warfighting functions, not just intelligence.

Consider the implications of asking and answering the following questions:

Does the Army require fundamental doctrinal principles (with supporting doctrinal techniques and procedures) to enable the planning for, and sharing, of military information across all warfighting functions, to be leveraged in the conduct of bi-lateral and multinational operations and efforts? If this question is answered in the affirmative, then also ask and answer:

- **How is the Army's ability to plan for and share military information across all warfighting functions in the conduct of bi-lateral and multinational operations trained and assessed with respect to ADRP 1-03 The Army Universal Task List?**
- **Is foreign disclosure (the process and act of planning for and sharing of military information, across all warfighting functions, leveraged for the benefit of the USG in the conduct of bi-lateral and multinational operations) best doctrinally defined as a function (a practical grouping of tasks and systems [people organizations, information, and processes] united by a common purpose)? If so, is it best addressed as a mission command, knowledge management, or some other function?**

Still not convinced of the need to institutionalize and operationalize foreign disclosure through doctrine, then consider this illustrative scenario:

You are the Commander of a brigade combat team (BCT). You have been missioned as part of a regionally aligned force to deploy to Africa where your BCT will conduct over 160 missions in over 30 countries. As you begin your mis-

sion analysis, you note requirements to conduct training on a variety of small unit individual and collective tasks. These include, but are not limited to, patrolling, fixed site defense, and live fire training. Additional training tasks will focus on human rights and the protection of civilians. It is expected that the entire BCT team will be leveraged to enhance this multinational training effort with additional topics related to the functional capabilities of your engineers, military police, as well as your primary staff. You also expect that you will spend a great deal of your personal time in senior key leader engagements. You have also realized that you may have occasion to share intelligence and/or force protection information with foreign partners as events unfold in the area of operations.

You have directed your Executive Officer (XO) to identify specified and implied tasks that may require the sharing of controlled unclassified information and/or classified military information to support your deployment as part of the Military Decision Making Process. Your initial guidance also your states that in order to ensure all of this is synchronized, a Foreign Disclosure (FD) Annex be prepared for the Task Force (TF) Operations Order. You also want to make sure that Foreign Disclosure training is conducted prior to deployment and the TF has worked out, trained to, and rehearsed processes and procedures for addressing foreign requests for information during the deployment. Finally, you want to make sure the TF has the right mix (by number and level) of Foreign Disclosure Officers (FDO) (those who can make actually disclosure decisions) and Foreign Disclosure Representatives (those who can coordinate disclosure requests, and then later effect disclosures once a decision has been made by an FDO).

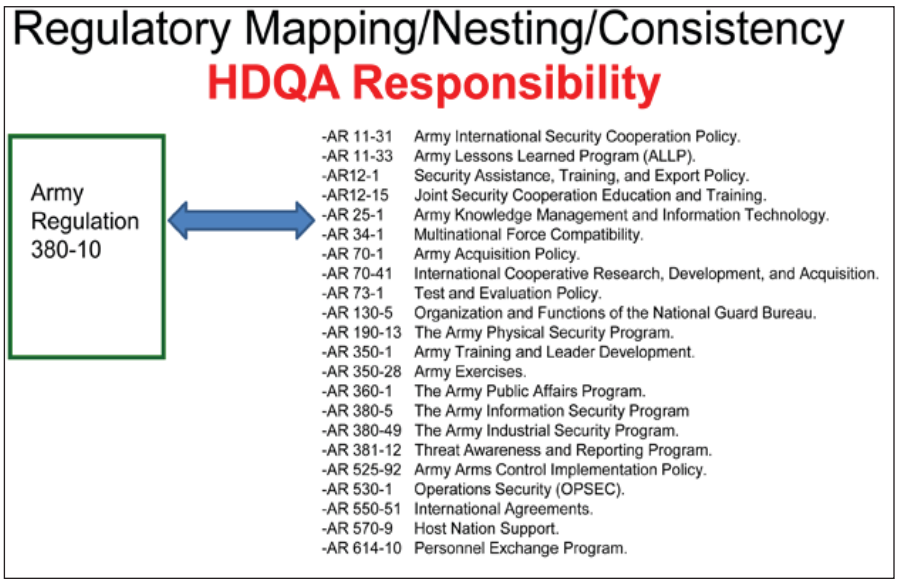
You have made the point to your XO that this is not an administrative, but an operational requirement. Your position is supported by the fact that "Full Spectrum" Operations includes Stability Operations as detailed in FM 3-07, which identifies Army support to security cooperation as a related activity and mission. Your position is further bolstered by the existence of FM 3-16 and FM 3-22. Since your success depends on your ability to share information, you have told the XO to convey to the staff that you consider the ability to share information as an essential TF task.

Now put yourself the boots of the BCT XO and Battle Staff:

- **What doctrinal information will we use to inform and guide our assessments and actions during the orders process, train up, deployment, and return to home station?**
- **What does an FD Annex look like, and who on the staff produces it?**
- **What is the recommended mix of FDOs/FDRs by numbers and levels?**
- **What are the individual and collective pre-deployment training tasks/standards for the TF with respect to FD?**

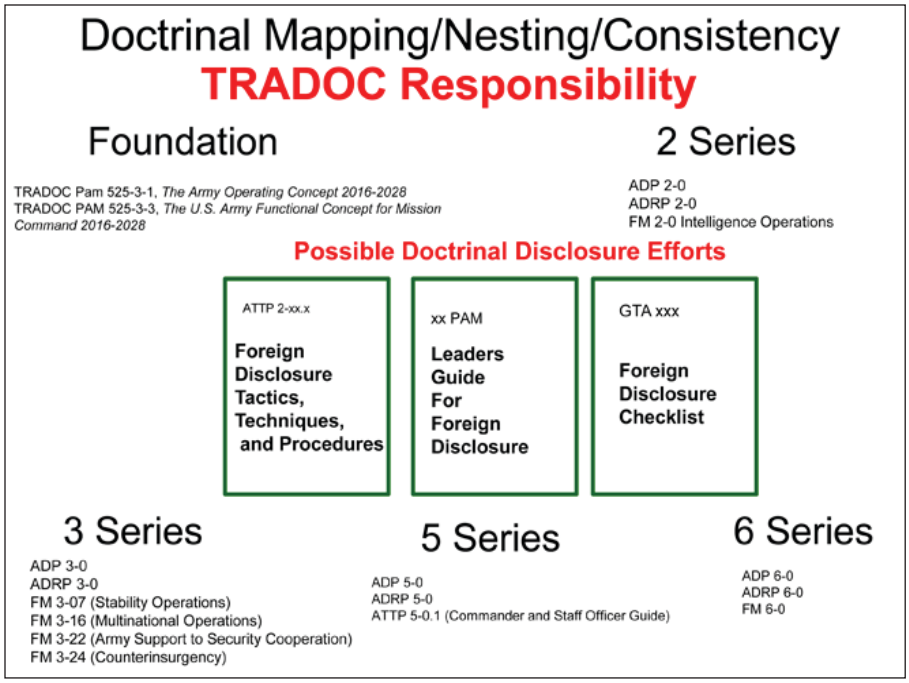
Eating the Elephant One Leg at Time:

Remember, this article is titled "Institutionalizing and Operationalizing Foreign Disclosure" so it has implications beyond doctrine. There is also a role in all of this for Headquarters, Department of the Army (HQDA). That role is ensuring that Army policy and regulations recognize and support the current and future operational environment. AR 380-10 Foreign Disclosure and Contacts with Foreign Representatives, the Army's primary FD regulation, must be synchronized with related policy and regulations. Ensuring this occurs is a primary task for the Office of the Deputy of Staff, G2 (Army Foreign Disclosure Branch).



Writing doctrine is a continuous and deliberate process. It is also an iterative and synchronized effort that ensures consistency across the Force and doctrinal proponents and publications. Just as HQDA has a responsibility to develop and synchronize foreign policy and regulations, TRADOC has the same responsibility for doctrinal publications.

In order for the Army to truly institutionalize and operationalize foreign disclosure, HQDA and TRADOC must become allies and freely coordinate and share information in support of a unified effort. It is only through these combined efforts will the Army address the challenges of foreign disclosure. Until such a time as both of these efforts mature and become fully integrated and synchronized, the



Army will continue to struggle with planning for and sharing military information across all warfighting functions to be leveraged in the conduct of bi-lateral and multinational operations and efforts. Not exactly the best way to *"Win in a Complex World."*

USAICoE Doctrine Note: Institutionalizing and operationalizing foreign disclosure is an important topic area. USAICOE Doctrine has been in extensive coordination with Mr. Scott Shultz and Mr. Dave Grob from DA G2 on operationalizing foreign disclosure. As a part of these efforts, on 26 April 2016 the Combined Arms Doctrine Directorate at Fort Leavenworth chaired a VTC on better tackling this issue within doctrine. As an outcome of the VTC, the Army doctrine community and DA G2 will team to form a doctrinal working group. The working group date has not yet been set to meet at the Pentagon to determine specific publications to update and to draft material for those publications. Additionally, TRADOC G2 is developing a tasker for a Hasty DOTMLPF Assessment for foreign disclosure. This assessment will take a broader look at how the Army can better institutionalize and operationalize foreign disclosure. Throughout the last few months Army G2, TRADOC G2, and the Intelligence Center have worked closely together to solve these issues.

LTC (R) Grob is currently the HQDA, ODCS G-2, Foreign Disclosure Branch, Strategist, Planner, and Integrator. He served on active duty from 1987 through 2007 in a variety of Infantry and Military Intelligence assignments to include multiple assignments with the 101st Airborne Division (AASLT) and the HQDA, ODCS G-3/5/7. He holds an MS in Strategic Intelligence from the National Intelligence University.

The Necessity for Social Media Intelligence in Today's Evolving Battlefields

by Captain Matthew F. Morgan

On 1 March 2016, General Joseph L. Votel, then Commander, U.S. Special Operations Command, stated in a congressional hearing that Social Media was likely an area of growth for the Special Forces community.[1] The reactions posted on numerous sites were mixed. I asked a small group of analysts what Social Media Intelligence, Criminal Intelligence, and Financial Intelligence meant to them. They had no clue. Social Media intelligence is often waved off as just another Open Source Intelligence job or maybe under the emerging Cyber sections. At first thought its use of information sharing platforms such as Facebook and Twitter immediately distance itself from any kind of military use. This could not be farther from the truth. During a deployment with limited access to mission related information/intelligence on SIPR and NIPR devices I constructed a SOCMINT cell as an experiment to explore what information was available. We were immediately able to produce weekly, and then daily intelligence summaries that were disseminated to all staff and command elements.

In August 2014 I published a study on Social Media Intelligence and its relevance today. I used case studies that included the Arab Spring, current use by Russia, the rise of ISIS, and use by national and international law enforcement agencies. I included real time intelligence posted by the Israel Defense Forces and Hamas seconds before, during, and after operations. I included real time battle damage assessment (from photos and videos) posted by Peshmerga forces during and after operations against ISIS forces. Other countries have weaponized Social Media and its use is tightly controlled by their governments for both tactical and strategic intelligence operations, information operations, and other uses. I obviously cannot present all 74 pages of my study here, but below I have included my Introduction and Conclusion sections as they are a fair and general snapshot of why the argument should be made to recognize SOCMINT, and perhaps explore its inclusion into the Military Intelligence school house curriculum.

Introduction

The proliferation of information through social media has ushered in a new era of intelligence collection and analysis. Never before in history has information been made immediately available through public sharing on such a grand scale. Social Media Intelligence (SOCMINT) has become a necessary discipline that fills a current intelligence gap in the Intelligence Community (IC). This new discipline allows the IC to effectively combat emerging threats utilizing social media for tactical and strategic advantages. Current social media case studies reveal an evolution of information that contribute to national defense and law enforcement operations. Through the examination of several key case studies, this paper identifies the dangers of ignoring this growing source of information and the perpetually evolving platforms that produce it. This paper will present an argument for the need to recognize a new intelligence discipline and analyze the rapidly growing amount of information published through these social media platforms.

The War on Terrorism began in the aftermath of the 9/11 attacks conducted against the U.S. by a foreign terrorist organization. This new war was launched with no geographical or doctrinal restrictions and began an era of redefining the nature of modern warfare. One vital element of this new era of global warfare has been the evolution of internet use by all those involved. The quickly expanding global reach of the internet during this new war has paved the way for numerous social media platforms to emerge.

This emergence of social media platforms has given historically repressed populations around the globe the ability to communicate ideas and grievances globally. The effect of this new age of communication and information sharing has led to the overthrow of governments, the rise of militant movements, an evolution in law enforcement capabilities, and new ways to conduct information warfare. Equally as groundbreaking is the new level of access the IC has gained to these populations and organizations.

Social media has become the world's fastest growing information resource. As Fitsanakis states "The emergence of interconnected computer networks arguably represent the biggest post-Cold War paradigm shift in tactical intelligence collection."[2] This new paradigm shift in tactical and strategic intelligence collection has not been thoroughly examined, nor adequately assessed for its positive or negative contribution to the intelligence and law enforcement community.

A review of recent intelligence and law enforcement collection training and certification programs revealed that this new form of collection and analysis was misinterpreted or missing from the curriculum. While Open Source Intelligence (OSINT) established procedures for monitoring web sites, news sources, and online blogs and journals, it has not yet expanded into the much larger sector of social media.

What remains is perhaps the largest intelligence gap in the history of intelligence collection as immeasurable amounts of data are uploaded every second across multiple social media platforms from every corner of the globe. This obvious intelligence gap in today's intelligence and law enforcement curriculum is an indicator that current intelligence collection techniques are once again becoming antiquated and obsolete.

The majority of relevant information in the collected metadata is captured by computer programs and can be made available to SOCMINT analysts. These analysts can determine what is relevant and to whom. This information is now being identified as vital because, unlike other sources, it is being presented continuously in real time and therefore has proven to be a valuable asset in a multitude of time sensitive events. Vilkaite claimed "With the times changing and the world becoming more and more globalized, journalism is becoming slightly outdated since the news gets onto social media platforms (e.g., Facebook and Twitter) much more quickly than onto the news websites".[3]

This rapidly expanding source of information has been tapped by U.S. and foreign intelligence as the newest and richest source of information and intelligence. It has only begun to be defined as an intelligence collection discipline and examined as a new battlefield for information operations. In fact the official Department of Defense dictionary does not contain a definition of social media. The merits of establishing this new collection discipline can be quantified by examining the amount of readily available information on social media and its contribution to real-time events. Through extensive examination of available sources this paper will examine the question, "Has the proliferation of information through social media had a positive or negative effect on intelligence collection?"

The establishment of SOCMINT would provide a professional group of analysts a standard set of guidelines and methods to follow. This would allow policy makers and intelligence customers a legitimate collection discipline to submit requests for information. By establishing SOCMINT as a legitimate collection discipline, this new source of information becomes a positive contribution to the intelligence community because time sensitive information has become readily available through these social media platforms.

Conclusion

SOCMINT became a necessary discipline to the IC with the emergence of the War on Terrorism. This new unconventional war changed how the U.S. would have to fight its enemies. This new war had no geographical boundaries and social media was the one platform that spanned the globe. This new war also had no defined timeline with the potential to be conducted indefinitely. Social media also provides necessary endless platforms that can be collected on and analyzed 24 hours a day indefinitely, with no cost or travel restrictions. The law enforcement community is faced with the same challenges and opportunities as their required connection to the population they serve will evolve at the same speed and depth as the social platforms they must collect on and analyze. Omand, Bartlett, and Miller have defined this new intelligence discipline as SOCMINT.[4] The emerging proliferation of information through social media has clearly changed intelligence collection and analysis forever. The ownership is on the IC to establish SOCMINT as a discipline to answer this critical paradigm shift in intelligence collection and analysis.

The terms "proliferation of information" and "paradigm shift" have been used repeatedly throughout this paper to make the point that these new platforms of information publication have changed the availability of information and intelligence to the world. Organizations that accept this and change with this paradigm shift such as Europe's law enforcement community and ISIS militants sweeping across Iraq have, and will, emerge victorious in the information wars being waged. During the development of this paper both the Israel Defense Forces and Hamas organizations publicized official military social media units charged with waging this information war while ground forces battle back and forth through conventional means. This emerging trend has added social media to the concept of asymmetrical warfare whether U.S. intelligence organizations have accepted it or not. This research has been conducted over nearly a three month period and an identifiable trend to quantify these statements has been the apparent rapid expansion of the IC's use of social media since this paper was initiated. In the course of the creation of the intelligence summaries for this paper social media analysts were encountered. The existence of such analysts is evidence that progress has been made in a short amount of time and that the U.S. IC is working diligently to close these intelligence gaps and compete in this new intelligence arena.

Even with the present day improvements in SOCMINT operations there are critical areas that still must be addressed. The first necessary step to legitimizing SOCMINT as an intelligence discipline is to establish a standard reference manual which discusses all responsibilities and standard operating procedures for conducting SOCMINT operations. This should include how to build priority intelligence requirements that can be answered through social media

platforms as well as how to isolate certain priority platforms to answer each intelligence requirement. The collection process itself should be outlined in this manual as well as reporting and disseminating procedures back to the customers. From this standard manual a curriculum should be developed and immediately incorporated into intelligence schools including practical exercises. It should be nested near the Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and OSINT portion of the curriculum. There should be an advanced training course added for individuals with a desire to operate in this field or to train leaders in SOCMINT to meet the growing requirements.

After a standardized curriculum and the advanced course is established it will be necessary to incorporate SOCMINT analysts into the IC. Because of the nature of these time sensitive platforms they should be required to operate inside 24-hour fusion cells with access to 24-hour tactical operation centers to deliver intelligence as it is posted. There is an identified need to colocate SOCMINT analysts with interpreters. The ideal scenario identified through this research is to place SOCMINT collectors and analysts in fusion cells where they can collaborate with other disciplines and contribute their products to intelligence summaries and answer time sensitive intelligence requirements by customers at all levels. They will operate most efficiently near HUMINT and SIGINT cells to supplement lethal targeting operations and assist in building link analysis charts for network tracking.

One clearly identifiable trend in this paper is the rapid pace at which social media is expanding and the pace at which the platforms evolve. Future operations cells will have to consider social media platforms and the amount of information provided through them in future planning sessions. An example of this rapid growth is that at the time this research began Facebook was barely considered a Large Cap stock and now qualifies as a Mega Cap stock. The CEO of Facebook, Mark Zuckerburg, has passed the CEOs of Google in valuation as the popular social media platform expanded its worth almost twice as much as analysts predicted this earnings season.

Predictive analysis would assess that on its current trajectory, Facebook will likely expand into every emerging market in the next decade and triple its customer base in half that time in countries such as China and Russia. That may be a cautious estimate as the actual growth rate of social media users is difficult to determine and has expanded at a rate that makes consistent assessments impossible. What this means to the IC is that if it indeed is as far behind other countries and organizations as this paper has shown then it will find it even more difficult to play catch up with these rapid rates of expansion. The amount of information becoming available through social media has already qualified as Big Data and surpassed that being collected and stored from communications and emails.

This paper has identified the strategic and tactical value in collecting and analyzing the growing amount of information being presented through social media platforms. It has shown quantifying numbers and historical examples of the successes of embracing it and the failures of acting too late. This paper has provided an elementary way forward for developing and implementing SOCMINT into the IC to confront this growing paradigm shift in intelligence collection. With these tools in place, the U.S. IC will be able to collect and analyze real time information being posted from all around the world and incorporate it into tactical operations and strategic policy recommendations faster than any established discipline has made possible in the history of the IC. By establishing this discipline to effectively monitor and assess this growing information source the IC will be able to compete with international adversaries as well as gain, and maintain, a critical advantage over emerging threats worldwide.

Endnotes

1. Leo Shane, "America's Silent Warriors Look to Up Their Game on Social Media," *Military Times*, 2 March 2016, at http://www.militarytimes.com/story/military/2016/03/02/votel-socom-social-media/81210372/.

2. Joseph Fitsanakis and Micah-Sage Bolden, "Social Networking as a Paradigm Shift in Tactical Intelligence Collection," *Mediterranean Council for Intelligence Studies*, 2012, 28. At http://www.rieas.gr/images/mcis2012.pdf.

3. Evelina Vilkaite, "The Relationship between the Media and Intelligence," E-International Relations Students, 22 March 2013, 3. At http://www.e-ir.info/2013/03/22/the-relationship-between-all-forms-of-media-and-intelligence-activity/.

4. David Omand, Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)", *Intelligence and National Security*, Vol. 27, no. 6, 2012, 801-23.

(Continued on page 45)

Joint UAV Swarming Integration Quick Reaction Test

by Mr. F. Patrick Filbert

Introduction

As technology improves, so does the capacity to expand a defensive perimeter to ever increasing ranges both horizontally and vertically. Identifying ways to penetrate this perimeter with assets and capabilities that do not require ever more expensive solutions requires creative use of current and emerging technological advances. Potential adversaries understand the U.S. is extremely technologically advanced with its warfighting systems. This requires a thinking enemy to develop ways to keep America's advanced systems outside their sphere of influence; specifically, to both deny and create an inability to gain access to specific areas of operation. In the current vernacular, this is called creating an anti-access/area denial (A2/AD) environment which has, as its backbone, advanced integrated air defense systems (IADS).

A Bit of History

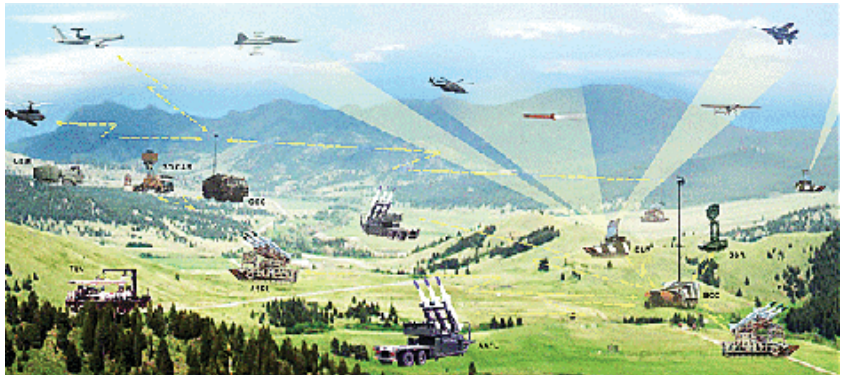
Being able to provide a "layered" offensive capability with manned kinetic/non-kinetic payload armed aircraft has been done for some time. One example is how a joint Army-Air Force helicopter team (Task Force Normandy, comprised of U.S. Air Force (USAF) MH-53J/PAVE LOW III and Army AH-64/APACHE attack helicopters) blinded Iraqi IADS early warning radars with non-kinetic electronic attack (PAVE LOW IIIs) and destroyed the radars (APACHES) with kinetic weapon's strikes (i.e., HELLFIRE missile, HYDRA rocket, and 25mm cannon fire) in the opening minutes of Operation Desert Storm. This allowed follow-on USAF strike aircraft access through coverage "holes" in Iraqi IADS to attack key targets further into Iraq.[1] Similarly, future use of an advanced wave of unmanned aircraft systems (UAS) equipped with electronic warfare (EW) payloads leading a subsequent wave of attacking aircraft from carrier strike groups is one potential way to enter and counter a potential adversary's A2/AD environment.

However, while emerging EW payload testing on UAS is occurring, mating electronic attack (EA) payloads onto a coordinated semi- or fully-autonomous swarm of smaller unmanned aircraft (UA) is still an emergent test environment effort. However, once such capabilities mature, being able to employ them requires that a foundational concept be in place. The Joint Unmanned Aerial Vehicle (UAV) Swarming Integration (JUSI) Quick Reaction Test (QRT) was directed on 27 February 2015 by the Deputy Director, Air Warfare under the authority of the Office of the Secretary of Defense, Director, Operational Test and Evaluation to address such a foundational approach.

The JUSI QRT was established under the Director of Operational Test and Evaluation's Joint Test and Evaluation Program on 29 July 2015. It is co-located with U.S. Pacific Command's (USPACOM) J8 Resources and Assessment Directorate, Camp H.M. Smith, Oahu, Hawaii. The JUSI QRT reports to the AF Joint Test Program Office, Nellis Air Force Base, Nevada and receives support from USPACOM J81 (Joint Innovation and Experimentation Division). The JUSI QRT will develop, test, and validate a concept of employment (CONEMP) for the integration and synchronization of swarming UA performing EA in support of the joint force against an advanced IADS. The JUSI QRT effort is focused on a 2015-2020 timeframe to research and identify previous and ongoing swarm related efforts while building a swarming UA community of interest, concurrent with CONEMP development.

Advanced IADs and How to Address Them–The Problem

Modern surface-to-air missile (SAM) systems are an integral part of advanced IADS. These IADS are, in turn, integral parts of a potential adversary's networked A2/AD environment. For the purpose of the JUSI QRT effort, IADS refers to a networked system of adversary capabilities (e.g., a series of detection and tracking radars coupled with SAMs) and not specific to one platform (i.e., an IADS on a warship by itself or a specific individual SAM such as an SA-20).



Notional Integrated Air Defense System.[2]

The joint forces do not currently have adequate ways to fully plan, integrate, or synchronize the effects delivered by UA swarms. This requires development and testing of a foundational CONEMP offering an effective planning methodology for delivering integrated effects of UA swarms against advanced IADS protecting targets with threat SAM arrays.

The joint force is currently over-reliant on standoff weapons (SOWs) and 4th/5th generation strike platforms to address the A2/AD challenge. UA swarms represent a potential additional approach, complementing existing platforms and weapons systems. Despite rapid technical advances in UA swarming development and demonstrations, the joint force lacks a CONEMP for operations requiring UA swarm-delivered effects. The lack of a CONEMP or other supporting documentation hinders requirements development, A2/AD countering, and precludes integration and synchronization with the rest of the joint force.

The Approach–Addressing the Problem

Combat capable and survivable UA with the capability to perform swarming functions are a new but quickly growing aspect of modern warfare. The JUSI QRT will take the first step to characterize, develop, and evaluate a CONEMP for using multiple UA of various sizes to deliver coordinated EA to enable other weapons and platforms (i.e., various types of SOWs, decoys, jammers, and 4th/5th generation platforms) access to counter A2/AD approaches. With the short lifespan of the JUSI QRT–one year–the effort will focus on CONEMP development supported by a series of modeling and simulation (M&S) runs over the course of three test events.

Integrated support by Johns Hopkins University's Applied Physics Laboratory's (JHU/APL) experienced M&S personnel during each of the test events will enable the QRT to gain data collection for the equivalent of hundreds of swarm flights; thus providing a cost saving aspect concurrent with data analysis to support CONEMP development. JHU/APL will provide M&S and analysis of the execution of UA with EA payloads against scenarios developed to test the UA's ability to deliver desired effects against an advanced IADS as part of an A2/AD environment.

The resulting qualitative and empirical data, once analyzed, will enable the JUSI QRT Team to assess findings, conclusions, and recommendations to revise the CONEMP between each test event with JUSI QRT's first test event, which wrapped up on 20 November 2015. Additionally, upon completion of each test event, a Joint Warfighter Advisory Group (JWAG) will be convened to receive test event results. The first JUSI QRT JWAG occurred on 9 December 2015. As the QRT process continues, it will lead to development of a finalized swarming UA CONEMP to provide the link to requirements development and capability integration for the joint force to have a distributed approach to complement existing solutions which focus on 4th/5th generation strike platforms and SOW.

Artist Concept of a Swarm (DARPA).[3]

The Way Ahead

At the end of the JUSI QRT, the resulting CONEMP will provide an effective operational context to inform requirements development, roadmaps and, eventually, tactics, techniques, and procedures (TTP) in several areas, including communication, automation, UA, and EA to deliver intended effects. The CONEMP will also serve to help focus future Department of Defense and industry investment. Future considerations related to swarming UA with EA payloads may include development, testing, and validation of TTP for UA with EA payloads. Such TTP would further reinforce the use of swarming UA by empowering the commander to develop standards in the areas of manning, equipping, training, and planning in the joint force. In the interim, the JUSI QRT developed CONEMP will provide planners, trainers, and their supporters with a start point for employment of this capability.

Endnotes

1. Jerome Martin, Lt Col, USAF, *"Victory from Above: Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm,"* (Air University Press, Maxwell Air Force Base, AL, June 1994).

2. Ajai Shukla, "New Delhi Could Have Anti-missile Shield by 2014," *Business Standard*, 29 August 2011, at http://www.business-standard.com/article/economy-policy/new-delhi-could-have-anti-missile-shield-by-2014-111082900066_1.

3. Elizabeth Palermo, "Fairy-Tale-Inspired 'Gremlin Drones' Could Spy in Swarms," *livescience,* 2 September 2015, at http://www.livescience.com/52073-darpa-gremlin-drones-program.html.

The author would like to thank Lt Col Matthew "Bulldog" Nicholson, Andrew "Wooly" Wolcott, Don Murvin, Brendan "K-PED" Pederson, and

Brock Schmalzel for their guidance and feedback during the writing of this article.

MAJ (RET) Filbert, U.S. Army, is the JUSI QRT Subject Matter Analyst-UAS. Commissioned an M1 Armor Officer, he transitioned to MI and served as an Assistant Brigade S2 during Operations Desert Shield/Desert Storm and an Intelligence Analyst during Operation Joint Force with C/J2 NATO SFOR in Bosnia. He has held command and staff positions from platoon through joint staff in the U.S., Europe, Bosnia, Korea, and the Middle East during a 24-year Army career. His last Active Duty position was Chief, Concept of Operations Branch, Joint UAS Center of Excellence, USJFCOM. Post military career efforts include joint counter-UAS TTP development, intelligence analysis in a USAF Intelligence Squadron and UAS Wing, and Project Manager for USPACOM J2's Socio-Cultural Analysis effort. He holds an MA in History from the University of Hawaii and earned his Master's Degree in Strategic Intelligence with Honors at the American Military University. His military education includes the Armor Officer Basic Course, Military Intelligence Transition and Advanced Courses, Signals Intelligence Course, the U.S. Army Command and General Staff College, and the U.S. Army Force Management College.

The Necessity for Social Media Intelligence in Today's Evolving Battlefields

(Continued from page 42)

CPT Morgan is currently an Operations Officer for the Capabilities Development & Integration Directorate at USAICoE, Fort Huachuca, Arizona. His previous assignments include SIGINT Platoon Leader, 4th BDE, 101st Airborne Division, Fort Campbell, Kentucky; Current Operations and Collection Manager, 4th BDE 101st (Forward Deployed Afghanistan); S2 OIC, 1-61st CAV and Targeting Officer/BISE Chief for RC-East, 4th BDE 101st (Forward Deployed Afghanistan); Battalion S2, 93d Military Police Battalion, Fort Bliss, Texas in which he deployed to Guantanamo Bay, Cuba in support of Operation Enduring Freedom as the Task Force Platinum Intelligence Officer, and Commander of the Punisher MP Detachment in the 93d Military Police Brigade. He holds an MA in Intelligence Studies with a Concentration in Intelligence Collection from American Military University. His military education includes the Critical Thinking Red Team Practitioners Course from the University of Foreign Military and Cultural Studies, Crime Analysis Applications from the Alpha Group Center for Crime and Intelligence Analysis, and the USCENTCOM Personality and Network Analysis Course from the Regional Joint Intelligence and Education.

Doctrine Note. The U.S. Army Intelligence Center of Excellence (USAICoE) agrees with the author that OSINT is an important and growing intelligence discipline. OSINT provides the foundation "…essential to generating intelligence knowledge" and offers the ability "…to satisfy intelligence and information requirements…."[1] Use of social media is a component of OSINT. Joint Publication 2-0 Joint Intelligence, refers to "web-based networking platforms" as an example of open sources.[2] Army Techniques Publication 2-22.9 Open-Source Intelligence, further makes note of social media as a component of OSINT.

Intelligence professionals, when conducting open source research, both on and off of the internet, must be mindful of OPSEC and Intelligence Oversight. AR 350-1 Operations Security provides guidance to prevent disclosure of critical and sensitive Department of Defense (DoD) information in any public domain. Intelligence professionals, when conducting open source research, must understand and comply with Executive Order 12333, DoD Directive 5100.20, DoD Regulation 5240.1-r, and AR 381-10 in order to practice proper Intelligence Oversight.

The draft Army Directive for U.S. Army Open Source Intelligence (OSINT) Activities is in staffing for Secretary of the Army's signature and publication. This directive, once signed and issued, will provide policies and procedures for U.S. Army OSINT activities in accordance with DoDI 3115.12. The Army Directive will prescribe critical procedures for U.S. Army OSINT activities including:

- ***Risk management under defined OSINT Activity Tiers.***
- ***Use of information requirements and collection plans.***
- ***Use of government devices and location of U.S. Army OSINT activities.***
- ***Use of social media for OSINT purposes.***
- ***Considerations for U.S. Persons' Identifying Information.***
- ***Considerations for intellectual property.***

OSINT training is available online through the Intelligence Knowledge Network and in classroom instruction provided by the U.S. Intelligence and Security Command (INSCOM) mobile training teams and by the Army Reserve Intelligence Support Centers. Basic OSINT training is provided in USAICoE institutional courses from enlisted through officer ranks. Efforts are underway, in coordination with INSCOM, to expand this training to include more advanced skills and potential national certification in OSINT analysis for graduating students.

Army units at echelons from brigade combat teams (BCTs) to Theater are actively engaged in OSINT research and analysis in support of operations worldwide. BCTs, during rotations at combat training centers, are exposed to the importance of integrating OSINT in their intelligence operations in order to effectively support the commander's decision-making and targeting.

We are happy to discuss the many ways that USAICoE is identifying and addressing gaps in U.S. Army OSINT capabilities. Questions may be directed to usarmy.huachuca.icoe.mbx.doctrine@mail.mil.

Endnotes

1. ATP 2-22.9 Open-Source Intelligence, July 2012.

2. JP 2-0 Joint Intelligence, 22 October 2013.

The CI Survey: An Agent's Tool for Lead Development

by Captain Daniel T. Miller and Mr. Rick Romero

The views and ideas expressed in this article are of the authors and not of the Military Intelligence Professional Bulletin, the United States Army Intelligence Center of Excellence, the United States Army Or Department of Defense."

Doctrine Note. The term Counterintelligence (CI) Survey as described in this article is not defined in Army policy or doctrine. The term CI Survey is the synchronized execution of various CI tasks for a supported unit, program, or activity. These tasks include, but are not limited to, the Covering Agent Program, mass and individual TARP briefings; CI conducted Threat Assessments; CI participation in Vulnerability Assessments; and cyber assessments of the supported unit's online digital profile and social media.

Introduction

A Counterintelligence (CI) Survey is an actively undertaken event in the CI field to develop leads and exchange with supported units. The common structure of the survey is cryptic, ill defined, and open to interpretation. Of the three Army Regulations covering CI and CI operations (ARs 381-10, 381-12, and 381-20), the first two never mention CI Surveys and the other only states, "CI advice and assistance (to a unit) may include…CI surveys and technical inspections."[1] ARs lack a definition of what a CI Survey actually is which greatly adds to the overall ambiguity of this operation. The only practical aid to CI Surveys is the 902d Military Intelligence (MI) Group *Investigations Handbook*, which states:

> ***CI and security surveys, regardless of the purpose conducted, (e.g., operations security evaluations of vulnerability assessments), should always be viewed as lead development opportunities. While we in fact conduct some CI Surveys primarily for the purpose of lead development, all such opportunities to talk to people within their work environment should be exploited. Always include questions regarding foreign contact and the basic indicators of espionage in any questionnaire developed for the survey. Surveys, especially of large populations, tend to generate numerous items of CI interest.[2]***

None of the three ARs nor the MI Handbook defines the operational term CI Survey or its components. Yet from the most junior agent to the most seasoned veteran, the term CI Survey evokes the same response from them as operational terms like "Raid or Ambush" to an Infantryman. This paper seeks to clarify the term CI Survey, and share best practices for the conduct of an effective survey.

The Kaiserslautern MI Detachment (KMID), 2d MI Battalion (BN), 66th MI Brigade Theater (MIB(T)) conducted a CI Survey on multiple units within the Kaiserslautern Military Community (KMC) in October 2014. The intent behind the survey was to develop CI leads in a military community that had uncharacteristically few. Prior to the survey, KMID had only two CI leads as compared to other U.S. Army Europe field offices that averaged 10 to 15 CI leads. Statistics indicated KMID needed to do something different. Thus, KMID conducted a CI Survey on the units of the KMC in order to generate leads and reaffirm the 66th MIB(T)'s presence within the KMC. Building upon the limited doctrine available, which simply states that a survey is a lead development tool, KMID asked several different questions. First, how does a unit conduct a CI Survey? Second, how will a survey develop leads? Lastly, what actions or constructs make a CI Survey?

The CI Survey

To lay the framework for the discussion, KMID's CI Survey used a multifaceted approach to surveying a unit. The first part was conducting a mass Threat Awareness and Reporting Program (TARP) brief to the unit in order to prime the target audience into thinking about TARP indicators. Following that, individuals selected throughout the chain of command were interviewed by a CI Team and given a personal one-on-one TARP interview. Overall KMID had eight teams working at once, with three interviews scheduled per day per team. While those eight teams conducted the interviews, another team conducted a CI threat vulnerability assessment (TVA) of the unit's workplace, and the supporting analyst conducted a Cyber TVA of the unit's cyber workplace. Each layer of the survey contributed to the overall picture of the unit, highlighting CI leads, which needed investigating.

Preparing for the CI Survey

Preparations for the survey consists of three steps. First, the office or detachment must select a unit to develop and assess for CI leads. Next, the unit must gain the support for the survey through the unit's command. Lastly, one must properly man and train for the survey. KMC houses 43,000 Army personnel, so surveying all of them is impossible. Through dialogue with the 2d MI BN and 66th MIB(T), KMID determined the survey needed to focus on the most at-risk units. KMID weighed and evaluated certain criteria

to include the number of previous CI incidents, ranks of commanders, a unit's foreign contact and travel, the unit's access to sensitive information, and the threat of foreign intelligence security services when deciding which units to survey. Once KMID leadership identified several units, the next task was convincing those unit's commands of the value and concept of such a survey.

One of the most interesting aspects of a CI Survey is its immense benefit to the surveyed command. KMID's proposition was to take a holistic look at the unit, assess the vulnerabilities, and develop a strategy with KMID to improve awareness. After the survey, the detachment produces products, specifically a comprehensive list of risks the command may (or may not) know about, which the command can then mitigate. Additionally, this list only goes to that command, addressing the vulnerability at the lowest level. The detachment gains investigative leads through the survey and the command gains an outside assessment of their organization. Everyone benefits by identifying potential vulnerabilities before they become a problem.

Concerning the training conducted prior to the survey, the standout achievement of the operation was the use of an unconventional CI Team due to the personnel restrictions within the 66th MIB(T). CI Agents were surged to KMID in order to conduct the operation. However, due to multiple commitments across Europe and Africa, there were not enough agents required to support the survey. KMID compensated by employing a dynamic briefing team concept that paired a military occupational specialty (MOS) 35L CI Special Agent with an MOS 35M Human Intelligence (HUMINT) Collector. KMID opted to take an unconventional approach to the conventional "CI Team" in order to field more teams. This approach eventually turned out to be the model for future intelligence teams within the 66th MIB(T).

This pairing greatly complements the two MOS, playing off the already trained strengths of each. A 35L receives training in investigations and the technical aspects of conducting an investigation. A 35M receives training on reading a person's reactions to a series of questions, specifically focusing on indicators and signs of deception, as well as recognizing information of intelligence value that might come up during the briefing. During the survey, the Agent led by asking the questions, while the 35M took notes, read body language, and assisted with follow up questions on missed leads. This team approach to interviews worked much better than the one-on-one approach and became one of the resounding successes of the survey.

Explaining the composite team concept during the training phase of the survey was invaluable because it exposed both the CI Agents and the HUMINT collectors to a new way of thinking and a new way to approach their jobs. There was clear skepticism at first, but after it was practiced, having that extra person in the two-on-one interview, specifically focused on different tasks, enabled the team to gather a much wider array of information than if it was just the single Agent. The other unintended benefit of the pairing was that both MOSs now have a much greater respect, understanding, and appreciation for what the other does, rather than the "You are CI, and you are HUMINT" attitude. It was team building at its finest.

Lead Development

KMID approached the survey along three lines of effort (LOEs) gauging the personnel, physical, and digital make-up of a unit. The personnel line of effort initially focused on the TARP, but then later expanded to include more in depth, two-on-one TARP briefs, focusing on the face-to-face interaction. The physical LOE included a CI focused TVA to look at the infrastructure of the unit and identify any vulnerabilities. A cyber TVA was conducted concurrently with the personnel and physical LOEs to scrutinize the unit's unclassified networks in order to identify additional potential vulnerabilities. This LOE paid particular attention to social media given its significance in modern society.

Doctrine Note. The term threat vulnerability assessment is two different types of protection assessments defined and discussed in AR 525-13 Antiterrorism, and ATP 3-37.2 Antiterrorism. Army CI conducts threat assessments and participates in vulnerability assessments in support of the Army Antiterrorism program.

A lead in itself is any reportable incident outlined in Chapter 3 of AR 381-12. So how do you find these leads? You talk to people. The foundation of the survey had to be personal, face-to-face conversations in order to develop these leads. With this approach, consider a lead a potential vulnerability. A lead can be a vulnerability in discipline, a vulnerability in security, or a vulnerability in morals. In order to maximize lead development and holistically view all the units' vulnerabilities, KMID determined that the survey must include how, and where, the units work. A CI focused TVA became the tool that determined a vulnerability for this LOE.[3] Additionally, to meet the intent of a holistic approach, the detachment also included a cyber vulnerability assessment. Every unit in the Army conducts day-to-day business over the internet, so KMID determined that a CI Survey had to look for vulnerability in not only the personnel in the unit, but also where they work, and what they do on the internet. Those three facets would give the agents involved a holistic view of the unit, all the while generating leads.

Conduct of the Survey

On the personnel LOE, flexibility when dealing with people is paramount. No-shows were quite frequent, and deemed to be an unavoidable obstacle during the survey. Regardless of rank, MOS, or gender, no-shows will happen. Therefore, having a point of contact (POC) within the surveyed unit, someone designated to push people into slots is invaluable. Without a POC, the survey team will waste hours of time. The other piece of flexibility is team changes. Due to myriad issues, team members often incur other tasks. Thus, going back to the training, everyone needs to be on the same page as far as expectations go in the event that partners switch. The mission comes first, team integrity does not. This shuffling of agents also gave some of the younger, more inexperienced agents time to learn from their seniors.

Concerning the physical LOE, each TVA actually generated zero leads and identified only limited physical security issues. The real benefit from a TVA is building relationships with the local garrison commander. CI's number one mission is Title X support to force protection. CI TVAs do just that. Leads are not everything, the physical TVA builds your reputation in the local area, which can be much more beneficial and actually lead to more investigative leads down the road. The TVAs are an investment in the community and show your team's support to the local garrison. The issues discovered are important, but quickly become more of a command issue or an anti-terrorism and force protection issue, rather than CI.

The Cyber TVA was the first of its kind conducted in Europe. KMID used an analyst to research the unit on the internet and collect as much information about the surveyed unit as possible. To quote the former Deputy Director of National Intelligence Thomas Fingar, "Open sources can provide up to 90 percent of the information needed to meet most U.S. intelligence needs."[4] This is equally true of the enemies of the U.S. and their ability to gather on us. The Cyber TVAs intent is to do just that and discover what information is readily available through open source. After intensive searches, the biggest culprits of open information were Linkedin Accounts, unit Family Readiness Group websites, and Facebook. Linkedin and Facebook are self-explanatory–too much information and not enough personal security.

After the survey, KMID took away 25 investigative leads, two CI cases and eight FORMICA leads. KMID went from two CI leads to 25 in a matter of three weeks. The survey was a resounding success, taking a stagnant CI area and reinvigorating it. The success is a direct result of the methodical planning and focusing of all the detachment's organizational energy. CI detachments must focus the most effort on the personnel LOE, which far outweighed the cyber and physical lines given the number of leads generated. This single metric alone should indicate where most of the survey's organizational energy should go. Physical and digital LOEs were equally important in giving the holistic picture of a unit, but not so much in lead development. Refining the process, more interviews with more teams is necessary. Evasively snooping can only produce so many leads; the people are what matter most. In the end, despite doctrine or the lack thereof, or even a best practice, the three LOEs approach to a CI Survey worked exceedingly well in developing leads for the CI field office.

Endnotes

1. AR 381-10 U.S. Army Intelligence Activities, 3 May 2007. (Publication is unclassified.) AR 381-12 Threat Awareness and Reporting Program, 4 October 2010. (Publication is unclassified.) AR 381-20 The Army Counterintelligence Program, 25 May 2010. (Publication is classified.)

2. U.S. Army Intelligence and Security Command. *902d MI Group Investigations Handbook*, Fort Meade, Maryland, 20 June 2010. (Publication is classified.)

3. AR 381-20 The Army Counterintelligence Program, Chapter 13, 10 May 2010. (Publication is classified.)

4. Thomas Fingar, *Remarks and Q&A by the Deputy Director of National Intelligence For Analysis & Chairman, National Intelligence Council*, 18 March 2008, The Council on Foreign Relations, New York, New York.

CPT Miller is currently the Detachment Commander for the Kaiserslautern MI Detachment, 2d MI Battalion, 66th MI Brigade. The mission of the unit is to provide Title X support to Force Protection for the USAG Rhineland-Pfalz and provide FORMICA support to the tenant units of the garrison. Previously, he served as the Battalion S2 for 1-91 CAV, 173rd ABCT, Grafenwoehr, Germany.

Mr. Romero is currently the Special Agent in Charge of the Kaiserslautern Field Office under the Kaiserslautern MI Detachment, 2d MI Battalion, 66th MI Brigade. Previously, he was the Special Agent in Charge of the Livorno Field Office in Livorno, Italy.

Home-Station HUMINT Training: Columbia Sentinel

Chief Warrant Officer Three David Clark

The 502D Military Intelligence Battalion, Joint Base Lewis-McChord, Washington, has conducted three iterations of home-station Human Intelligence (HUMINT) training. Each exercise has served to validate this training model, and has identified different elements for improvement in later sessions. Columbia Sentinel currently stands as a 12-day, three-phase exercise, incorporating classroom instruction (crawl phase), practical exercises and mission preparation (walk phase), and mission execution (run phase). Students are divided into pairs and given direct mentorship by their Operations Officer (O/O), an experienced HUMINT collector. Columbia Sentinel Iteration Three brought the training regimen closer to a full operational cycle and incorporated operations management training, though it still requires further refinement to fully meet all of the training objectives.

The primary goal of realistic home-station Military Source Operations (MSO) training is to simulate a full HUMINT operational cycle. During iteration three, instructors were able to provide four days of personal meetings, an increase in comparison to previous exercises, and provided significant classroom and operational emphasis on Mission and Target Analysis (MTA). Students received two hours of MTA training during the classroom portion, and incorporated the lessons learned into all the operational acts that were performed during training.

However, Columbia Sentinel is still unable to convincingly simulate the earlier, developmental stages of the operations cycle based on the time constraints of the course. Three training days are devoted to classroom instruction, and the other four to practical exercises and mission preparation. Bringing the training to a full cycle would mean incorporating an additional two or three meetings, depending on the students' performance, and this is not feasible with the current time allotted. Extending the training by three to four training days could address this issue, but it may be difficult for company and battalion commanders to safeguard a 15- or 16-day exercise from external intervention.

The incorporation of operations management training into Columbia Sentinel resulted in a significant increase in training value for both the students and instructors involved in the exercise. HUMINT Collection Teams will not deploy or collect information without operations management through 2X channels, except in very specific circumstances. Bringing an Operational Management Team (OMT) into the training enabled a more realistic, battle-focused training event, and allowed the Exercise Control (EXCON) personnel to adjust the collection focus during the exercise without the heavy hand of scripted information.

Furthermore, OMT operations are difficult to train. While OMTs exist at multiple levels across the Army, there is no doctrinal reference on how to train the tasks for which these teams are responsible. During this iteration, senior intelligence personnel drafted training specifically related to operations management and continuously coached the trainees on best practices. Developing and implementing this kind of training significantly benefits the Battalion's warfighting function by addressing a critical shortfall. Most mid-career HUMINT Collector NCOs have not previously been prepared to assume oversight over their assigned collectors in accordance with the Battalion's mission. The OMTs were also able to consistently guide and refine the students' collection operations and focus through direct tasking and requirements–a critical task for any HUMINT-related enterprise.

The exercise also incorporated All-Source Intelligence Analysts into the OMTs as organic elements, arguably a practice that should be supported during both training and warfighting functions. The analysts participated in all of the training provided to HUMINT Collectors, allowing them to gain insight into the responsibilities of single-source collectors. As training progressed, analysts were able to smoothly integrate into the OMTs and provided support during both the preparation and execution phases of training. During the preparation phase, MOS 35F Soldiers were able to provide operational graphics, prepare analytical matrices, and evaluate the (minimal) dossiers provided to the students. Once the collectors began operations, the analysts reviewed and collated intelligence information, prepared link and event analysis diagrams, and developed summary analytical products to brief both students and EXCON personnel.

Even with these achievements, there is still significant room for Columbia Sentinel to grow for future iterations. A consistent complaint during mid-course and post-course after action reviews was that junior HUMINT Collectors had

not been given enough lead time to familiarize themselves with all of the doctrinal references related to the controlled MSO. This exercise was the first to prepare welcome letters for attendees, and future iterations will include these letters with the Operations Order authorizing the exercise, along with a list of references for prospective students to review.

The lack of operational dossiers has been referenced, but should be mentioned again as an area for improvement. Students were provided with a Notice of Intelligence Potential Report to initiate the exercise, but had no other documents to reference to prepare for the operation. While this is distressingly common in the operational world, this is not conducive to training. The dossiers and reports generated by the students during iteration three will be adapted into training aides for future exercises, allowing students to fully utilize the lessons taught during the MTA class, as well as increasing the realism of the exercise.

An additional aspect of realism for Columbia Sentinel would include an O/O-like mentor for the OMTs. The personnel assigned to the OMTs during this iteration did not possess the S1 or V4 Additional Skill Identifiers or their associated training, which limited their ability to successfully evaluate the tradecraft employed by the students. EXCON personnel were able to provide some input during the walk/preparation phase of training, but their other duties precluded significant involvement during the run phase of training. Dedicating a qualified mentor to the OMTs for the duration of the exercise would expand their effective management, further train OMT personnel on best practices, and provide a realistic, battle-focused element to home-station training.

Conducting live environment intelligence collection training is critical to preparing Soldiers, NCOs, and teams to execute their warfighter functions. Training events like Columbia Sentinel allow new collectors to prepare for advanced assignments and training, and provide certified leaders with the opportunity to exercise their skills. While the training is intense in both resources and time, it remains critical to Battalion readiness and preparation for future missions. Future iterations should move towards a full HUMINT Operational Cycle, and should continue to incorporate operations management as a student task, rather than defaulting to the EXCON.

CW3 Clark is currently assigned as a program manager with the High-Value Detainee Interrogation Group in Washington, D.C. Previously, he served as the senior HUMINT Technician for 502^{D} MI Battalion, where he oversaw training and implementation of HUMINT collection methodology. Mr. Clark is a graduate of the Source Operations Course, the Defense Strategic Debriefer Course, and has served multiple combat tours as an OMT Leader in Iraq and Afghanistan.

Doctrine Note. There are a number of doctrinal and collective training products that units can use to support their training. Army doctrine standardizes fundamental principles, tactics, techniques, procedures, and terms and symbols throughout the Army. Army doctrine forms the basis for training. Current doctrine on the HUMINT OMTs includes:

ATP 2-19.4 Brigade Combat Team–paragraphs 1-37and 1-38 Human Intelligence; 2-29 and 2-30 Human Intelligence Collection Platoon; 2-35 and 2-36 Information Collection Platoon.

FM 2-22.3 HUMINT Collector Operations–OMTs are discussed throughout this publication. A search reveals 109 references to the OMTs. Some highlights can be found in paragraphs 2-10 Operational Management Team, throughout Chapter 4, HUMINT Operations Planning and Management, 10-5 through 10-14 Source Administrative Reports, 10-16 through 10-18 Reporting Architecture, 12-45 through 12-51 HUMINT Source Selection

ATP 2-22.31, HUMINT MSO Techniques–This is a classified document.

ATP 2-22.33, 2X Staff Procedures and Techniques–This is a classified document.

These publications can be accessed through the Army Publishing Directorate at http://www.apd.army.mil

The Combined Arms Training Strategies (CATS) provides task-based event driven training strategies, designed to assist the unit commander in planning, and executing training events that enable the unit to build and sustain Soldier, leader, and unit proficiency in mission essential tasks. The CATS provide training events, frequency, and duration that a commander uses in developing unit training guidance, strategy, and calendars. CATS offers links to task selections, their supporting collective tasks, and their supporting individual task. CATS can be accessed for training through the Army Training Network at http://atn.army.mil/.

One example of a number of collective tasks covering the OMT is Task # 34-5-0222, Manage Human Intelligence (HUMINT) Collection Activities. CATS provides the task, conditions, and standards, along with lists (with links) to the supporting individual tasks, supported AUTL/UJTL tasks, and supporting collective tasks.

The Intelligence Center of Excellence acknowledges that finding the right information in CATS can be challenging, but with a small investment of time, the payoff can be well worth the effort. In a future MIPB article, we will explore in more detail how to navigate CATS.

For more information regarding doctrine and training development support, please forward your questions to usarmy.huachuca.icoe.mbx.doctrine@mail.mil.

The Military Intelligence Corps 2016 Hall of Fame Inductees

General Keith B. Alexander, U.S. Army, Retired

GEN Alexander, the Military Intelligence (MI) Corps' only four-star general, graduated from the U.S. Military Academy in 1974 and was commissioned a Second Lieutenant in Armor. His first experience in the MI field was as the S4 and Border Field Office Commander in the 511th MI Battalion, 66th MI Group, in Germany. In between advanced educational opportunities, he commanded at the company, battalion, and brigade levels, and served as the Assistant Chief of Staff, G2, of the 1st Armored Division during Operation DESERT STORM.

In the mid-1990s, while leading the Army Intelligence Initiatives Group, GEN Alexander built the digital battlefield visualization concept for enhanced situational awareness and planning. He later stood up the capability in the XVIII Airborne Corps and expanded it further while serving as the Deputy Director for Intelligence, J2, for the Joint Chiefs of Staff. Throughout the late 1990s, GEN Alexander served as the J2 for U.S. Central Command, providing predictive analysis on actions related to Iraq, Pakistan, Syria, Yemen, and the al Qaeda terrorist organization. In March 2001, he assumed command of the U.S. Army Intelligence and Security Command and steered its considerable efforts in Southwest Asia following 9/11. Appointed the Army's Deputy Chief of Staff, G2 in 2003, GEN Alexander directed the initial Joint Operational Capability-Iraq that evolved into the Distributed Common Ground System-Army, the all-source database automated system for processing and exploiting information for intelligence production.

His active military service culminated in his simultaneous assignments as the Director, National Security Agency (NSA), and Commander, U.S. Cyber Command. GEN Alexander's focus on enterprise architecture and advanced analysis markedly improved the processing, analyzing, sharing, and utilization of information for, and by, decision makers. During a time of rapid technological convergence,

he led the NSA and interagency efforts in identifying major threats to critical systems and establishing effective network defense. His leadership was invaluable in forging and implementing the Comprehensive National Cybersecurity Initiative and in the strengthening of collaborative ties between the Departments of Defense, Justice, and Homeland Security, the Intelligence Community, and private sector. Finally, one of GEN Alexander's most enduring contributions was the establishment of the U.S. Cyber Command, charged with defending the nation by planning, coordinating, conducting operations and defending the Nation and Department of Defense networks in cyberspace.

GEN Alexander retired in April 2014 after a 40-year career as one of the Army Intelligence's greatest leaders. His military awards and badges include the Defense Distinguished Service Medal, Army Distinguished Service Medal (1 Oak Leaf Cluster), Defense Superior Service Medal (1 Oak Leaf Cluster), Legion of Merit (4 Oak Leaf Clusters), Bronze Star Medal, Meritorious Service Medal (4 Oak Leaf Clusters), Air Medal, Army Commendation Medal (1 Oak Leaf Cluster), Army Achievement Medal (1 Oak Leaf Cluster), the Senior Parachutist Badge ,and the Joint Chiefs of Staff, Army Staff, U.S. Cyber Command, and NSA Identification Badges. GEN Alexander is also the recipient of the 2016 U.S. Military Academy Distinguished Graduate Award, given to graduates whose character, distinguished service, and stature draw wholesome comparison to the qualities for which West Point strives, in keeping with its motto: "Duty, Honor, Country."

Lieutenant General Richard P. Zahner, U.S. Army, Retired

LTG Zahner was commissioned a Second Lieutenant in Military Intelligence following his graduation from Cornell University as a Distinguished Military Graduate in 1976. His earliest assignments with the 82nd Airborne Division, Fort Bragg, North Carolina, included several key shaping positions during the transition of Army Intelligence to the Combat Electronic Warfare and Intelligence force structure. He was also a "plank-owner" of the Joint Special Operations Command, for which he developed tactics, techniques, and procedures and identified, acquired, and integrated leading edge technology to drive the intelligence process and battle rhythm.

Throughout the 1990s and into the 21st century, LTG Zahner served as an intelligence staff officer at division, Corps, theater, and national levels and commanded the 102nd MI Battalion and the 525th MI Brigade (Airborne). Throughout this period, he developed new systems and procedures to deal with the new intelligence challenges of the Balkans, illustrating the forward thinking innovation that proved significant in the post-9/11 period. During the early years of Operations ENDURING FREEDOM and IRAQI FREEDOM, while Assistant J2 for U.S. Central Command, LTG Zahner significantly changed how the Army developed, processed, and disseminated intelligence in a counterinsurgency environment. He continued to provide exceptional support to both Multi-National Forces, Iraq (MNF-I) and NATO in Afghanistan while serving as J2 for the U.S. European Command and C2 of MNF-I. He designed and established NATO's first Intelligence Fusion Center as well as the intelligence structures of Iraq's Ministry of Defense, Ministry of Interior, and Border Force.

Following eight months as the Director of Signals Intelligence, National Security Agency, LTG Zahner was hand-picked by the Secretary of Defense to serve as Deputy Undersecretary of Defense for Intelligence and Warfighting Support. He led the Intelligence, Surveillance, and Reconnaissance Task Force in its first year; helped build the initial concept design for U.S. Cyber Command; restructured intelligence elements of ten Combatant Commands into a common support core with tailored analytic capabilities; and redrafted policy charters of each DoD Intelligence Agency. During his subsequent assignment as the Deputy Chief of Staff, G2, Department of the Army, he not only pushed for critical improvements in intelligence architecture and analysis for the warfighter but also built on his predecessor's efforts to "rebalance" the MI force structure and systems to address the realities of a changed conventional and asymmetric threat environment.

LTG Zahner retired in 2012 after a lifetime of exceptional achievement and contributions to Army Intelligence. During his distinguished 36-year career as a U.S. Army officer, he received the following awards and badges: the Defense

Distinguished Service Medal, Distinguished Service Medal, Defense Superior Service Medal (3 Oak Leaf Clusters), Legion of Merit (3 Oak Leaf Clusters), Bronze Star Medal, Defense Meritorious Service Medal, Meritorious Service Medal (3 Oak Leaf Clusters), Joint Service Commendation Medal, Army Commendation Medal (1 Oak Leaf Cluster), Joint Service Achievement Medal, Army Achievement Medal, Parachutist Badge, Ranger Tab, Office of the Secretary of Defense Identification Badge, and the Army Staff Identification Badge.

Colonel Terrance M. Ford, U.S. Army, Retired

COL Ford entered the Army through the ROTC program at The Citadel in 1970. He served in a number of counterintelligence (CI) and other assignments in Germany, Korea, and the U.S. throughout the 1970s and early 1980s. Much of his career was spent in Germany where his comprehensive expertise in Soviet Union military tactics and doctrine was instrumental to U.S. activities during the Cold War. While serving in Germany, he commanded the 766th MI (CI) Detachment, the 302nd MI Battalion, and the 66th MI Brigade. He also served as the Regimental 2, 2nd Armored Cavalry Regiment, G2, 1st Infantry Division, during Operation DESERT STORM; and J2 of Joint Task Force PROVIDE PROMISE, a humanitarian relief effort in the former Yugoslavia.

In 1995, COL Ford became the Deputy Chief of Staff, U.S. Army Europe and 7th Army. He was the key proponent in developing and integrating MI doctrine, organizations, and systems in the initial phases of the Balkan crisis. His keen insights proved invaluable in providing senior leaders with the best intelligence in support of tactical operations. He also facilitated the transition of U.S. Army Human Intelligence units and personnel to the Defense Intelligence Agency (DIA) and initiated a reorganization of CI assets to compensate for the significant reduction of such assets in theater.

COL Ford next served as Executive Officer to the Director of the DIA, followed by duty as the Staff Director for Operations, DIA. He played an active role in identifying and generating discussion about future threats, opening new Defense Attaché offices in Southeast and Central Asia and Africa, and guiding DIA through several global security challenges. During his tenure, DIA received its fourth Joint Meritorious Unit Award and the Killian Award, the latter given by the President's Foreign Intelligence Advisory Board for the organization's efforts on foreign intelligence activities critical to national security. COL Ford was also instrumental in the formation of the Defense Alumni Association.

COL Ford concluded his active duty career in 1998 after almost 29 years of service and continued to contribute to Army Intelligence as an Army Civilian. As a member of the Defense Intelligence Senior Executive Service since September 1998, Mr. Ford served as the Vice and Acting Director for Operations, Defense HUMINT Service, and for six years, he served as the Army's Assistant Deputy Chief of Staff for Intelligence. In 2008, Mr. Ford was the Army's nominee, and subsequently selected, to serve as the first J2/Director of Intelligence and Knowledge Development, U.S. Africa Command. Currently, he serves as the National Intelligence Manager for Africa at the Office of the Director of National Intelligence.

COL Ford's military awards and badges include the Defense Superior Service Medal, Legion of Merit (2 Oak Leaf Clusters), Bronze Star Medal, Defense Meritorious Service Medal, Meritorious Service Medal (2 Oak Leaf Clusters), Army Commendation Medal (5 Oak Leaf Clusters), Joint Commendation Medal, Army Achievement Medal, and the Parachutist Badge. His civilian awards include three Presidential Rank Awards (two Distinguished and one Meritorious), the Joint Distinguished Civilian Service Award, the U.S. Army Award for Exceptional Civilian Service and two DIA Director's Awards.

Chief Warrant Officer Three Brian K. Bounds, U.S. Army, Retired

CW3 Bounds enlisted in the U.S. Army in 1986 and first served as an Intelligence Analyst providing support to the 82nd Airborne Division for several contingency and operations plans. In 1990, then Sergeant Bounds was reassigned to the Intelligence and Electronic Warfare Test Directorate at Fort Huachuca, where he conducted operational testing of Signals Intelligence collection and exploitation tools. He next spent three years as the Senior Analyst for C Company, 1st Battalion, 10th Special Forces, in Germany, after which he attended the Warrant Officer Candidate Course.

In 1990, he was assigned to Fort Hood as the All-Source Intelligence Technician in the III Corps MI Support Element. His responsibilities included intelligence support to deep operations, integration of Special Operations Forces into conventional operations and Corps-level targeting through conventional and unconventional means. Additionally, he led the development of automation tools that significantly reduced the time required to develop a consolidated intelligence picture.

In 1997, Bounds was selected for assignment as the All-Source Intelligence Technician for the 75th Ranger Regiment. By automating existing capabilities, he produced quicker and more accurate intelligence assessments used by the Regimental staff and command in their decision making processes. Mr. Bounds left Fort Benning in 2000 when he was hand selected for assignment to the Joint Special Operations Command (JSOC). His primary responsibility was the development of targeting techniques and technology insertions for use in the joint SOF community, particularly during the early execution stages of Operations ENDURING FREEDOM and IRAQI FREEDOM.

With the sponsorship of the Undersecretary of Defense for Intelligence, Mr. Bounds formed a study team of experts from across the Intelligence Community to resolve issues of policy, technology, organizational practices, governance, and resource constraints that limited the sharing of critical information. More than 180 interviews with MI professionals working in Iraq and Afghanistan identified 300 specific issues that hindered the ability to share information effectively. Recommendations from this study resulted in significant improvements in theater-wide information reporting and repository strategies, education and training processes, and communications architectures capable of supporting an effective information-sharing environment. As a result, tactical reporting that previously took days to reach battle space owners was reduced to minutes or hours. These efforts to expand intelligence support by improving collaboration tools and procedures for more effective planning and decision making processes were a hallmark of Mr. Bounds' career.

CW3 Bounds concluded 20 years of military service in 2006 and has been a Department of Army Civilian at JSOC for the past eight years. His military awards and badges include the Legion of Merit, Bronze Star Medal (1 Oak Leaf Cluster), Meritorious Service Medal (3 Oak Leaf Clusters), Army Commendation Medal (2 Oak Leaf Clusters), Army Achievement Medal (3 Oak Leaf Clusters), the Good Conduct Medal (3 awards), and the Parachutist Badge.

Command Sergeant Major Gerardus F. Wykoff, U.S. Army, Retired

CSM Jerry Wykoff began his enlisted military career in December 1983 and joined Military Intelligence in 1988 as a Ground Surveillance Radar Operator assigned to the 102nd MI Battalion in Korea. He had subsequent assignments as a Team Leader, Squad Leader, Platoon Sergeant, and First Sergeant in Germany and at Fort Campbell, Kentucky.

In 2003, during Operation IRAQI FREEDOM 1, then-Master Sergeant Wykoff served as the Chief of the 501st MI Battalion's HUMINT Operations Cell, controlling 18 Tactical HUMINT Teams operating in Baghdad. The intelligence his cell produced directly contributed to the capture of more than 25 top-ranking Iraqi officials. After graduating from the Sergeants Major Academy, he returned to Iraq as the Command Sergeant Major of the Brigade Troops Battalion, 2nd Brigade, 101st Airborne Division. Command Sergeant Major Wykoff personally established the first Iraqi NCO training course in the Southern Baghdad Area of Operations. Additionally, his own performance was reflected in the remarkable record of his Soldiers, who received 343 combat awards during the deployment.

After developing realistic and relevant training for MI Soldiers while serving as the 111th MI Brigade Command Sergeant Major, CSM Wykoff became the MI Corps Command Sergeant Major in 2007. In addition to advising on all matters concerning the 40,000 enlisted Soldiers within the MI Corps, CSM Wykoff conducted leader circulations to active and reserve MI units worldwide, providing a source of great inspiration and essential information to MI Soldiers across the Army. His tactical and operational experience, coupled with his drive and passion for training, were instrumental in shaping the MI Corps of today and tomorrow.

To improve intelligence support to deployed commanders in theater, he assisted in the development and execution of a 48 week Arabic immersion course at Fort Huachuca for linguists, the creation of tactical overwatch Geospatial Intelligence training, and the first implementation of unmanned aerial vehicles in combined live fire exercises for students, making the the U.S. Army Intelligence Center of Excellence the only school in the U.S. Army Training and Doctrine Command conducting this type of realistic training. His commitment to the professional development of MI Soldiers was obvious in his personal involvement in the Sergeant Audie Murphy Club, the accreditation of the Noncommissioned Officers Academy as an Institution of Excellence, and improvements to the qualifications and training of MI Soldiers supporting commanders across the Army. In addition to his dedication to U.S. Army Soldiers, CSM Wykoff assisted his counterparts in Israel, Jordan, Japan, and Romania in establishing NCOA-equivalent schools to further develop their professional education system.

CSM Wykoff retired from the US Army in June 2010, concluding 26 years of leadership and unwavering dedication to Soldiers and their Families. His awards and badges include the Legion of Merit, Bronze Star (1 Oak Leaf Cluster), Meritorious Service Medal (2 Oak Leaf Clusters), Army Commendation Medal (5 Oak Leaf Clusters), Army Good Conduct Medal (6 awards), and the Parachutist, Air Assault, and Combat Action Badges.

MILITARY INTELLIGENCE CORPS
HALL OF FAME

The MI Hall of Fame Nomination Process Has Changed

The Military Intelligence (MI) Corps established the Hall of Fame in 1988, a year after the activation of the Corps itself. The Hall of Fame honors those individuals who have made a significant or enduring contribution to the MI profession. Commissioned officers, warrant officers, enlisted Soldiers, and professional Civilians who have served in a U.S. Army intelligence unit or intelligence position are eligible for nomination after they have been separated or retired for two years. Including the Class of 2016, 254 MI professionals have been inducted.

Since 1988, few changes have been made to the nomination process. However, beginning with the 2017 Nomination Board, which will meet in November 2016, the requirements for nominations have been streamlined and standardized, and the procedures for the Board have changed substantially.

To nominate an individual for the Hall of Fame, the following materials must be submitted:

a. Standardized one-page nomination letter that includes a paragraph of no more than 150 words stating succinctly the justification for the nominee's inclusion in the Hall of Fame.

b. Standardized career biography.

c. Narrative justification, totaling no more than two pages, that outlines the key accomplishments of the nominee that warrant induction into the Hall of Fame and his/her impact on the Army and MI.

d. Photograph of the nominee.

Endorsement letters are also encouraged, but not required, and are limited to three, each of which should be no more than one page in length. All materials submitted should be unclassified, although a classified addendum will be accepted in special cases.

Nomination Board Members will now review five separate categories of nominations: General Officers, Officers, Warrant Officers, Enlisted, and Civilian. Specifically, Board Members will evaluate, on a scale of 1 to 5, the nominee's significant and/or enduring contribution to military intelligence *commensurate with his/her grade or rank*, whether based on documented sustained service or on heroic actions/valorous awards. Consequently, nominators should ensure their narrative justification directly addresses the following six evaluation criteria:

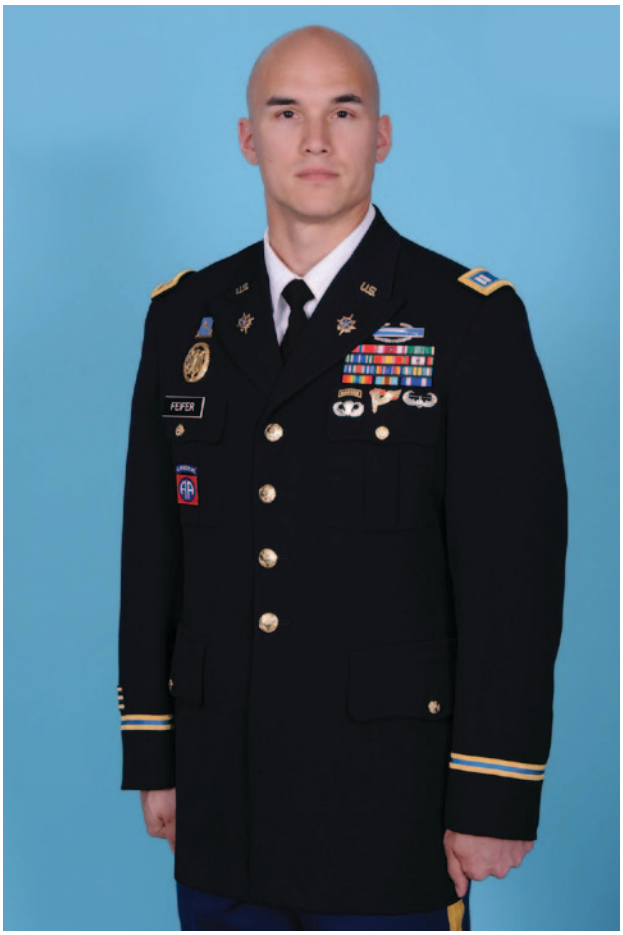
1. Significant documented contributions.
2. Sustained superior performance.
3. Accomplishments far exceeding grade/rank.
4. Inspirational leader.
5. Impact of accomplishments on the MI Corps.
6. Enduring nature of accomplishments.

The new nomination requirements and Board procedures standardize the process and provide for a more measurable and equitable evaluation of what constitutes a "significant or enduring contribution" for all grades and ranks.

Additional details about the nomination requirements and Nomination Board procedures, as well as the standardized formats for nomination letters and career biographies, can be found on the Hall of Fame website: https://www.ikn.army.mil/apps/MIHOF/Home, or by contacting the Board Recorder at lori.s.tagg.civ@mail.mil.

Captain Joseph E. Feifer
2016 Recipient
LTG Sidney T. Weinstein Award
For Excellence in Military Intelligence

The MI Corps created the Lieutenant General Sidney T. Weinstein Award in 2007 to honor the accomplishments of the "Father of Modern Military Intelligence." LTG Weinstein was not only a fine officer; he was a mentor, a role model, a friend to many, and a dedicated family man. This award is given annually to one MI Captain who, through his or her actions, demonstrates the values and ideals for which LTG Weinstein stood: Duty, Honor, and Country.



CPT Joseph E. Feifer was commissioned as an Infantry officer through the Reserve Officer Training Corps after graduation from the University of San Francisco in 2008. Following his completion of the Infantry Basic Officer Leader Course and the U.S. Army Ranger Course at Fort Benning, Georgia, he was assigned to 1st Battalion, 327th Infantry Regiment, 101st Airborne Division (Air Assault) as a Battalion Assistant S3. He then deployed to Kunar Province, Afghanistan, where he served as a Rifle Platoon Leader in support of Operation Enduring Freedom XI from May 2010 to April 2011.

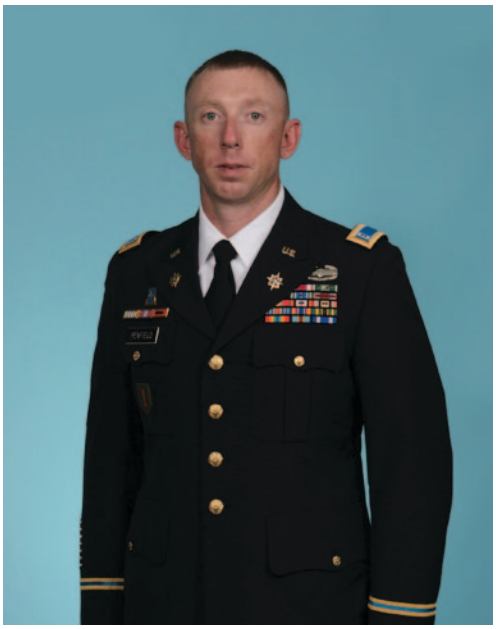
After completing the MI Officer Transition Course and the MI Captains Career Course in December 2012, CPT Feifer was assigned to 3rd Brigade Combat Team, 82nd Airborne Division, as the Brigade S2X and Assistant S2. He finished a yearlong Global Response Force rotation in November 2014 and was selected to serve as Commander of the MI Company, 307th Engineer Battalion (Airborne). On short notice, he rapidly deployed his company to Iraq in support of Operation Inherent Resolve from January through September 2015.

CPT Feifer's Soldiers constituted the primary workforce within the Panther Brigade Intelligence Support Element and SIGINT Support Element at Camp Buehring, Kuwait, as well as providing unmanned aircraft system (UAS) support in Al Anbar province, and all conventional Counterintelligence and Human Intelligence in Iraq. CPT Feifer enhanced the intelligence support capability of his company by advising the brigade's Senior Intelligence Officer on the strategic placement of his Soldiers throughout the battlefield. As a result, his Paratroopers were deployed to six geographically separated locations across the Combined Joint Task Force–Operation Inherent Resolve area of responsibility (AOR), as well as an analytical cell in Fort Bragg, North Carolina.

Assuming the dual mantles of Assistant Brigade Combat Team S2 and Lead Intelligence Planner, CPT Feifer orchestrated the Brigade's intelligence production cycle. He directly contributed to the inception of the Brigade Social Media Analysis and Exploitation Cell and the production of over 200 daily intelligence updates socialized with the broader Intelligence Community and Commanders across the AOR. CPT Feifer's UAS Platoon provided more than 5,000 hours of near-real time full motion video coverage in 580 sorties over two provinces and was the first to conduct simultaneous target designation for multiple target engagements. CPT Feifer's expertise in fusing human, signals, geospatial, and open source intelligence generated a holistic view of the operational environment that fundamentally informed strategic decision making processes and shaped U.S. foreign policy.

CW2 David S. Penfield
2016 Recipient
CW5 Rex A. Williams Award
For Excellence in Military Intelligence

The MI Corps established the Chief Warrant Officer Five Rex A. Williams Award in 2016 to recognize the outstanding achievements of a Company Grade Warrant Officer (WO1-CW2) within the MI community. This award is named in honor of an icon in MI, who spent his 31-year military career improving training, mentoring countless Soldiers, and helping define the foundations of intelligence analysis. CW5 Williams also served as the first Chief Warrant Officer of the MI Corps. He continues to serve the MI Corps as a Department of Army Civilian.



CW2 David S. Penfield joined the Army as an Intercept, Electronic Warfare Systems Repairer (MOS 33W), in 1999 after graduating high school. He completed an Associate's Degree in Applied Science through Cochise College in March 2016. His military education includes Unmanned Aerial Vehicle Electronic Maintenance Specialist Course in 2004, multiple MI Systems Maintenance courses, MI Systems Maintainer/Integrator Basic Noncommissioned Officer Course in 2008, Warrant Officer Candidate School in 2009, MI Warrant Officer Basic Course in 2009, and the MI Warrant Officer Advanced Course in 2015.

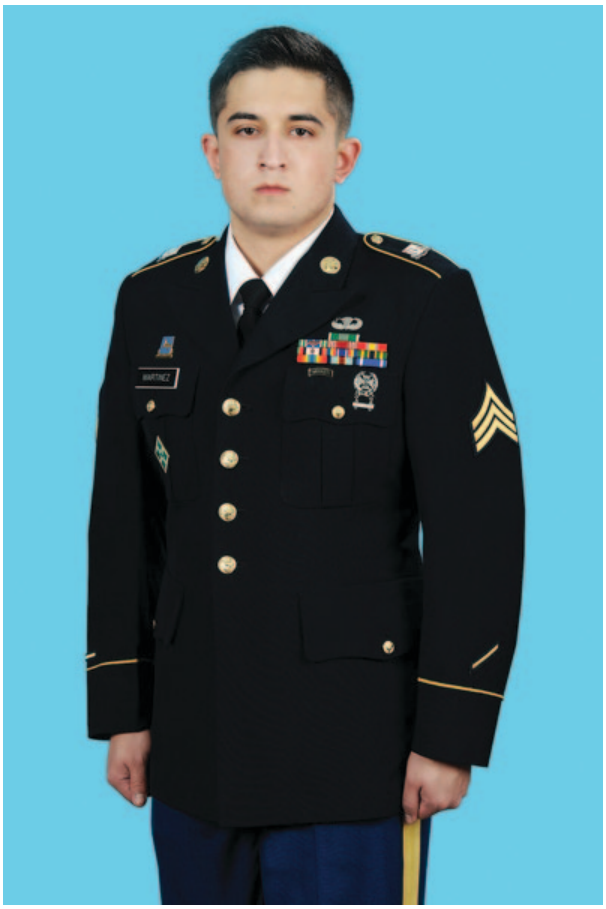
CW2 Penfield is currently the Intelligence Systems and Maintenance Technician (MOS 353T) for D Company, 65th Brigade Engineer Battalion, 2nd Stryker Brigade Combat Team (BCT), 25th Infantry Division (ID). His other assignments include: MI Systems Maintenance/Integration Technician, Bravo Company, 4th Brigade (BDE) Special Troops Battalion, 4th Infantry BCT, 1st ID with one deployment to Iraq in support of Operation Iraqi Freedom (OIF) and one deployment to Afghanistan in support of Operation Enduring Freedom (OEF); UAS Maintenance Platoon Sergeant, Alpha Company, 224th MI BDE, deployed in support of OIF; Information Processing Facility Maintenance Squad Leader, Bravo Company, 224th MI Battalion, 525th MI BDE which was reflagged under the 513th MI BDE during his assignment; Senior Intercept/Electronic Warfare Systems Maintainer/Repairer, Bravo Company, 165th MI Battalion, 205th MI BDE, deployed to Afghanistan with CTF Bayonet, 173rd Airborne Infantry BCT support of OEF; MI Systems Maintainer/Integrator, 66th MI Company, 3rd Squadron, 3rd Armored Cavalry Regiment, deployed in support of OIF and Operation BRIGHT STAR.

In 2014, CW2 Penfield deployed with the 2nd Stryker BCT during its rotation to the National Training Center (NTC) where he enabled the entire BCT to be the first rotational unit to fully integrate and employ the Distributed Common Ground System-Army (DCGS-A) in a Decisive Action Training Environment scenario. He set a new standard for the BCT and the NTC in the rapid sharing of intelligence information across a distributed battlespace against a highly dynamic and well-equipped threat. He coordinated maintenance support across the BCT's area of operations and assisted NTC with the generation of a DCGS-A pre-execution checklist. His techniques for employing and supporting DCGS-A during NTC were documented as best practices by the U.S. Army Intelligence Center of Excellence (USAICoE) Lessons Learned Team.

CW2 Penfield then pioneered a revolutionary DCGS-A architecture that made the infamously complicated system more user friendly with less maintenance support requirements. His architecture simplified and expedited the DCGS-A network between the lower echelons and the Brigade Intelligence Support Element's Intelligence Fusion Servers thus enabling the BCT to distribute an unprecedentedly complete common operating picture with other Army Battle Command Systems during Lightning Forge 16-01, a division-level exercise in the Hawaiian Islands. CW2 Penfield has been recognized by the 25th ID and I Corps Commanding Generals and sought by BCTs across the Army for his expertise on DCGS-A architecture and employment. Yet again, CW2 Penfield's tactics, techniques, and procedures for employing DCGS-A during Lightning Forge were documented by USAICoE's Lessons Learned Team. Simultaneously, he kept the BCT at a high state of readiness to react as a deployable contingency unit within the U.S. Pacific Command area of responsibility.

Sergeant Matthew T. Martinez
2016 Recipient
CSM Doug Russell Award
For Excellence in Military Intelligence

The Command Sergeant Major Doug Russell Award was created in 2001 in honor of an esteemed Noncommissioned Officer who personified the integrity, moral courage, and loyalty espoused in the NCO Creed. CSM Russell served in uniform for 32 years, followed by 14 years as the Director of NCO and Enlisted Affairs, Director of Retiree Activities in the Association of the U.S. Army, and President of the American Military Society. The award is presented annually to an outstanding Soldier in the rank of Sergeant or below, who has made a significant contribution to the MI Corps.



SGT Matthew Martinez enlisted into the U.S. Army as a Human Intelligence (HUMINT) Collector (MOS 35M) in August 2010. After completing Basic Combat Training and the HUMINT Collectors Course, he was assigned as a HUMINT Collector to A Company, 2nd Special Troops Battalion, 2nd Brigade, 4th Infantry Division. As a Private First Class, he deployed to Kandahar Province in support of Operation Enduring Freedom from July 2011 to May 2012. While deployed, he served in a noncommissioned officer (NCO) position as a reports officer for an Operational Management Team and as a HUMINT Collector on a HUMINT Collection Team. After the deployment, SGT Martinez attended the Basic Leader Course, serving as the class Platoon Sergeant and earning the Commandant's List.

After completing his assignment with 4th Infantry Division, SGT Martinez reenlisted for Airborne School, with a follow-on assignment as a HUMINT Collector in the MI Company, 54th Brigade Engineer Battalion (Airborne), 173rd Infantry Brigade Combat Team (Airborne). Since May 2013, SGT Martinez has served as a Team Leader and Squad Leader and has led HUMINT Collectors in exercises in Germany, Slovenia, Italy, and Spain. He completed the Source Operations Course at Fort Huachuca, Arizona, in 2014, and then graduated from Ranger School in January 2015, the first NCO from the company to earn the coveted Ranger Tab.

In April 2015, SGT Martinez was chosen to initiate the first ever HUMINT mission of its kind in Ukraine. He led his HUMINT Collection Team to overwhelming success, providing U.S. and NATO commanders with pertinent information about the Ukrainian conflict with Russian and Russian-led Separatist Forces.

Simultaneously, as part of a multi-national training force, SGT Martinez worked closely with the 1-91st Cavalry Regiment (Airborne) S2 to facilitate interoperability among U.S., Ukrainian, Canadian, Lithuanian, and British forces. He provided advice on the best training methods and assisted in developing the first doctrine and training aids for Ukrainian counter-unmanned aerial vehicle training. His efforts undoubtedly contributed to the survivability of Ukrainian National Guard Soldiers.

After returning from Ukraine and graduating the Defense Strategic Debriefing Course, SGT Martinez developed and provided training on tactical questioning and detainee operations for the Soldiers of the 2-503rd Infantry (A), 173rd IBCT (A). Finally, at the end of 2015, SGT Martinez was selected to support the Joint Military Training Group–Ukraine to train the Ukrainian Ministry of Defense Army and to forge new ground for HUMINT operations in Ukraine. SGT Martinez's dedicated service in 2015 not only contributed to the success of his unit's mission, but also furthered the objectives of the European theater and the strategic mission of the U.S. Army as a whole.

USAICoE Initiatives in Botswana

by Captain Nathan Hogan and Chief Warrant Officer Three Charles Davis

Originally known as Bechuanaland and split as northern and southern regions, Botswana was governed in the north by Great Britain and in the south by Cape Colony. The country was unified (north and south) by an act of British Parliament in 1965 and formally recognized as Botswana in 1966. The new country chose to focus on economic stability and population welfare during its first decade, not establishing a national military until 1977.

Photo credit: CW3 Davis

In March 2015 we began contributing to the development of this exceptional organization. Small, compared to the leading militaries in the world, Botswana is organized as a National Defense Force (BDF) with ground, air, and defense logistics forces under one primary command instead of distinct services. The BDF's mission is *to defend the country and provide for the security of Botswana, participate in external security cooperation activities, and contribute in domestic support operations*.[1] The U.S. maintains strong relationships with Botswana and is a principal contributor to officer education, providing U.S. training initiatives for numerous leaders each year. This effort also includes sending training support teams to Botswana, providing us with a unique once in a lifetime opportunity.

In March 2015 the U.S. Army Intelligence Center of Excellence (USAICoE) was tasked with developing and ultimately instructing a four-week Advanced Tactical Intelligence Course (ATIC). The process involved developing a scope of training, which would build on the BDF's Basic Intelligence Course, already in its fourth year of implementation. After many planning meetings at Fort Huachuca and two trips to Botswana, USAICoE had a pilot program approved and ready for execution.

The BDF, during our final planning meeting, maintained three priorities for this advanced training. They wished to focus on critical thinking, briefing skills, and developing the students' writing capabilities. The BDF hoped to accomplish this through cornerstone courses on Critical Thinking, the Military Decision Making Process, Small Unit Tactics, and Advanced Analytics.

As we began to work through a schedule, which included requirements for tea in the morning and afternoon, CW3 Davis reflected on his time with 4/3ID and how the S2 Section approached Soldier development for our Afghanistan deployment. To teach PMESII, ASCOPE, and Critical Thinking, the Vanguard Fusion Cell decided to develop country studies over several months, compartmentalized into the PMESII factors. He remembered this process provided many discussions, driving the critical thinking of the young Soldiers.

To organize the BDF instruction in a similar manner, the training team broke the class into small groups, each with their own country focus. This approach was particularly useful as the Director of Defense Intelligence's staff provided several areas of concern and interest that the students could use to develop their knowledge. Organizing the groups this way also proved extremely effective in generating analytic discussion and aided in small group exercises, which included current events briefings and storyboard development in each group's focus area.

During the first days of training, we focused on briefing skills, research, and writing techniques. While the majority of the officers had personal computers and were familiar with internet tools, a number of the NCOs had limited exposure to data mining in this manner. However, within the small groups, they were able to develop one another, and we were particularly pleased with the level of commitment officers displayed towards the success of the NCOs. Having worked towards the development of MI elements in Iraq and Afghanistan, it was refreshing to see the unity of effort within the BDF.

In an effort to include critical thinking within the writing portion of the course, the training team introduced students to position papers. Utilizing this writing tool provided many opportunities to discuss topics of value and importance to the soldiers, the Defense Force, and Botswana. Students were required to reflect on issues they felt could be resolved or processes which might be enhanced, then develop their own position papers on the topic. Discussions included integration of women into their military, which began in 2009 (first with officers) and is now well underway. The 25 final papers included topics such as the need for formal PT uniforms, development of translators and interpreters within MI, illegal immigration across Botswana borders, personnel shortages in key counter-poaching areas, and the controversial (in Botswana) gay rights issue.

Reviewing these papers has been an interesting lesson in the similarities between our two countries. BDF is dealing with repeated deployments (to their counter-poaching compounds). They are struggling with meeting training requirements during these rotations. The BDF is going through an integration period with their female service members. The country is addressing the issue of gay and lesbian rights, while also confronting illegal immigration issues from the surrounding nations. As the training team reviewed the student assessments of the problem and recommended solutions, we wondered why we had not seen more opportunities to address our own issues. While service members in the U.S. Army are inundated with survey after survey, we are seldom encouraged to develop assessments and recommendations on prevailing issues that affect us all.

Photo credit: CW3 Davis

There were numerous opportunities for discussions with BDF officers and NCOs. We had opportunities to meet and speak with several senior members of the BDF and met the President of the Republic of Botswana, His Excellency Lieutenant General Dr. Ian Khama, while receiving instruction at the BDF Snake Park. The park provides soldier orientation training for bush life and includes education on a number of the most poisonous snakes in the world.

Snake Park might suggest this training is oriented to the snakes only; that would be a serious error in judgment. We were introduced to the typical African lion, white lions, hyenas, wild dogs, and leopards. It was an exceptional lesson in professional training, which occurs at the BDF National Headquarters. The highlight of this opportunity was watching His Excellency interact with the predators, demonstrating his devotion to their protection and reinforcing why counter-poaching operations remains one of his top priorities.

The training team was informed from the outset that the strategic concern for the Botswana government and consequently the BDF is the preservation of natural resources in the form of wildlife. According to current figures, poaching is the fourth largest international criminal enterprise. Botswana sees this as a threat to national economic survival. In an effort to avoid 'mirroring' and ensuring that the ATIC, which is to become a standing BDF course, be relevant to the BDF, the team took steps to ensure they understood the primary deployment concerns of BDF Intelligence.

In order to better understand their concerns and increase the training team's knowledge to develop practical exercises that were applicable to the class, the team conducted terrain association walks and watched anti-poaching operations. By observing Preserve Park rangers and BDF personnel, we were able to experience the tracking and confirmation process utilized to account for the small rhino population at Mokolodi Preserve, just outside Gaborone. The team participated in two such events, tracking and counting white rhinoceroses. So far, the reserve has not had a poaching incident due to its proximity to the capital city and its smaller size, when compared to the larger parks to the north and along the borders. These trips gave insight into terrain, tactics (both BDF and poachers), missions, and end-states of all parties, the population's concerns.

On one of our weekends, the training team conducted the initial assessment of a potential staff ride for future courses. The BDF does not have this practice. However, when the BDF MI director of training and an accompanying senior NCO instructor spent a week at Fort Huachuca, they participated in a staff ride to Fort Bowie with MI Captains Career Course students, in order to reinforce Intelligence Preparation of the Battlefield/Battlespace and Mission Command principles. This sparked interest in establishing a staff ride within the new BDF ATIC.

Upon study, the training team looked at two major wars fought in Southern Africa, which would have appropriate battlefields to provide excellent researchable engagements, and which would reinforce multiple elements learned within ATIC. These were the Zulu and the Boer Wars. The closest major engagement area was Mafeking (Maheking) South Africa, the site of a 219-day siege between the British holding the town and the Boers who had encircled it. The training team spent a day with the MI Director of Training,

(Continued on page 72)

Intelligence Lessons and Best Practices from Multinational Operations

by Mr. Chet Brown, Chief, Lessons Learned

In keeping with our penchant for providing a Top Ten List and in support of this MIPB issue's theme, the U.S. Army Intelligence Center of Excellence (ICoE) Lessons Learned Team offers this Top Ten Lessons and Best Practices (L&BP) collected from multinational operations. We hope this list will assist you in planning and conducting training and operations. Some of the enduring challenges identified in operating within a multinational force can be mitigated by effective planning. You must first be aware of the challenges before they can be addressed in your plans, the benefit intended by this month's Top Ten column.

A secondary benefit of providing you with L&BP is to overcome the paradox created by simultaneously imposing the principle of "Train as you will Fight"[1] and the Joint doctrine declaration that "U.S. commanders should expect to conduct military operations as part of a multinational force (MNF)."[2] There are few opportunities in which U.S. Army forces are able to train in peacetime with all of the foreign partners with whom they'll operate as part of an MNF.

As you review the L&BP please know the challenges and concerns of MNF information sharing and interoperability are not limited to the intelligence warfighting function. What you may glean from this column can be informative to others in your organization. Joint Publication 3-16 Multinational Operations provides additional insights to consider when planning and conducting multinational operations. Another valuable reference of MNF lessons is the Center for Army Lessons Learned Handbook No. 15-17 Commander's Guide to Multinational Interoperability, published in September 2015.

The most important lesson in preparing to operate within an MNF is to understand the concept of the operation (CONOP) your unit will employ to share information and intelligence with the MNF members. Information and intelligence are not interchangeable terms when describing how U.S. forces will inform, and be informed by, differing MNF members. Army Regulation 380-10 Foreign Disclosure and Contacts with Foreign Representatives, provides policy and procedures for disclosing information to our foreign partners. An important distinction intelligence professionals should know is the difference between Information Security classification and Foreign Disclosure (FD) procedures. AR 380-10 provides more information on this subject. When in doubt, it's always best to seek guidance from your unit's respective Information and Operations Security Officers, and Foreign Disclosure Officer (FDO) or Representative.

Top Ten Multinational Operation Lessons and Best Practices of U.S. Forces

1. Every intelligence production section should have at least one trained and certified Foreign Disclosure Representative (FDR). Having an FDR in each section provides an immediately available resource to provide guidance in, and approval of, sharing information and intelligence with MNF members. Multiple sections with FDR qualified personnel provide a necessary redundant FDR capability to the overall organization when the primary FDR is unavailable. Each section's FDR personnel are very useful in determining how best to resolve the impact on the FD process as information moves (analog or digital) from one section to another.

2. Integrate the FDO process into collective training events. ICoE LL collection and unit-provided after action reports indicate FD challenges may have been mitigated if the unit rehearsed FD procedures during collective training prior to operations. Applying lessons learned of the value of FD trained personnel, several brigade combat teams, and MI elements ensured a sufficient quantity of personnel were trained and certified as FDO/FDR to oversee the unit's FD process. An additional lesson was learned upon beginning MNF operations when the units realized they were neither prepared to process the type and volume of information nor immediately proficient in the specific personnel and automation system tasks required to conduct the FD process. All personnel who shared these lessons with us believed the problems would have been mitigated, if not eliminated, by

incorporating the FD process in Home Station collective or pre-mission readiness/certification training exercises.

3. Clearly describe in unit standard operating procedures (SOP) or tactical SOP (TACSOP) the role and responsibilities of unit FDO/FDR personnel. Specifying who is responsible for what and when in the FD process is the beginning of an effective MNF information sharing strategy. Describing the roles and responsibilities of FDRs in each section allow one to identify specified and implied FD tasks required for the section to perform its respective function. Collective training events are particularly useful in discovering problems, challenges, techniques and procedures that are not always evident when drafting an SOP. Collective training assessments may validate the sufficiency of the unit's FD CONOP or identify additional challenges requiring action.

4. Identify any existing (pre-dating the MNF formation) intelligence sharing agreements or treaty requirements the U.S. may have with individual MNF members. You may not have to start from scratch, or unilaterally develop, a FD CONOP. There may already be a FD process or agreement in place you can use or tailor.

5. Identify, establish, train, and rehearse using the digital and/or analog systems to be used in sharing information and intelligence with MNF partners. A best practice is to identify as early as possible the manner and mechanisms with which the information will be shared within the MNF. An additional best practice in maintaining an efficient FD process is to train and practice using "Write for Release" techniques. Do not assume information sharing procedures for one MNF remain the same for another MNF. This remains true if countries who are members of one MNF simultaneously participate in another (or multiple) MNF. Confirm with the authoritative FDO, usually at the Combatant Command, how information is shared within the MNF.

6. Train and rehearse differing FD techniques or procedures (if any) of affected MNF partners. We know from multiple coalition operations that nations are neither similarly equipped (analog or digital) nor experienced in operating with U.S. forces. U.S. forces cannot assume one standard mechanism for sharing information with all MNF members. Tailor the FD CONOP to the situation. It's a best practice to confirm the tailored CONOP can be implemented with the equipment member nations bring to the MNF. Incorrectly assuming the equipment an MNF member used to share information during previous combined operations would be the same equipment used in a subsequent MNF can render the FD CONOPS useless and impact the MNF mission accomplishment.

7. A best practice is to provide MNF members with a Common Understanding of Terms. It is not enough to only provide translations of U.S. products. Acronyms, abbreviations, reporting formats, and tactical tasks need to be clearly defined in a glossary for all MNF partners to reference.

8. Exchange Liaison Officers (LNOs). Exchanging LNOs with the MNF forces enhances mission command and dissemination of intelligence during operations. A best practice is to identify LNOs early and involve them in mission planning. LNOs must understand and be proficient in the FDO process to facilitate appropriate information sharing. Understand and incorporate into any FDO/FDR training or CONOP development, that LNO personnel will probably not be MI personnel. Aspects of information or intelligence sharing that are well known by most MI personnel may not be as widely known by non-MI personnel.

9. Understand how each MNF partner's respective intelligence enterprise operates. MNF intelligence assets may collect, receive, process, and disseminate intelligence differently than U.S. forces. Additional differences may exist in how MNF tactical level intelligence capabilities interact with their respective nation's intelligence apparatus. Understanding the differing strengths and considerations of MNF partners allows one to identify how best to use each MNF participant's capabilities to achieve the commander's intent.

10. Leverage the available capabilities of your foreign partners in accordance with your unit's mission variables. MNF members have differing, and sometimes superior, intelligence capabilities available. Understanding how MNF partners receive and process intelligence will better inform the MNF information collection plan. Understanding the capabilities and limitations of MNF forces should also be used in designing the most efficient intelligence reporting and communications architecture possible. Develop, and rehearse with MNF partners, a feasible intelligence reporting and communications Primary, Alternate, Contingency and Emergency plan.

These Top Ten L&BP from MNF operations are only a few items of information available and reflect observations from operations and training to provide you with an initial self-development azimuth on which to proceed.

MI LL Homepage at https://army.deps.mil/Army/CMDS/USAICoE_Other/CDID/Lessons%20Learned/SitePages/Home.asp

Be sure to use CAC EMAIL certification; not your regular certificate when prompted.

Endnotes

1. ADP 7-0 Training Units and Developing Leaders, August 2012.

2. JP 3-16 Multinational Operations, July 2013.

Doctrine Corner

by Lee Goodman

MI Pub 2-0.3 Intelligence Processing, Exploitation, and Dissemination

Since the onset of the wars in Afghanistan and Iraq, the operational environment has become more complex. This complexity is characterized by a multitude of groups, ranging from friendly supporters and neutral observers to malicious opportunists and direct threats. In order to meet the challenges of a complex environment we must deliver high-resolution, multi-discipline intelligence to leaders at all levels–all in real or near-real time. Conducting intelligence processing, exploitation, and dissemination (PED) of data efficiently is the cornerstone of this effort, beginning with the transition from platform centric PED to a more holistic enterprise strategy.

Army doctrine has long recognized the functions of processing, initial analysis, and reporting, and the requirement for providing combat information. Today, joint and Army doctrine recognizes these functions under the concept of PED and the core capability of intelligence PED. In joint doctrine, PED is a general concept that facilitates the allocation of assets to support intelligence operations. Under the joint PED concept, planners examine all collection assets and determine if allocation of additional personnel and systems is required to exploit the collected information.

Beyond doctrine, PED plays an important role within the Department of Defense (DOD) intelligence capabilities development. PED began as processing and intelligence exploitation support for unique systems and capabilities, for example, full-motion video from unmanned aircraft systems. Unlike previous Geospatial Intelligence (GEOINT) collection capabilities, full-motion video did not have an automated capability to process raw data into a useable format and supporting personnel to perform initial exploitation. Therefore, a separate PED capability was required. Since 2006, PED requirements have grown significantly, and DOD has created many different PED capabilities across the intelligence enterprise. The following discussions are excerpts from MI Pub 2-0.3

PED Defined

Processing, exploitation, and dissemination is the execution of the related functions that convert and refine collected data into usable information, distribute the information for further analysis, and provide combat information to commanders and staffs.

PED is not exclusive to MI organizations; other branches employ sensor collection capabilities. Therefore, PED conducted by intelligence personnel or units is called intelligence PED. Intelligence PED facilitates efficient use and distribution of information following collection. In essence, intelligence PED is the way the intelligence warfighting function processes collected data and information, performs initial analysis (exploitation), and provides information in a useable form for further analysis. During initial analysis, some information will be identified as combat information. In those cases, the combat information is disseminated to commanders and staffs.

Intelligence PED Support to Operations

Intelligence PED plays an important role in providing commanders situational awareness crucial to mission command. The Army must monitor advances in satellite and sensor technology and secure communications and advanced analytics while honing human abilities to work in complex, degraded, and disrupted conditions. Achieving flexibility, which often requires some redundancy, is essential. For example, PED nodes should have mutually supporting continuity of operation plans, and intelligence staffs should develop primary, alternate, contingency, and emergency communications plans for every mission, thus ensuring data availability to support mission command.

The principles of conducting Intelligence PED operations include:

- Engage regionally–Intelligence PED and analytic nodes develop deep regional expertise through regional alignment and focus on regionally aligned missions.
- Balance PED–The synchronization of PED enablers across echelons and throughout the intelligence enterprise to maximize resources.
- Aid situational understanding through action–Army PED must support this effort by providing real-time, multidiscipline information that improves situational understanding and by integrating PED support into the supported unit's communications.
- Sustain high tempo operations–Supports high tempo operations by leveraging redundant communications

and task organizing PED enablers to meet commanders' priorities. Planners anticipate PED output requirements and tailor PED functions to leverage tipping and cueing of sensors to meet information requirements and support compressed decision making cycles.

- Support defense support of civil authorities–When directed, Army units support civil authorities in a wide range of operations. Army units use their intelligence assets and PED enablers to support those missions according to the governing law and doctrine.
- Optimize human performance–Leaders must recognize technology limitations and optimize the role of personnel during the performance of PED functions. Organizations that perform PED functions deliberately develop personnel to perform PED functions through discipline-specific training, certification, and other professional development programs.

Intelligence PED Strategy

The accurate and timely distribution of information resulting from this effort depends on exercising a multi-echeloned strategy that maximizes PED enablers across echelons and throughout the intelligence enterprise. The strategy becomes increasingly more important as the amount of sensor data continues to outpace the ability of a single unit to conduct PED with only organic resources. PED is performed according to the following complementary concepts:

- Expeditionary PED is the attachment of expeditionary military intelligence brigades (E-MIBs) and PED enablers to deploying forces. As part of force tailoring, Corps, division, and brigade combat team (BCT) commands identify the PED enablers necessary to support information collection. When tasked, the U.S. Army Intelligence and Security Command task-organizes assets from its aerial intelligence brigades, MIB(Theater), or functional brigades to deploy with identified Corps, division, or BCT headquarters. Expeditionary PED is often required when infrastructure is underdeveloped, continuity of operation plans are required, or when reach capabilities cannot support high-priority, time-sensitive requirements. PED Soldiers deploy and conduct PED for the supported commander, most often with limited to no ability to reach back to home station or national databases. Consequently, the expeditionary PED team will provide time-dominant (first phase imagery exploitation) and limited content-dominant exploitation (second and third phase imagery exploitation) on the ground to support commanders' intelligence requirements
- Reach PED provides PED from a sanctuary location with a robust communications infrastructure, enabling national to tactical multi-disciplined intelligence capability support to the deployed commander. The intent behind reach PED is to create and maintain a system-agnostic capability, tailorable to any mission. Reach PED operations are characterized by the routing of GEOINT and Signals Intelligence (SIGINT) data from a theater to a CONUS-sanctuary location where the data is processed, exploited, and disseminated, and the resulting information is made discoverable to the intelligence enterprise and redistributed back to forward deployed commands.

An important part of intelligence PED is ensuring information is distributed with adequate context and formatted to facilitate understanding or make subsequent analysis easier. Another important aspect of PED is providing feedback on the effectiveness of collection relative to taskings and expected results. All PED methods are related closely to planning, information collection, intelligence analysis, and control via technical channels. Receiving feedback gives leaders and staffs information they need to maintain synchronization of intelligence operations with the overall operation. This synchronization may include re-tasking MI collection assets or cueing other MI collection assets.

The current approach to intelligence PED reflects a deliberate solution to the increased complexity of intelligence operations and the explosion of available data and information that results from information collection. This approach is part of meeting the enduring challenge to get the right information to the right place at the right time. The amount of available data and information will continue to grow exponentially. In response, the Army is placing a major emphasis on resourcing, planning, executing, and maintaining a continuous assessment of PED. This approach is resourced with and executed by a broad variety of intelligence PED capabilities.

Conclusion

The U.S. Army Intelligence Center of Excellence Doctrine Directorate will develop and publish MI Pub 2-01.3 shortly after the publication of Change 1 to ADP 2-0 Intelligence and ADRP 2-0 Intelligence. We will staff MI Pub 2-0.3 publication for a final time this summer. The principal audience for MI Publication 2-0.3 is the Soldiers assigned to the intelligence sections organized as part of theater, Corps, division, and BCT headquarters, and to the MI units conducting intelligence operations.

MI Publication 2-0.3:

- Amplifies the PED discussions in ADP 2-0 and ADRP 2-0, to include advising the commander and staff on PED planning considerations related to intelligence architectures, force tailoring, information collection/intelli-

gence, surveillance, and reconnaissance, and situation development.

- Describes PED functions associated with single-source analysis and the production of all-source intelligence and the single-source analysis associated with the:
  - *Intelligence disciplines:* counterintelligence, GEOINT, human intelligence, measurement and signature intelligence, open-source intelligence, SIGINT, and technical intelligence.
  - *Complementary intelligence capabilities:* biometrics-enabled intelligence, cyber-enabled intelligence, document and media exploitation, and forensic-enabled intelligence.
- Identifies and discusses tactics, techniques, and procedures for PED functions conducted within the PED enterprise.
- Discusses the communications architectures and enablers that facilitate a unit's ability to process, exploit, and disseminate single-source information.
- Discusses the procedures, requirements, and timelines for reporting within intelligence, operations, and technical channels.

The New Doctrine Structure and How to Use It

by Craig Sieting

Introduction

31 December 2015 marked the end of a three year Army effort to re-engineer and revise all Army doctrine. The times of hauling around a foot locker packed with every field manual (FM) you could possibly need during a deployment or field exercise are long gone. Doctrine 2015 stems from the conscious decision to reduce the Army doctrinal holdings from over 650 FMs, to a reduced number of publications. Additional mandates for Doctrine 2015 were to eliminate redundancy as much as possible, and discuss processes, tactics, techniques, and procedures in the appropriate tier of doctrinal publication. An additional intent was to make doctrine available to Soldiers on electronic media.

What is Doctrine?

Doctrine consists of fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.[1] It is a discussion of how military forces do business. Doctrine uses a common language to address intellectual tools used to solve military problems, and contribute to a shared professional culture. Doctrine is not hard-and-fast rules. Doctrine consists of:

- ***Principles.*** A comprehensive and fundamental rule (of war) that guides how an organization or function approaches and thinks about the conduct of operations.
- ***Tactics.*** The employment and ordered arrangement of forces in relation to each other.
- ***Techniques.*** Non-prescriptive ways or methods used to perform mission, functions, or tasks. Often described in terms of steps.
- ***Procedures.*** Standard, detailed steps in an established order, executed the same way at all times regardless of the circumstances, formats for reports, and specific control measures.
- ***Terms and Symbols.*** Terms and symbols with common military meaning (JP 1-02).[2]

The New Doctrine Hierarchy

As mentioned earlier, the Army has adopted a new doctrine hierarchy:

- **Army doctrine publications (ADP).** These publications discuss fundamental principles. There are 16 ADPs in the Army.
- **Army doctrine reference publications (ADRP).** These publications provide detailed information on fundamentals. There are 16 ADRPs in the Army which expand on the ADP discussions.
- **Field manuals (FM).** FMs provide information on tactics and procedures. There are 51 FMs in the Army. Military Intelligence has two FMs (FM 2-0 Intelligence, and FM 2-22.3 HUMINT Collector Operations).
- **Army techniques publications (ATP).** These publications discuss various techniques to accomplish the mission. The U.S. Army Intelligence Center of Excellence (USAICoE) Commanding General determines the number of ATPs USAICoE produces.[3]

Current MI Doctrine Inventory

The current MI doctrine inventory stands at 35 publications: ADP 2-0, ADRP 2-0, FM 2-0, FM 2-22.3, ATPs (21), Training Circulars (TC) (6), and Military Intelligence Publications (MI Pubs) (4). As of December 2015 we met all of our Army Doctrine 2015 requirements. However, we are working a number of other doctrinal projects not associated with Doctrine 2015. Five publications in the final steps of development are:

- ATP 2-22.2 VOL II, CI.
- ATP 2-22.2 VOL III, CI Investigations Handbook.
- ATP 2-22.33 Source Validation and 2X Operations.
- ATP 2-22.6 VOL II, SIGINT Guide.
- ATP 2-22.9 OSINT.
- ATP 2-91.9 Intelligence Support to CYBER.

Currently the USAICoE Doctrine Directorate has six TCs that are functioning as place holders until the information can be placed in the appropriate doctrine publication. See Figure 1 for the current MI Doctrine Inventory.

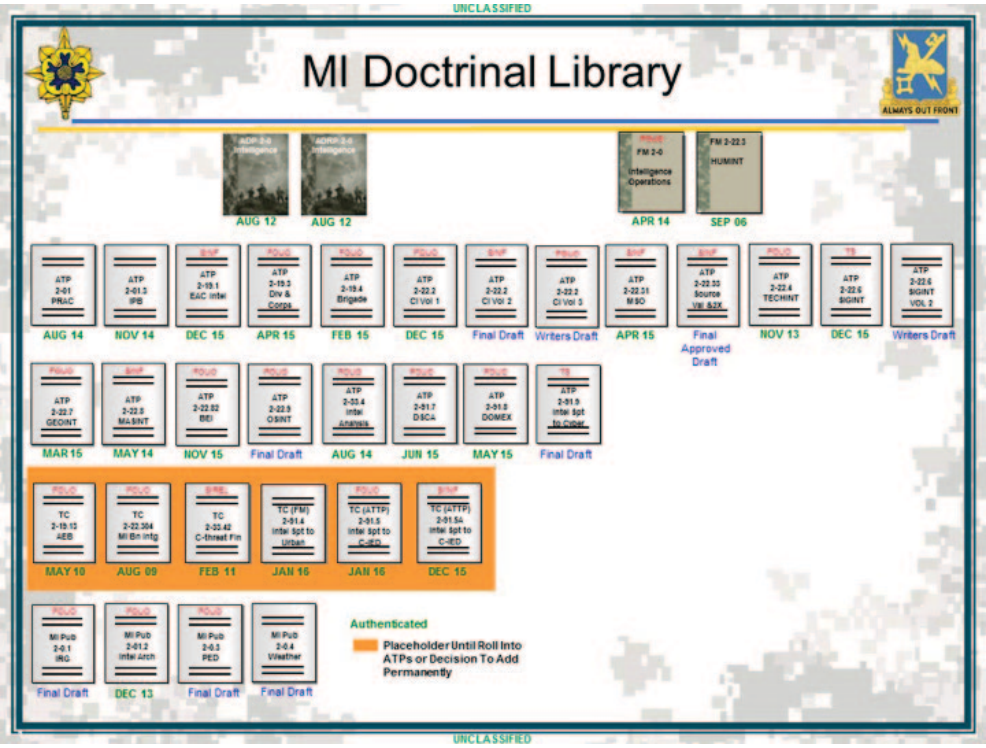


Figure 1.

The Doctrine Directorate developed and published four MI Pubs. These publications are approved by the Commander, USAICoE, and complement Army intelligence doctrine.

MI doctrine is moving towards making quick changes to doctrine focused on major and critical fixes, and away from the time consuming full revision process as the primary means to keep doctrine relevant to Soldiers. By doing this, the "shelf life" of MI doctrine publications is extended. There will still be the requirement to complete a full revision of publications by exception. The timing will depend on a number of factors to include changes to policy, processes, terminolgy, and higher level combined arms and intelligence doctrine.

Unclassified MI doctine publications can be found on the Army Publishing Directorate (APD) website, at http://www.apd.army.mil/ProductMap.asp and on the Intelligence Knowledge Network (IKN) https://ikn.army.mil, at Resources>MI Active Doctrine. Classified MI doctrine is posted on SIPRNET at IKN-S at https://ikn.army.smil.mil, at Resources>MI Active Doctrine. (A window opens in the IKN-S Doctrine Website. Select MI Active Doctrine from the left menu.) On JWICS, go to DAIIS>Hosted Websites>USAICoE>United States Army Intelligence Center of Excellence Doctrine.

How Can You Help?

As we move forward with doctrine, our intent is to update doctrine publications on a three year rotational cycle. By doing this, we believe we can keep doctrine current and relevant. We need your help doing this. Doctrine depends on input from Soldiers and civilians in the force executing operations. If you receive correspondence from the Doctrine Directorate requesting feedback or a review of a publication, please provide comments or suggestions. A listing of the current MI Doctrine Inventory begins on the next page.

We also take unsolicited suggestions or comments on any of our publications at any time, not just in the update cycle. Provide the number, title of the publication, paragraph number, and a brief comment with the recommended change. This information will be retained and addressed in the appropriate update cycle. You can send suggestions and comments to the Doctrine Directorate email at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. This will assist the Directorate in keeping doctrine relevant and current for Soldiers.

Endnotes

1. TRADOC Regulation 25-36 The Doctrine Publication Program, 21 May 2014, 5.

2. ADP 1-01 Doctrine Primer, 2 September 2014, 2-1 to 2-2.

3. ADP 1-01, 2-4 to 2-6.

Publication Number	Publication Title	Authenticated
ADP 2-0	Intelligence	31-Aug-12
Provides a common construct for intel. It describes the key aspects of intel support to unified land operations and establishes the doctrinal foundation for Army intelligence. This publication along with ADRP 2-0 is the foundation for the intelligence warfighting function and subsequent doctrine development.		
ADRP 2-0	Intelligence	31-Aug-12
This is the Army's reference publication for Army intelligence. It provides a common construct for intel doctrine from which Army forces adapt to conduct ops. It discusses: intel in unified land operations; the purpose and role of intelligence; intel core competencies; the intelligence warfighting function; the intelligence enterprise; the intelligence process; and intelligence capabilities. This publication along with ADP 2-0 is the foundation for the intelligence warfighting function and subsequent doctrine development.		
FM 2-0	Intelligence Operations	15-Apr-14
Describes how Military Intelligence units and collection assets conduct intelligence operations to accomplish the tasks developed during information collection. It also contains the descriptions of the Army tactical tasks included in the intelligence warfighting function, doctrine on language support, and doctrine on employing remote sensors. This manual is designed to be used with ADPs 2-0, 3-0, and 5-0 and ADRPs 2-0, 3-0, and 5-0.		
FM 2-22.3	Human Intelligence (HUMINT) Collector Operations	6-Sep-06
Provides doctrinal guidance, techniques, and procedures governing the employment of HUMINT collection and analytical assets in support of the Commander's intelligence needs. It outlines: HUMINT operations; the HUMINT collector's role within the intelligence operating system; and the roles and responsibilities of the HUMINT collectors and the roles of those providing the command, control, and technical support of HUMINT collection operations.		
ATP 2-01	Planning Requirements & Assessing Collection (PRAC)	19-Aug-14
Establishes doctrine for the specific tasks under planning requirements and assessing collection. It expands on the principles in FM 3-55. ATP 2-01 should be used in conjunction with FM 3-55 and with FM 2-0. Readers should be familiar with fundamental doctrine contained in ADPs 2-0, 3-0, 5-0, and 6-0 and ADRPs 2-0, 3-0, 5-0, and 6-0.		
ATP 2-01.3	Intelligence Preparation of the Battlefield (IPB)	10-Nov-14
Constitutes current Army and Marine Corps doctrine on how to systematically evaluate the effects of significant characteristics of the operational environment for specific missions. It describes how the commander and staff examine mission variables to understand how these variables may affect ops. It discusses IPB as a critical component of Military Decision Making Process and how IPB supports decisionmaking, as well as integrating processes and continuing activities. It also facilitates a common understanding, foundational concepts, and methods of the IPB process.		
ATP 2-19.1	**Echelons Above Corps (EAC)**	17-Dec-15
Describes the roles, responsibilities, and capabilities of intelligence organizations at echelons above corps. It outlines the vision, mission, and enduring functions of functional intelligence commands, theater Military Intelligence brigades, and the intelligence elements of Army Service Component Command; roles, responsibilities, and organizational relationships of echelons above corps military intelligence organizations and the support they provide to the intelligence enterprise; mission, structure, and organization of Intelligence and Security Command (INSCOM); and support provided by the 300th Military Intelligence Brigade (Linguist), Military Intelligence Readiness Command, Army Cryptologic Operations Directorate, and Army Geospatial-intel (GEOINT) Office.		
ATP 2-19.3	Corps and Division Intelligence	26-Mar-15
Provides non-prescriptive intel techniques for supporting corps and divisions conducting offense, defense, and stability tasks for Soldiers assigned to intelligence cells organized as part of corps and division headquarters and the higher and subordinate command intelligence cells that coordinate and collaborate with the corps or division intelligence cell during operations.		
ATP 2-19.4	Brigade Combat Team (BCT) and Below Intelligence	10-Feb-15
Provides techniques for intel support to BCT operations. The techniques in this manual apply to the range of military operations and all echelons of the infantry, armored, and Stryker BCTs.		
ATP 2-22.2-1	Counterintelligence (CI) Volume I	11-Dec-15
Establishes the Army's doctrinal publication for CI investigations, analysis and production, and technical services and support activities. It provides techniques for, and examples of, using Army CI assets at all echelons and in all operational environments. It outlines the: CI mission areas and CI specific functions; roles and responsibilities of Army, joint, and national CI elements and the United States Intelligence Community; specific techniques and procedures for conducting CI investigations, analysis, technical services, and support activities in support of Army operations and programs; and considerations for CI support in specific operations, missions, and environments.		
ATP 2-22.2-2	**Counterintelligence Volume II**	
Provides the Army's doctrinal guidance on CI operations and collection activities. It includes information on: fundamentals of CI collection and operations; CI functions and techniques; and considerations for specific operations and unique missions and envrionments.		
ATP 2-22.23 Volume III	Counterintelligence Investigations HB	Author's Draft
Provides doctrine specific to CI investigations.		

Publication Number	Publication Title	Authenticated
ATP 2-22.31	**Human Intelligence (HUMINT) Military Source Operations (MSO)**	17-Apr-15
Consolidates doctrine on Army HUMINT military source operations, clandestine military source operations, debriefings, liaisons, and screening. It provides detailed doctrine for Army HUMINT collectors at the tactical, operational, and strategic echelons. This publication covers fundamentals of HUMINT activities, HUMINT functions and techniques, and considerations for specific operations and unique missions and environments.		
ATP 2-22.33	**2X and Source Validation**	Final Draft
Provides detailed doctrine to military intelligence Soldiers serving in G-2X or S-2X staff elements. The 2X staff element manages CI and HUMINT operations at all Army echelons above brigade combat team. However, this manual focuses on 2X staff elements at the Brigade Combat Team and division. It also includes discussion on source validation.		
ATP 2-22.33	**2X** **(This publication will be superseded when the new ATP 2-22.33 is authenticated)**	6-June-14
Provides detailed doctrine to military intelligence Soldiers serving in G-2X or S-2X staff elements. The 2X staff element manages CI and HUMINT operations at all Army echelons above brigade combat team. However, this manual focuses on 2X staff elements at Brigade Combat Team and division.		
ATP 2-22.6	**Signals Intelligence (SIGINT)**	17-Dec-15
Outlines fundamentals and techniques for SIGINT activities in support of Army operations and specific missions. This manual also addresses the relationship between Army tactical SIGINT elements and those at the operational and national levels in providing intelligence support to operational and strategic missions.		
ATP 2-22.7	Geo-Spatial Intelligence (GEOINT)	26-Mar-15
Provides doctrinal guidance concerning GEOINT. It focuses on the fundamentals of GEOINT as well as specific tasks and techniques for performing GEOINT activities. The principal audience for ATP 2-22.7 is commanders, intelligence officers, engineer officers, staff planners, and GEOINT cells at brigades, divisions, corps, theater armies, and the Army Special Operations Command.		
ATP 2-22.8	**Measures and Signatures Intelligence (MASINT)**	30-May-14
Establishes doctrine for MASINT. It discusses the six MASINT technical data sources, what each provides, and how data is collected from them. The manual discusses the conduct of MASINT operations and the processes for developing collected technical data into intelligence. It also provides an overview of unattended ground sensors and describes the capabilities of MASINT collection systems.		
ATP 2-22.82	Biometrics Enabled Intelligence (BEI)	2-Nov-15
Provides guidance concerning the use of biometric information by intelligenec professionals, protection operations personnel, personnel involved in detainee screening or operations, and personnel involved in targeting operations. It addresses BEI, the fundamentals of biometrics, and biometric systems, as well as with biometric tools used in current operations. The manual discusses the biometric processes in support of the intelligence process, roles and responsibilities of intelligence units and individuals using biometrics, and intelligence considerations for the use of biometrically enabled watch lists.		
ATP 2-22.9	Open Source Intelligence (OSINT)	10-Jul-12
Establishes a common understanding, foundational concepts, and methods of use for Army OSINT. It highlights the characterization of OSINT as an intelligence discipline, its interrelationship with other intelligence disciplines, and its applicability to unified land operations. This publication: provides fundamental principles and terminology for Army units that conduct OSINT exploitation; discusses tactics, techniques, and procedures for Army units that conduct OSINT exploitation; provides a catalyst for renewing and emphasizing Army awareness of the value of publicly available information and open sources; establishes a common understanding of OSINT; and develops systematic approaches to plan, prepare, collect, and produce intelligence from publicly available information from open sources.		
ATP 2-33.4	Intelligence Analysis	18-Aug-14
Provides information on how intelligence personnel conduct intelligence analysis in support of unified land operations. It describes approaches used to conduct intelligence analysis and describes how intelligence analysis assists commanders with understanding the complex environments in which Army forces conduct ops. This manual emphasizes the act of intelligence analysis as a collaborative networked activity. This manual complements doctrinal guidance provided in ADP 2-0 and ADRP 2-0. It provides direction for intelligence personnel at all echelons. This publication provides guidelines for the conduct of intelligence analysis to commanders and staffs of Army units and is recommended for incorporation into institutional programs of instruction and unit training.		
ATP 2-91.7	Intelligence Support to Defense Support to Civil Authorities (DSCA)	29-Jun-15
Provides Army doctrine for intelligence support to DSCA. It explains how military intelligence Soldiers adapt military intelligence skills and techniques to provide support to civil authorities during operations in the homeland. It also discusses some of the sensitivities, laws, regulations, and policies that govern providing military intelligence support to DSCA and collecting information and producing intelligence within the Homeland. This manual describes the techniques intelligence staffs at all echelons use to support situation development and situational awareness for the commander when conducting DSCA. It describes the homeland security framework and the missions and functions of federal, state, local, tribal, and private sector organizations that make up that framework.		
ATP 2-91.8	Document and Media Exploitation (DOMEX)	5-May-15
Updates and expands existing doctrine on DOMEX based on technology and emerging lessons learned in current Army ops. It discusses intelligence support to DOMEX at all echelons. This manual informs commanders and staffs about the mission, requirements, and capabilities of DOMEX assets. It provides commanders and staffs with tools to integrate and synchronize DOMEX activities and techniques.		

Publication Number	Publication Title	Authenticated
ATP 2-91.9	**Intel Spt to Cyber Electromagnetic Activities**	Final Draft
Outlines fundamentals, as well as techniques, for intelligence support to cyber electromagnetic activities in support of Army operations and specific missions. This publication also addresses the relationship between Army tactical intelligence elements and their relationship with the operational and national levels in providing intelligence support to operational and strategic missions. The information contained in this manual applies to Soldiers conducting intelligence support to cyber electromagnetic activities and serves as a reference for military intelligence commanders and staff planners.		
TC 2-19.13	Aerial Exploitation Battalion	1-May-10
Provides doctrine for intel organizations, officers, NCOs, and Soldiers in modular units and information collection planners on the proper use of aerial exploitation battalion and aerial reconnaissance battalion assets. It describes those battalions' organization; history; mission and support sets; and tactics, techniques, and procedures for efficient use of these assets.		
TC 2-22.304	**MI BN (Interrogation)**	3-Aug-09
Provides doctrinal guidance concerning the MI Battalion (Interrogation). Complements existing doctrine such as FM 2-22.3 and incorporates enduring lessons learned from ops.		
TC 2-33.42	**Counter Threat Finance (CTF)**	21-Feb-11
Establishes doctrine for Army counter threat finance and threat finance analysis ops. Addresses CTF missions from brigade through Army specific activities at national-level agencies and centers. It includes examples of threat finance activities that Soldiers encounter in counterthreat finance ops.		
TC 2-91.4	Support to Urban Operations	25-Dec-15
Provides intelligence professionals a basic framework within which to focus on providing commanders with effective intelligence support for operations in the urban environment.		
TC 2-91.5	Support to Counter Improvised Explosive Devices Vol I	20-Jan-16
Outlines a detailed analytical approach to assess and predict enemy improvised explosive device operations using the intelligence disciplines, associated processes, and information collection assets. It supports counter improvised explosive device lines of effort and provides information to develop an understanding of the improvised explosive device threat and counter improvised explosive device requirements.		
TC 2-91.5A	**Support to Counter Improvised Explosive Device Vol II**	14-Dec-15
Contains classified products and examples from past operations that support counter improvised explosive device lines of effort.		
MI PUB 2-01	Intelligence Reference Guide	Final Draft
Captures information relevant to the environments the Army and Army intelligence are experiencing. It is a useful resource of information for commanders, intelligence and operations staff officers, warrant officers, NCOs, and analysts at all skill levels and echelons.		
MI PUB 2-02.2	Intelligence Architecture	4-Feb-14
Provides a guide to planning, preparing, deploying, and redeploying the intelligence architecture from corps to maneuver company level during the conduct of offensive, defensive, and stability missions and tasks. The intelligence architecture is an important part of the overall communications architecture.		
MI PUB, 2-0.3	Proccessing Exploitation and Dissemination	Final Draft
Provides nonprescriptive intel guidance and techniques on the planning, preparation, execution, and assessment of the processing, exploitation, and dissemination functions conducted by intelligence assets assigned to, attached to, or supporting corps, division, or Brigade Combat Team operations.		
MI PUB 2-0.4,	Weather	Final Draft
Describes how intelligence staffs can effectively integrate and exploit weather information and knowledge to aid the commander's ability to understand situations, make decisions, direct action, and lead forces toward mission accomplishment. This weather information and knowledge is applied within the operations and intelligence processes to enable the successful conduct of operations.		
MI PUB 2-0.5	Signals Intelligence (SIGINT) Reference Guide	Final Draft
Provides doctrinal guidance concerning SIGINT, to include definitions and functions, the SIGINT enterprise, the policies governing SIGINT, and detailed explanations regarding typical tasks conducted by SIGINT personnel. Its focus is to outline the fundamentals of SIGINT; to identify the authorities, policies and regulations governing SIGINT activities; and describe how SIGINT supports the combatant commander's mission. This Pub also provides the scientific theories and practical examples for MI personnel conducting SIGINT activities.		

Legend

SIPR	
JWICS	

Culture Corner

Culture Training 101: Cross-Cultural Respect

by Barton J. Fischer-Steinkraus

For the last ten years, Soldiers around the country received the required culture training prior to deploying. The Army did its part in reducing Soldiers from jeopardizing their missions, embarrassing themselves, or at worst, causing international incidents through cultural miscues. Introducing respect into the culture ballgame is a way for leaders to develop trust in their Soldiers to "do the right thing." Respect is defined as holding something or someone in high or special regard, while the U.S. Army (2016) further identifies respect as trusting that people are doing the right thing and fulfilling their promises. The Army Values already place respect as a Soldier responsibility, so what more can leaders do to prepare their Soldiers? Care, compassion, and trust all begin with respect, and leaders should believe that their Soldiers would act this way anywhere in the world.

Currently, Soldiers deploy to nearly 150 countries worldwide, some of them with complex or multiple cultures within the same border (CNN, 2016). So, should we put all our emphasis into making sure Soldiers understand those basic behaviors or norms? It is valuable to know a culture's religious practice, how they view time, and their native language. However, training time is always a rare commodity for operational units, so the Army could look beyond just those societal norms. Sending our military into different cultures with an understanding of cross-cultural respect will allow the Soldiers to build relationships and develop trust with their counterparts as well as the local populace, because it matters less how you shake hands than what you do after the handshake.

Dr. Richard Lewis (2006) explains how building a relationship is vitally important for a large number of cultures around the world. Mission success is dependent on the strength or weakness of the relationship when working with these countries. He identifies those relationship builders as multi-active cultures, which are warm, emotional, and impulsive. Those multi-active cultures rely on relationships to guide the rest of their activities. Brazil, Jordan, Kenya, Zimbabwe, and Mexico are all multi-active and their people want to feel comfortable before "getting down to business." While I worked in Zimbabwe, the Zimbabweans I worked with would not do business with people they did not know, respect, or consider a friend. It is not important that the local populace prays five times a day. What is important is that the Soldier respects the fact that the locals pray five times a day, and does not inhibit their ability to pray. Do you actively listen to what the locals are telling you? Do you show you care by following up on issues or problems? As Mackenzie (2011) explains, respect is the "social lubricant" that allows cross-cultural communications to flow smoothly between people from much different cultures.

Before you can respect someone from another culture, or anyone for that matter, you must understand how to show them respect according to their cultural practices and norms. We cannot demand respect, and then immediately expect them to show respect in return. Human cultural contexts, not distinct cultures, require respect to avoid conflict (Haydon, 2006). For that respect to "stick," the receiver must "feel" respected instead of having the sense of being manipulated (Mackenzie, 2011). An example of cross-cultural respect is a culture that holds the elderly in high regard because they have wisdom, knowledge, and life experiences. Soldiers should understand this and know their focus of respect would primarily be toward the eldest member of the group. Asking people with the experience or those who know what worked, what did not, and what factors of respect are key in these situations is an ideal way to learn cross-cultural respect (Mackenzie, 2011). A lot is lost in being disrespectful, but not much is lost, if anything, from being respectful while meeting, negotiating, or just interacting with people from a local population.

Respect is the way for Soldiers to prepare the operational environment for the mission. Soldiers will continue to deploy to those 150 countries around the world, so leaders must continue to prepare their Soldiers for cross-cultural interaction. Starting with the Army Values as the basis and relating that to cross-cultural respect as the beginning for

all communications, key leadership engagements, and negotiations is the road Army leaders should follow. However, using Dr. Lewis' Cultural Types model allows Soldiers to see the cross-cultural communication style generally used by a specific country. Multi-active cultures tend to use emotions to guide trust, communications, and respect building (Lewis, 2006). How we wish to be treated when we deploy is how we should examine how we treat our counterparts and the local population while deployed. Empathy, perspective taking, encouragement, cooperation, dignified treatment, appreciation, admiration, esteem, honor, reverence, deference, liking, equality, and tolerance are all ways that Soldiers should treat people if looking for ways to gain respect, earn trust, and build lasting relationships.

References

Haydon, G. (2006). "Respect for Persons and for Cultures as a Basis for National and Global Citizenship." *Journal of Moral Education*, 35(4), 457-471.

Hofstede, G., Hofstede, G. J., and Minkov, M. (2010). *Cultures and Organizations: Intercultural Cooperation and Its Importance for Survival*. New York, NY: McGraw-Hill Books.

Lewis, R. D. (2006). *When Cultures Collide: Leading Across Cultures* (3rd ed.). Boston, MA: Nicholas Brealey International.

Mackenzie, L. & Wallace, M. (2011). "The Communication of Respect as A Significant Dimension of Cross-cultural Communication Competence." *Cross-Cultural Communication*, 7(3), 10-18. doi: 10.3968/j.ccc.1923670020110703.175.

U.S. Military Personnel by Country (2012). CNN. Retrieved from http://www.cnn.com/interactive/2012/04/us/table.military.troops/.

Living the Army Values (n.d.). Retrieved from http://www.goarmy.com/Soldier-life/being-a-Soldier/living-the-army-values.html.

Mr. Fischer-Steinkraus is a Training Specialist with the TRADOC Culture Center, Fort Huachuca, Arizona. He retired from the U.S. Army and served as Senior Instructor, Warrant Officer Career College; Senior Battalion WO/Ops, Team Leader, and MFF Team Leader in the 3rd Special Forces Group (A); as an analyst for the Defense Intelligence Agency; and as Detachment Commander/Program Director for the U.S. Army Special Warfare Center and School. He holds a BS in Business Administration from the University of Maryland and an MS in Strategic Intelligence from the National Intelligence University.

USAICoE Initiatives in Botswana

(Continued from page 61)

Photo credit: CW3 Davis

conducting an initial reconnaissance to build this historical engagement of the Second Boer War. This concept resulted in the writing of a lesson plan to incorporate staff rides into future classes.

The team kept in mind the principles of Foreign Internal Defense operations to ensure that the requirements for USAICoE, the Department of State, U.S. Africa Command, and the BDF were met to the extent possible within the constraints of time and resources. As more and more Army formations are asked to conduct training outside of the standard military transitions team/security force assistance advisor team model, it becomes increasingly important to understand end-states expected of the various entities, cross-cultural communications and concerns, and of course, information and operations security, and Force Protection.

Endnote

1. http://www.gov.bw/en/Ministries--Authorities/Ministries/State-President/Botswana-Defence-Force-BDF/About-the-BDF1.

CPT Hogan and CW3 Davis are instructors at USAICoE, Fort Huachuca, Arizona.

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.

Contact phone numbers are: 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:106470-000