

MI Professional Bulletin

July - September 2019
PB 34-19-3

INTELLIGENCE WITHIN THE SFAB



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

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

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

Our mailing address: MIPB (ATZS-DST-B), Dir. of Doctrine and Intel Sys Trng, USAICoE, 550 Cibeque St., Fort Huachuca, AZ 85613-7017

Commanding General

MG Robert P. Walters, Jr. (through 19 July)

Commanding General

MG Laura A. Potter (beginning 19 July)

Chief of Staff

COL Peter J. Don

Chief Warrant Officer, MI Corps

CW5 David J. Bassili

Command Sergeant Major, MI Corps

CSM Warren K. Robinson

STAFF:

Editor

Tracey A. Remus

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

Associate Editor

Maria T. Eichmann

Design and Layout

Emma R. Morris

Cover Design

Emma R. Morris

Military Staff Officer

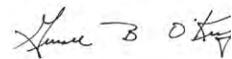
CPT Emily R. Morrison

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'KEEFFE
Administrative Assistant
to the Secretary of the Army
1912378

From the Editor

The following themes and deadlines are established:

January-March 2020, *Intelligence at Echelons Above Corps*. This issue will discuss aspects of intelligence support and operations at Echelons Above Corps. Deadline for article submission is 28 September 2019.

April-June 2020, *Intelligence Analysis*. This issue will focus on the various aspects of intelligence analysis and their importance to operations. Deadline for article submission is 19 December 2019.

July-September 2020, *Collection Management*. This issue will focus on how the intelligence staff executes the tasks of collection management in support of information collection. Deadline for article submission is 3 April 2020.

If you would like to receive a notification email when new MIPB issues become available on Intelligence Knowledge Network, send an email to usarmy.huachuca.icoe.mbx.mipb@mail.mil requesting addition to MIPB's announcement distribution list.

If you would like to receive a notification email when new intelligence doctrine is published, send an email to usarmy.huachuca.icoe.mbxdoctrine@mail.mil requesting addition to the new doctrine announcement distribution list.

For us to be a successful professional bulletin, we depend on you, the reader. Please call or email me with any questions regarding article submissions or any other aspects of MIPB. We welcome your input and suggestions.



Tracey A. Remus

Editor

MIPB Professional Bulletin

July - September 2019

PB 34-19-3

Volume 45 Number 3

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.

We wish to extend our genuine thanks and appreciation to LTC Todd Harkrader, 1st Security Force Assistance Brigade (SFAB) S-2 and "stakeholder" for this issue of MIPB. His enthusiasm for and extensive knowledge of the SFAB mission were instrumental to developing this issue. We would also like to thank CW3 Jason Schelte, 1st SFAB Geospatial Engineering Technician, for his assistance with the early author coordination.



INTELLIGENCE WITHIN THE SFAB



FEATURES

- 7 Security Force Assistance Brigades: An Introduction**
by LTC Todd Harkrader
- 9 Lessons Learned and the Way Ahead for the SFAB Intelligence Warfighting Function**
by LTC Todd Harkrader
- 16 Establishing the Intelligence Readiness of a Security Force Assistance Brigade**
by MAJ Aaron Bragg, CW3 Nick Rife, and CW2 Jay Gaines
- 20 Knowledge Management for Small Teams**
by CPT David C. Millikan and SPC Kaitlin M. McFarlane
- 24 Interesting Things Happen at Intersections**
by CPT William J. George
- 29 SFAB Geospatial Intelligence Support: Advising the Afghan National Army**
by CW3 Jason A. Schelte
- 34 The S303 Enemy Observation Report**
by CW2 Clyde A. Hunter and CW2 Aaron A. Johnson
- 40 Military Intelligence Junior Officer Development at the Joint Multinational Readiness Center**
by COL James L. Snyder, CPT Ryan M. Hardin, and CPT Kent D. Homrighausen

DEPARTMENTS

- 2 Always Out Front**
- 4 CSM Forum**
- 5 Technical Perspective**

- 44 Lessons Learned**
- 47 Doctrine Corner**

Inside back cover: Contact and Article Submission Information



Always Out Front

by Major General Robert P. Walters, Jr.

Commanding General

U.S. Army Intelligence Center of Excellence



The theme of last quarter's *Military Intelligence Professional Bulletin* (MIPB) was military intelligence (MI) support to U.S. Army special operations, a force established more than 60 years ago. In contrast, one of the subjects in this unique dual-themed MIPB issue is the relatively new Security Force Assistance Brigades (SFABs) and the intelligence warfighting function's support to those brigades. SFABs were created when U.S. Army Chief of Staff GEN Mark A. Milley recognized the value in having a professional advisor force to train, advise, and assist our partners. This allows deployed units to focus on their operational missions while the SFABs mentor and train foreign security forces. The second theme in this issue is Army intelligence strategies and innovations, which includes articles derived from topics briefed at the 2019 Intelligence Senior Leaders Conference (ISLC).

Readiness remains the Army's top priority. The way we fight, our pacing threat, and our doctrine have all changed in the last few years to ensure the Total Army Force is prepared to meet the readiness strategy. This is no different for the MI Corps. An article by LTG Scott D. Berrier, U.S. Army Deputy Chief of Staff for Intelligence, G-2, titled "Mission Command Intelligence in Multi-Domain Operations," addresses the subject of MI readiness. LTG Berrier explains that Mission Command Intelligence "is the Army intelligence enterprise's overarching framework to achieve an end state of a ready Army intelligence team supporting mission command against all threats in multi-domain operations by 2028." He discusses improvements to our intelligence warfighting function as a by-product of these changes. One of these improvements is the caliber of intelligence Soldiers and their ability to be self-sufficient and less reliant on "commercial-sector providers." Another improvement is greater cooperation with the U.S. Army Cyber Center of Excellence to ensure secure



networks. LTG Berrier also addresses the ever-increasing amounts of data and the development of a cloud-based network, which the U.S. Army Intelligence Center of Excellence (USAICoE) is a partner in tackling.

At the ISLC, which USAICoE hosted in February, a common discussion was the ability to maintain or increase the intelligence warfighting function's readiness. The U.S. Army Intelligence and Security Command (INSCOM) gave a briefing highlighting the use of the intelligence enterprise in support of large-scale combat operations. After the conference, MG Gary W. Johnston, INSCOM Commanding General, provided an article that describes INSCOM's strategy to connect and deliver the intelligence enterprise across the Army. The U.S. Army Futures Command's Intelligence Capability Development and Integration Directorate (CDID) briefed the subject of sensor challenges in multi-domain operations at echelons above brigade and provided an article on the subject for this MIPB issue. There is also an article by the CDID about enabling battalion S-2 sections for the pace of large-scale ground combat operations.

In the Army, soldiering is a team sport; this is something I continuously tell the leaders at Fort Huachuca, as we cannot accomplish our mission alone. The Army is structured to ensure the various echelons support one another: the company supports the platoon, which supports the squad. This structured support also works in reverse in that brigade and division elements push and pull information from each other to accomplish the mission. During the ISLC, I was able to witness this support—how intelligence leaders from numerous echelons came together to identify and solve current issues.

We concluded the conference with the presentation of four 2019 awards for excellence in MI, in honor of LTG Sidney T. Weinstein, CW5 Rex Williams, CSM Doug

Russell, and a newly established MI Civilian award that recognizes the achievements of Ms. Dorothe K. Matlack, one of MI's early pioneers and champions of Army human intelligence efforts. The ISLC was an excellent venue for senior MI professionals to recognize the accomplishments of this year's award recipients.

As I mentioned at the beginning of this column, the other theme of this issue is intelligence within the SFAB. The 1st SFAB returned from its 9-month deployment to Afghanistan in December 2018, and the 2nd SFAB is currently in the country. These two brigades have already discovered lessons learned concerning our intelligence warfighting function, which is essential for intelligence professionals to study and implement for the next four SFABs. LTC Harkrader, MAJ Bragg, and others have highlighted vital lessons from the 1st and 2nd SFABs. An interesting topic in LTC Harkrader's article is the potential success of the Distributed Common Ground System-Army Capability Drop 1's effectiveness for the combat advising team, even though this capability was not explicitly developed for the SFABs. MAJ Bragg explains a three-pillar

strategy to assist intelligence readiness, which involves building a team, configuring the architecture, and training the intelligence warfighting function. Not only does his article provide a blueprint on how the 2nd SFAB conducted intelligence operations, but it also allows us, as intelligence professionals, to determine how we can improve the process.

Last, but certainly not least, is a piece written by the USAICoE Doctrine Division on the recently published ATP 2-01.3, *Intelligence Preparation of the Battlefield*. Intelligence preparation of the battlefield (IPB) is an important process and critical to tactical operations, so much so that the next issue of MIPB will focus on all aspects of the IPB process.

This quarter's issue of MIPB has a wide range of articles to improve the intelligence professional in diverse environments, with the overall goal of having the "Army intelligence team supporting mission command against all threats." The intelligence corps and its professionals are ready to tackle any problem or enemy. 

Always Out Front!

Excerpt from "Success of First SFAB in Afghanistan Proves

'Army Got it Right,' Commander Says"

by C. Todd Lopez

Army Brig. Gen. Scott Jackson, 1st SFAB commander, spoke today at the Pentagon as part of an Army Current Operations Engagement Tour. He said the Army's concept for the new unit—one earmarked exclusively for advise and assist missions—was spot on...

Lessons Learned

Jackson outlined two key lessons-learned from their time in Afghanistan. First, that [they] learned their ability to affect change within those they advise and assist was greater than they thought.

"As our Afghan partners began to understand the value of 1st SFAB advisors, they asked us for more," Jackson said. "So our teams partnered with more and more Afghan units as the deployment progressed."

Another lesson, he said, was that persistent presence with partners pays off.

"Units with persistent partners made more progress in planning and conducting offensive operations and in integrating organic Afghan enablers like field artillery and the Afghan air force than unpersistent partnered units," Jackson said.

Those lessons and others were passed to the follow-on unit, the 2nd SFAB, as well as to the Security Force Assistance Command.

Another observation: the Afghan military is doing just fine. They're in charge of their own operations. And while U.S. presence can provide guidance when needed — and it is asked for — the Afghans were proving successful at doing their own security missions without U.S. soldiers running alongside them. It turns out that just having an SFAB advise and assist presence has emboldened Afghan security to success.

"We saw enormous offensive maneuver generated, and not just at the brigade level," said Army Lt. Col. Brian Ducote, commander of the 1st Battalion, 1st SFAB. "They weren't over-dependent. They were able to execute offensive operations themselves. It was a huge confidence builder when we were sometimes just present. Even if we didn't support them, just us being there gave them the confidence to execute on independent offensive operations."

Endnote

C. Todd Lopez, "Success of First SFAB in Afghanistan Proves 'Army Got it Right,' Commander Says," U.S. Department of Defense News (May 8, 2019), <https://dod.defense.gov/News/Article/Article/1842220/success-of-first-sfab-in-afghanistan-proves-army-got-it-right-commander-says/>.



CSM Forum

by Command Sergeant Major Warren K. Robinson
Command Sergeant Major of the MI Corps
U.S. Army Intelligence Center of Excellence



U.S. Army Chief of Staff GEN Mark A. Milley identified the Security Force Assistance Brigade (SFAB) as one of his top priorities. He recognized the need to have a permanent, professional advisor force to train, advise, and assist allied and partner nation forces. The Army has most recently deployed the 2nd SFAB to Afghanistan and is actively recruiting Soldiers to stand up three other brigades for future operations supporting combatant commands worldwide. Military intelligence (MI) provides support to these units, and SFABs offer a relatively new, dynamic opportunity for MI Soldiers.

To serve in the SFABs, Soldiers must volunteer and then go through a screening and selection process. During the process, they undergo physical assessments, display military occupational specialty proficiency, complete an interview, and take training courses—including intense training specific to the advisory mission.

While some MI noncommissioned officers (NCOs) are involved in the training, advising, and assisting mission that is at the core of the SFAB, other MI Soldiers spend the majority of their time providing intelligence to the commanders and their teams. Soldiers must quickly fuse and analyze intelligence from multiple disciplines to provide a clear picture for the commanders in a fast-paced environment. Recruiters emphasize these aspects of the SFAB mission to encourage MI Soldiers to volunteer.

Volunteering for an SFAB assignment provides both financial benefits and rewarding experiences. First off, there is a \$5,000 bonus, and Soldiers who reenlist to volunteer receive additional cash bonuses. However, more important is the potential for promotion. Specialists are automatically promoted to sergeant after successful completion of



their training. Overall promotion rates for senior NCOs are significantly better than the normal selection rates MI typically sees, and semi-centralized selection boards offer higher consideration to SFAB volunteers. An SFAB assignment is considered tactical broadening, and the U.S. Army Intelligence Center of Excellence also lists the SFAB as the number one broadening opportunity for NCO promotion consideration. An additional motivator is having a choice of duty assignment after successful completion of an SFAB assignment.

Second, being part of an SFAB offers a unique MI experience. It means working with a team that transfers skills to ensure allied and partner nation forces are prepared to fight and win. When doing this, Soldiers get another perspective of the intelligence warfighting function, and they have the opportunity to lead and conduct intelligence operations. They will also learn to pull intelligence from U.S. Army Intelligence and Security Command, U.S. Army Forces Command, and special operations forces operating in and responsible for that theater. Soldiers will learn about the importance of intelligence fusion and how the disciplines work together—something many may not have seen in their careers. Relationship building is also necessary to provide the best intelligence support. This puts some leaders out of their comfort zone but is important for any future assignment.

The value of being assigned to an SFAB is operating in a dynamic environment, working with a group of dedicated professionals, and receiving some form of monetary or promotion benefit. The more long-lasting value lies in the experience leaders will bring to the fight regardless of where they go in the future.



Always Out Front!



Technical Perspective

by Chief Warrant Officer 5 David J. Bassili

Chief Warrant Officer of the MI Corps

U.S. Army Intelligence Center of Excellence



The ancient Greek philosopher Heraclitus has been quoted as saying that change is the only constant in life! If by chance you haven't been paying attention, the Army is in the midst of significant change. Everything is changing—organizational structure, planning, equipping, and talent management, among other things (some rapidly, others steadily)—to meet the demands of multi-domain operations against our peer competitors. This quarter's *Military Intelligence Professional Bulletin* (MIPB) focuses on some of the change efforts the Military Intelligence (MI) Corps is making to meet the challenges of multi-domain operations. As the administrators, managers, maintainers, operators, and integrators of the MI Corps' systems and capabilities, we as warrant officers must remain conversant on the details of these changes. We must generate constructive input on employment strategies and candid (timely) input on potential (likely) second and third order effects of the change. If we as "professionals" don't make time to address and contribute to change, we put ourselves at risk—change is going to happen. You can choose to let it steamroll you, or you can embrace it and attempt to shape it in your favor. One of the greatest attributes of MIPB is that every article published includes the author's biography, and through that, general point of contact information is obtainable. If you're going to be a part of the change process, I challenge you all to reach out to the authors with recommendations or questions. And when the tasking to review and complete a comment resolution matrix (CRM) hits your inbox, take the time to read through the concept, capability, doctrinal publication, etc. Resist the urge to delete the CRM or to simply move on and keep your experiences and lessons learned to yourself.

The framework driving our Corps' change effort is Mission Command Intelligence (MCI). As LTG Berrier describes in his article, modernizing the essential components of MCI



(sensors, data, and analysis enabled by a cloud-based architecture) is the driving force to enabling intelligence at the speed of mission command. The essential components of MCI should come as no surprise to most. They directly correlate to the intelligence warfighting function's core competencies of intelligence operations; intelligence synchronization; intelligence processing, exploitation, and dissemination; and intelligence analysis.

The forthcoming articles provide a brief summation on the modernization of the Terrestrial Layer System, Tactical

Intelligence Targeting Access Node, and Multi-Domain Sensing System sensor capability development efforts. The articles also provide information about potential organizational changes in the U.S. Army Intelligence and Security Command (INSCOM) MI brigades-theater, corps expeditionary-MI brigades, and brigade combat team MI companies. These changes include the addition of an electronic warfare force structure and a return of the technical control and analysis element to maximize personnel capacity to employ and exploit these emerging sensors. The effort to modernize how we manage, process, and exploit data to better enable a relevant and timely common intelligence picture and relieve the burden of data management at the tactical echelon (to facilitate more analysis rather than processing) is captured in the Distributed Common Ground System-Army's Capability Drops 1 and 2. This modernization effort is also envisioned in INSCOM's strategy to "connect and deliver the intelligence enterprise." While intelligence preparation of the battlefield remains predominately unchanged (a stalwart means of sense-making), the latest version (re-)incorporates aspects of assessing our former peer competitor (the Soviet Union) as it relates to today's concept of large-scale ground combat operations. This version also adds elements of the electromagnetic spectrum and cyberspace to how we view and assess the operational environment. Encompassing all this

is a discussion on addressing intelligence policy, rooted in a pre-technological era, and if and how we might consider modifications in concert with emerging change.

While not wholly an MI or newly emerging organization, our Army's Security Force Assistance Brigades (SFABs) provide another venue for professionals to contribute and develop new capabilities and concepts through innovation, initiative, and imagination. For the foreseeable future, these organizations will remain a volunteer opportunity for those among us looking to challenge their personal experiences and knowledge in a semi-ambiguous employment environment. Based on my personal interaction and observation of those currently serving in these organizations, the return is both personally and professionally challenging and beneficial, if even a little gratifying. These MIPB articles provide a glimpse into the opportunities, challenges, and successes an SFAB assignment offers. If interested, CW4 Kris Johnson and CW4 Chris Moore can chart the path for the next opportunity available to you.

In closing, please take the time to read the amazing and inspiring biographies of this year's MI Hall of Fame inductees, specifically our very own CW5 Stephen Kiss. Many of you will probably notice the number of consecutive years outside the continental United States CW5 Kiss spent developing and employing his regional expertise (this fact does not escape me, as I participate in Army talent management discussions). CW5 Kiss is most deserving of this acknowledgement and is an inspirational figure we should all look to for a sense of professional direction. Finally, as the process to develop the previously discussed capabilities and concepts matures, I again challenge you all to find a way to contribute, either through document reviews and CRMs or by getting involved in the operational trials of new capabilities as part of the new fix-test-fix strategy of capability development. The future is yours to embrace. 

Always Out Front!

Excerpt from "Success of First SFAB in Afghanistan Proves 'Army Got it Right,' Commander Says" by C. Todd Lopez

Home Again

Back home now for six months, [Army BG Scott] Jackson [1st SFAB Commander] said the brigade is back to repairing equipment, replacing teammates and conducting individual and small-unit training to prepare for its next mission. He said their goal is to provide the Army a unit ready for the next deployment, though orders for that next mission have not yet come down.

The advise and assist mission is one the Army has done for years, but it's something the Army had previously done in an ad hoc fashion. Brigade combat teams, for instance, had in the past been tasked to send some of their own overseas as part of security transition teams or security force assistance teams to conduct training missions with foreign militaries. Sometimes, however, the manner in which these teams were created may not have consistently facilitated the highest quality of preparation.

The SFAB units, on the other hand, are exclusively designated to conduct advise and assist missions overseas. And they are extensively trained to conduct those missions before they go. Additionally, the new SFABs mean regular BCTs will no longer need to conduct advise and assist missions.

The Army plans to have one National Guard and five active-duty SFABs. The 1st SFAB stood up at Fort Benning, Georgia, in early 2018. The 2nd SFAB is based at Fort Bragg, North Carolina, but is now deployed to Afghanistan. The 3rd SFAB, based at Fort Hood, Texas, is now gearing up for its own first deployment. The 4th SFAB, based at Fort Carson, Colorado, is standing up, as is the 54th SFAB, a National Guard unit that will be spread across six states. The 5th SFAB, to be based at Joint Base Lewis-McChord, Washington, is still being planned.

"As subsequent SFABs come online, it creates a huge capacity for the rest of the combatant commands in the world," Jackson said. "I would be confident to say that there are assessments ongoing to see where else you could apply SFABs besides Afghanistan."

Endnote

C. Todd Lopez, "Success of First SFAB in Afghanistan Proves 'Army Got it Right,' Commander Says," U.S. Department of Defense News (May 8, 2019), <https://dod.defense.gov/News/Article/Article/1842220/success-of-first-sfab-in-afghanistan-proves-army-got-it-right-commander-says/>.

Train

Advise

Assist



Security Force Assistance Brigades: An Introduction

by Lieutenant Colonel Todd Harkrader

In early 2017, the U.S. Army announced the creation of the 1st Security Force Assistance Brigade (SFAB) to assess, advise, support, and liaise with foreign security forces. A total of five active component SFABs and one National Guard SFAB are now either active, standing up, or planned. These specialized brigades are poised to become a critical instrument of national power and a key tool in the Army's inventory.

But what exactly are SFABs? What units are in an SFAB and what is their mission? Most importantly for the readers of the *Military Intelligence Professional Bulletin* (MIPB), what makes up the SFAB's intelligence warfighting function, how does the Army employ it, and what are the lessons learned from the past 2 years? This quarter's MIPB answers many of these questions and more.

The Army has specially manned, trained, and equipped these brigades for their primary mission of advising and working alongside foreign military partners. Consisting of an all-volunteer force of approximately 800 personnel, an SFAB is based on the structure of a traditional brigade combat team but without the junior enlisted and company grade officers. SFABs consist of two infantry battalions, a cavalry squadron, a field artillery battalion, an engineer bat-

talion, a support battalion, a headquarters and headquarters company, a military intelligence company, and a signal company. When fully employed, a single SFAB can produce 61 advisory teams across the various echelons and diverse warfighting functions of their foreign security force partner.

The SFAB's core mission set and purpose is threefold:

- ◆ First, an SFAB provides geographic combatant commanders with a purpose-built, sustainable theater security cooperation advising element to assess, advise, support, and liaise with foreign security forces. From preparing for great power competition to working with foreign security forces to counter threats to internal defense, SFABs afford combatant commanders a powerful and flexible tool to leverage their respective areas of responsibility.
- ◆ Second, SFABs "buy back" readiness for the Army by reducing the burden on brigade combat teams that are routinely called upon to support security cooperation missions. Years of this practice have reduced the readiness and capacity of brigade combat teams and the divisions they support at a time when a resurgent Russia and China threaten to tip the global balance of power.



1st SFAB



2nd SFAB



3rd SFAB

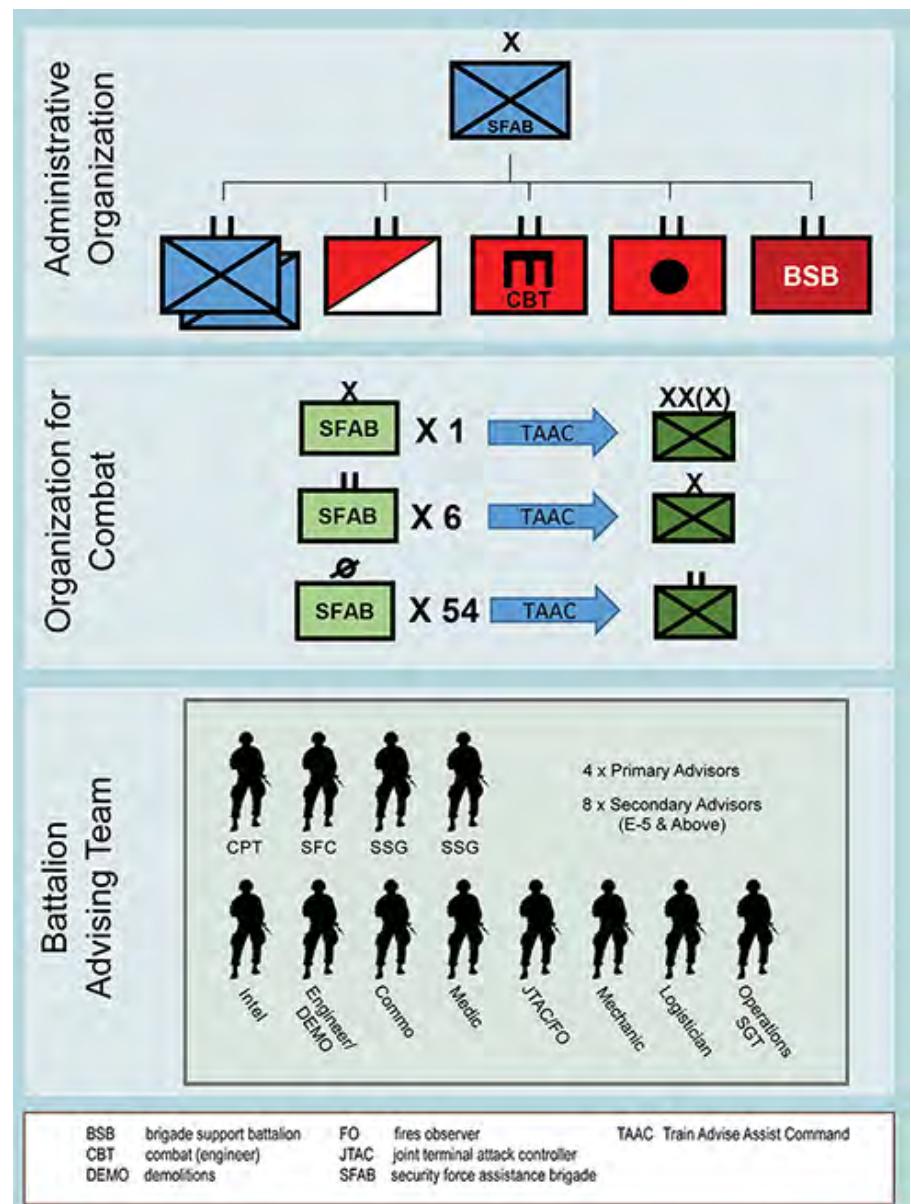


4th SFAB

- ♦ Third, in the event of a major high-intensity conflict, an SFAB consisting of senior officers, warrant officers, and noncommissioned officers can rapidly expand with an influx of junior personnel to form new brigade combat teams.

A relatively small yet highly effective cadre of intelligence professionals function within each SFAB. Consisting of officers, warrant officers, and noncommissioned officers of various ranks and disciplines, the men and women of the brigade S-2, battalion S-2, military intelligence company, and combat advising teams in an SFAB provide combatant commanders with a plethora of intelligence advising expertise. Unconstrained to a particular task organization, these personnel can operate in numerous configurations across more than one combatant command simultaneously if necessary for both persistent and episodic advising missions.

In this edition of MIPB, authors from the 1st and 2nd SFABs, and the U.S. Army Intelligence Center of Excellence Lessons Learned team provide readers a unique perspective on the training, employment, retraining, and mission command of SFABs, as well as the intelligence enterprise support provided to SFABs during their creation. Although new, the intelligence warfighting function of SFABs is already establishing a legacy rich with history, lessons learned, and strategic impacts that will continue to grow in the years to come.



SFAB Organizational Design

LTC Todd Harkrader was the first brigade S-2 for 1st Security Force Assistance Brigade at Fort Benning, GA. He previously served as the battalion operations officer and executive officer for 2nd Military Intelligence Battalion, 66th Military Intelligence Brigade, and as the operations officer for the U.S. Army Europe G-2 Intelligence Security Cooperation Section. He is currently assigned to the Pentagon in Washington, DC.

SFAB RECRUITING

“Victorious Together”

Enlisted: (910) 570-9975/5131

Officer: (910) 570-5159



<https://www.goarmy.com/careers-and-jobs/current-and-prior-service/advance-your-career/security-force-assistance-brigade.html>



U.S. Army photo by Sean Kimmons

SPC Stephen Powers, right, a communications advisor with Combat Advisor Team 1131, uses the Afghan National Tracking System to show his counterparts where Afghan soldiers are located during a clearing operation near Kabul, Afghanistan, September 16, 2018.

Lessons Learned and the Way Ahead for the SFAB Intelligence Warfighting Function

by Lieutenant Colonel Todd Harkrader

Introduction

In the summer of 2017, the 1st Security Force Assistance Brigade (SFAB) was in the process of manning, training, and equipping the first-ever SFAB when it received notification of an accelerated deployment timeline to support advising efforts in Afghanistan. The author, who was the brigade staff officer (S-2) of the 1st SFAB, and a small cadre of truly exceptional intelligence professionals were tasked with building, training, and deploying the first-ever SFAB intelligence warfighting function in just 6 months. Over the past 2 years, 1st SFAB completed a Joint Readiness Training Center (JRTC) proof of principal rotation, a JRTC validation rotation, and the first-ever rotation in a combat zone for an SFAB supporting operations in Afghanistan. Through it all, the 1st SFAB intelligence warfighting function continued to grow, adapt,

and prepare for the future while keeping an eye on how to train intelligence advisors and improve the SFAB intelligence enterprise as a whole.

In this article, readers will find both lessons learned and recommendations for the future of the SFAB intelligence warfighting function. The first half of the article covers the task organization and employment of the SFAB intelligence warfighting function in Afghanistan. It also provides observations on advising constraints created by mission command requirements as well as a discussion and recommendations for the SFAB intelligence architecture. The second half focuses on the recommended training glide path for building an intelligence advisor and closes with final thoughts from the author on the future of the SFAB intelligence warfighting function.

Building and Employing the Intelligence Warfighting Function Team

The initial deployment of the 1st SFAB saw the entirety of the organization's intelligence warfighting function employed in every Train Advise Assist Command and Task Force area of responsibility across Afghanistan. Consisting of approximately 30 brigade intelligence staff (S-2), battalion S-2, and military intelligence (MI) company advisors, plus 29 intelligence enablers added to the combat advisor teams shortly before deployment, the 1st SFAB intelligence warfighting function advised at every echelon up to the corps level. The 1st SFAB intelligence advisors also worked closely with provincial senior leaders of the Afghan National Directorate of Security as well as the MI kandak (MI battalion equivalent) of the Afghan National Army's 203rd Corps. The sheer scope and depth of intelligence advising that this relatively small cohort achieved was exceptional and proved critical in leveraging U.S. and North Atlantic Treaty Organization (NATO) enablers to support the Afghan National Army's offensive operations and election security activities.

Immediately before the first of two JRTC rotations, a decision was made to task-organize the MI company to support both the brigade S-2 and battalion S-2 sections. This turned out to be critical to the success of intelligence warfighting function advising. Although modified during the 1st SFAB's deployment, the original modified table of organization and equipment (MTOE) for battalion S-2 sections only consisted of a 35D (All-Source Intelligence Officer) captain and a 35F (Intelligence Analyst) staff sergeant, with several of the battalion S-2s not having previously served as battalion S-2s. Each battalion S-2 was augmented with either a 350F (All-Source Intelligence Technician) chief warrant officer 2 or a 35F staff sergeant, as well as one 351L (Counterintelligence Technician) or 35L (Counterintelligence Agent) to provide counterintelligence (CI) support to force protection (Title 10 of U.S. Code).¹

With the brigade S-2 section providing senior leadership and mission command to the Task Force Southeast G-2 section, all 35Ts (Military Intelligence Systems Maintainer/Integrator) and 35Gs (Geospatial Intelligence Imagery Analyst) were leveraged to augment the Task Force Southeast's intelligence and electronic warfare and geospatial intelligence mission command and advising function. The MI company command team handled day-to-day institutional advising of the 203rd Corps and MI kandak while the brigade S-2 officer in charge functioned as both the Task Force Southeast G-2 and the primary advisor for National Directorate of Security senior leaders in the seven provinces encompassing the area of responsibility. Because 1st SFAB



Photo courtesy of LTC Todd Harkrader

Advisors from the 1st Security Force Assistance Brigade S-2 team during their 2018 deployment to Afghanistan.

intelligence leaders performed both mission command and advising functions at nearly every echelon, the augmentation of MI company personnel provided a much needed capacity to battalion S-2s and is a recommended best practice for all future SFAB S-2s to consider.

Although prepared to function primarily as intelligence advisors, the mission requirements levied against the 1st SFAB in Afghanistan created a dynamic environment in which a majority of the intelligence leadership was "dual hatting" in both a mission command and an advising role. These competing demands ultimately degraded some of our capability to perform intelligence advising, particularly at the brigade and corps level where persistent, daily advising and leveraging of NATO enablers were critical to the success of our Afghan partners. In several lessons learned forums, a major regret of intelligence advisors was a desire to do more across multiple intelligence disciplines—something they never achieved because of the competing requirement to perform mission command functions. In spite of these challenges, intelligence personnel identified and acted upon opportunities to advise, particularly within the brigade S-2 and elements of the MI company supporting the mission command functions of the Task Force Southeast G-2 team.

SFAB Intelligence Architecture

1st SFAB's deployment also identified gaps within the intelligence architecture of the organization. Simply put, the current allocation of the Distributed Common Ground System-Army (DCGS-A) components residing within SFABs does not fully meet the needs of the SFAB intelligence warfighting function in an expeditionary environment. Although part of the ineffectiveness of DCGS-A was tied to a standardized system employment by intelligence warfighting function stakeholders across the area of responsibility, the pending Service Pack 1 upgrade provides only a limited number of Portable Multi-Function Workstations down to the

battalion level and does not address the 36 x intelligence advisors at the combat advisor team level. Conversations with leaders across 1st SFAB indicate a strong agreement that small intelligence warfighting function advising teams or solitary advisors on combat advisor teams need a system-agnostic, “plug and play” classified capability to quickly “push and pull” intelligence while also providing a ruggedized platform from which to operate. Such a capability is truly critical when one considers a future in which SFABs operate concurrently in multiple combatant command (COCOM) areas of responsibility.

The SFAB senior intelligence officers agree that Capability Drop 1, or a similar capability, is a perfect solution for combat advisor team intelligence advisors and that the system may be the answer for battalion- and brigade-level advisors as well. Although not currently earmarked for SFABs, Capability Drop 1 removes the need for bulky servers, equipment, and associated intelligence and electronic warfare support. It also arms the user with both a suite of intelligence warfighting function applications and portability/flexibility in employing the system, which is perfect for small teams operating independently in distributed locations. If combined with Service Pack 1 at the brigade and battalion level, SFABs would have the ability to establish reachback nodes in garrison with Service Pack 1 tied into theater intelligence brigades while forward-deployed teams link into

the overall architecture with Capability Drop 1 equipment. With the future of SFAB deployments pointing squarely at aligning with and supporting multiple COCOMs through rotational, persistent advising, it is important to resource SFABs with this mission essential intelligence architecture in the immediate future.

Building an Intelligence Advisor

Before the 1st SFAB’s deployment, the author participated in a U.S. Army Intelligence Center of Excellence (USAICoE) Lessons Learned forum and described how the 1st SFAB was “building” intelligence warfighting function advisors within an extremely constrained timeline. This discussion also included recommendations on “MI skills refresher training” and “high-payoff intelligence enabler training,” which are military occupational specialty (MOS)-specific training opportunities that, if training time was available, would pay long-term dividends to intelligence advising. A majority of these training concepts and recommendations never reached fruition because of the unit’s deployment timeline. However, revisiting this foundational document in the months following our deployment proved invaluable and provided a road map for the 1st SFAB’s MI Training Strategy moving forward.

As illustrated in Figure 1, the foundation of the SFAB intelligence warfighting function training is attendance at the Combat Advisor Training Course at Fort Benning, Georgia.

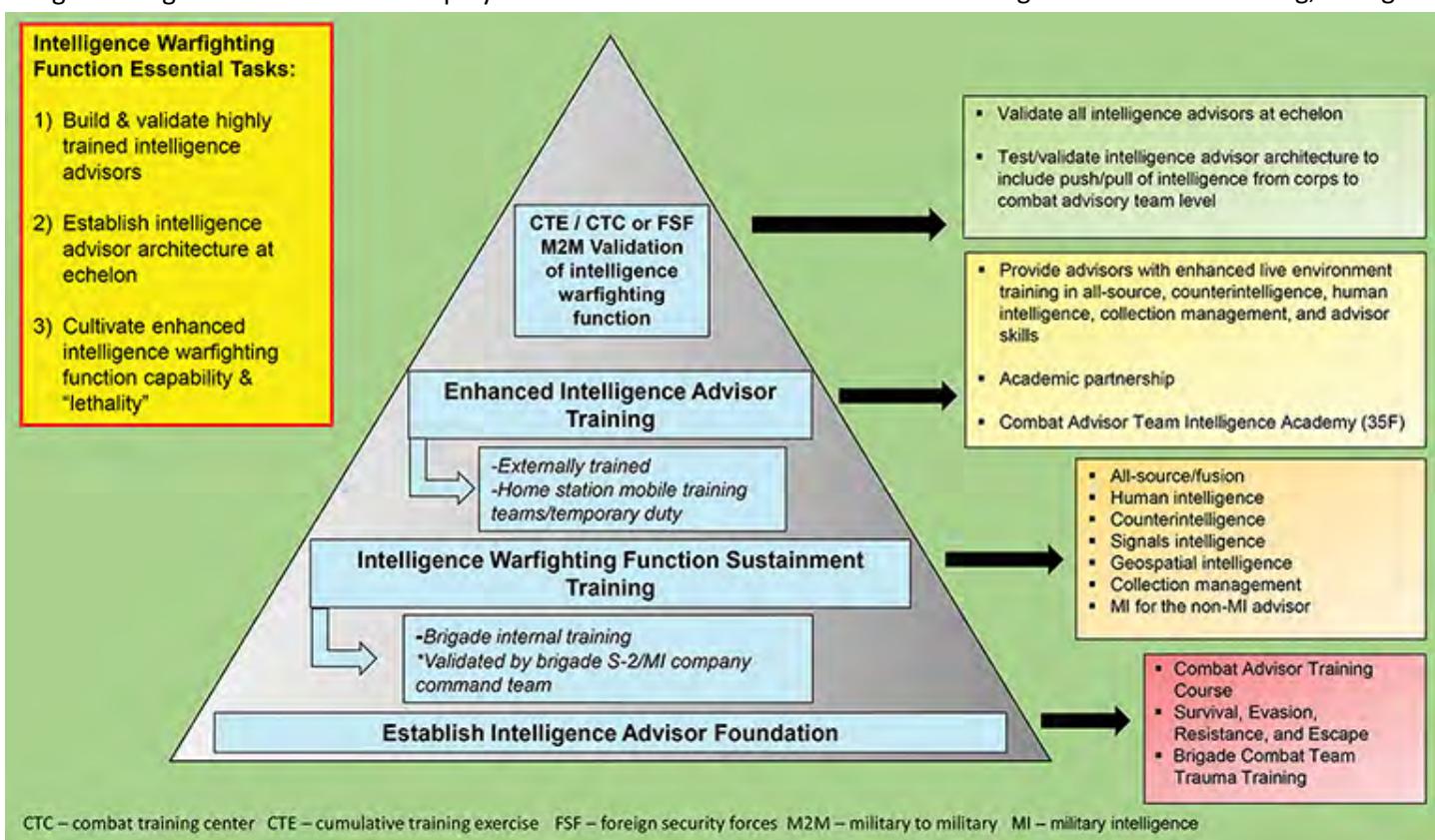


Figure 1. Building an Intelligence Warfighting Function Advisor

The revamped program has drawn heavily from 1st SFAB lessons learned and has increased in scope and duration. Unfortunately, modifications to the SFAB intelligence warfighting function MTOE in 2018 stripped the brigade S-2 and MI company of advisor billets. Now, coding of all positions except the brigade S-2 officer in charge is in operations support roles. This was likely a cost-saving decision due to the expense of the advanced communications kit and sidearm required for advisors as well as the availability of school billets at the advisor academy. The unintended consequence of this decision is that nearly all brigade S-2 and MI company personnel are not authorized to attend the Combat Advisor Training Course although they are the most experienced intelligence subject matter experts (SMEs) in the brigade and are the best suited to execute intelligence advising. 1st SFAB is in the process of requesting a readjustment to advisor coding because the Combat Advisor Training Course is the bedrock starting point on which an advisor is built.

Intelligence Advising Sustainment Training

The next step in building an intelligence advisor is intelligence warfighting function sustainment training, an evolu-

tion of the MI skills refresher training the brigade executed before its deployment in 2018. As the 1st SFAB intelligence warfighting function came together in the summer of 2017, it was clear that many personnel, particularly junior 35Fs at the combat advisor team level, had a limited understanding of intelligence disciplines outside of their unique skillsets. Led by SMEs in the brigade S-2 and MI company, the unit executed a series of brown-bag lunch sessions to “re-green” intelligence personnel on the totality of intelligence disciplines. As with a majority of our predeployment intelligence training, these sessions were abbreviated in scope, yet set a framework for the future.

SFAB intelligence warfighting function sustainment training, shown in Figure 2, reviews the various intelligence disciplines from the “Intelligence 101” level and is designed to baseline attendees with common terms of reference while also covering intelligence warfighting function lessons learned from Afghanistan.

Led by SMEs from the brigade S-2 and MI company, these blocks of instruction are “scalable, scopeable, and repeatable” as the 1st SFAB reconstitutes the intelligence warfighting function of the organization. They also afford

All-Source Intelligence:	Human Intelligence:	Counterintelligence:	
<ul style="list-style-type: none"> <input type="checkbox"/> IPB / MDMP <input type="checkbox"/> Intelligence support to targeting <input type="checkbox"/> All-source fusion <input type="checkbox"/> Analytical bias <input type="checkbox"/> Soldier as a sensor <input type="checkbox"/> IEW overview/intelligence architecture 	<ul style="list-style-type: none"> <input type="checkbox"/> HUMINT mission management <input type="checkbox"/> HUMINT capabilities overview <input type="checkbox"/> Tactical questioning <input type="checkbox"/> Interrogations overview 	<ul style="list-style-type: none"> <input type="checkbox"/> CI mission management <input type="checkbox"/> CI capabilities overview <input type="checkbox"/> Tailored TARP <input type="checkbox"/> Threat vulnerability assessment overview <input type="checkbox"/> CHARCS user training 	
*ANA TAA Lessons Learned	*ANA TAA Lessons Learned	*ANA TAA Lessons Learned	
Signals Intelligence:	Geospatial Intelligence:	Collection Management:	
<ul style="list-style-type: none"> <input type="checkbox"/> Intro to SIGINT <input type="checkbox"/> SIGINT capabilities overview <input type="checkbox"/> SIGINT support to operations <input type="checkbox"/> Low-level voice intercept overview 	<ul style="list-style-type: none"> <input type="checkbox"/> Intro to GEOINT / capabilities overview <input type="checkbox"/> GWS overview <input type="checkbox"/> GEOINT support to targeting <input type="checkbox"/> Map ordering process 	<ul style="list-style-type: none"> <input type="checkbox"/> Collection management <input type="checkbox"/> ISR synchronization <input type="checkbox"/> UAS / ISR overview 	
*ANA TAA Lessons Learned	*ANA TAA Lessons Learned	*ANA TAA Lessons Learned	
ANA CHARCS	Afghan National Army Counterintelligence and Human Intelligence Automated Reporting and Collection System	IPB ISR MDMP MI SIGINT TAA TARP UAS	intelligence preparation of the battlefield intelligence, surveillance, and reconnaissance military decision-making process military intelligence signals intelligence target audience analysis Threat Awareness and Reporting Program unmanned aircraft system
CI GEOINT GWS HUMINT IEW	counterintelligence geospatial intelligence GEOINT Workstation human intelligence intelligence and electronic warfare	*** Also forms foundation of “MI for the Non-MI Advisor”	

Figure 2. SFAB Intelligence Warfighting Function Sustainment Training

opportunities for brigade S-2 and MI company personnel to complete mission essential task list tasks through actual instruction based on programs of instruction they develop.

An added benefit of this instruction is that it forms an exceptional introduction for non-35 series personnel 1st SFAB is currently cross-training to perform intelligence advising/mission command functions at the combat advisor team level until actual 35Fs are recruited. Just this year, 19 x non-35 series personnel have completed a multiday program of instruction titled “MI for the Non-MI Advisor” that provides the organization flexibility in future training and team readiness for deployments. These personnel include 11B (Infantryman), 12B (Combat Engineer), 13F (Joint Fire Support Specialist), 19D (Cavalry Scout), 25U (Signal Support Systems Specialist), 68W (Combat Medic Specialist), 89D (Explosive Ordnance Disposal Specialist), and 91B (Wheeled Vehicle Mechanic).

Enhanced Intelligence Advisor Training Focus

The next level of intelligence advisor training consists of six focus areas, shown in Figure 3, identified as training shortfalls and opportunities during the unit’s deployment to Afghanistan. Key to this training is leveraging the U.S. Army Intelligence and Security Command (INSCOM) Foundry program’s mobile training teams, theater intelligence brigade live environment training, and other temporary duty (TDY) or mobile training team opportunities to meet our training end state.

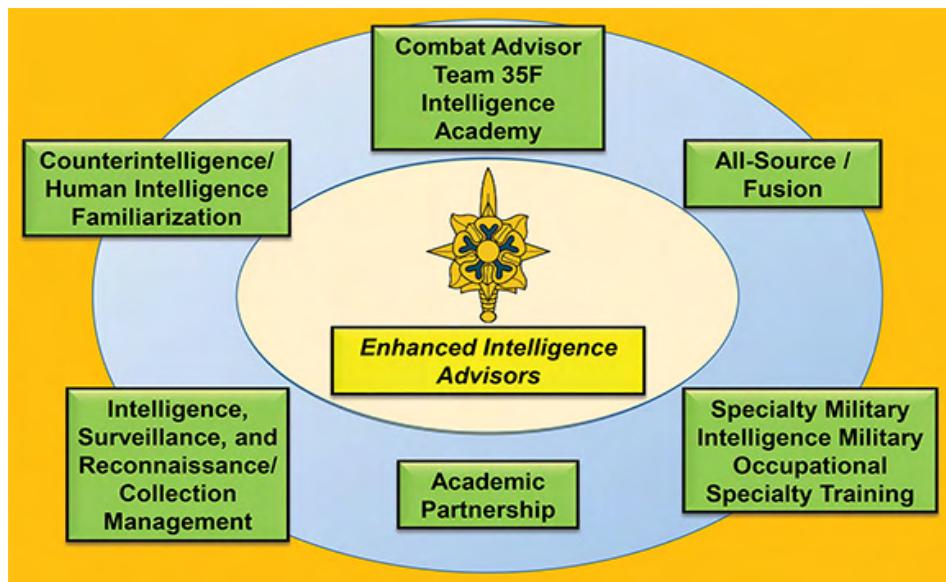


Figure 3. Enhanced Intelligence Advisor Training Focus

Focus Area: Combat Advisor Team 35F Intelligence Academy. This training currently occurs in the aforementioned intelligence warfighting function sustainment training and receives additional augmentation from the Foundry program’s mobile training teams. The 1st SFAB is also looking

at options to send several SMEs to an executive session of the Intelligence Advisor Training Course at Fort Bragg, North Carolina. Considering the 1st SFAB’s current intelligence personnel manning and timeline, it is not feasible to send more than 50 personnel TDY to attend this training; however, leveraging brigade S-2 and MI company personnel in a “train the trainer” capacity is an outstanding way to both standardize and mobilize the program of instruction currently taught at the Intelligence Advisor Training Course.

Focus Area: All-Source and Fusion. Advanced training in all-source analysis and fusion is another focus area. This training was executed recently, leveraging a modified version of the Foundry program’s AS301 and AS302 (All-Source Production) mobile training team courses that focus on the fundamentals of all-source analysis, fusion, targeting, and production but without an emphasis on DCGS-A. The 1st SFAB is also standing up a COCOM analytic initiative using brigade S-2 and MI company all-source personnel to begin establishing contacts and intelligence read books on the various COCOMs in which the SFAB may be employed. Once assigned to a particular COCOM, the COCOM teams will form the foundation of intelligence advising packages and enablers to support forward-deployed advising packages. They will also serve as SMEs to provide predeployment training to deploying combat advisor teams.

Focus Area: CI and Human Intelligence (HUMINT) Familiarization. Based on feedback from intelligence advisors in Afghanistan, the next recommended training focus area is CI and HUMINT familiarization.

The 1st SFAB was fortunate to host modified versions of the HU103 and HU303 courses from the INSCOM Foundry program, which train interpersonal skills for collectors. Although intelligence advisors are obviously not HUMINT collectors, the interpersonal skillsets taught to HUMINT personnel are incredibly relevant to intelligence advisors attempting to establish relationships with foreign security forces. The 1st SFAB is also leveraging CI personnel from the MI company to build out an advanced insider threat exercise and associated training designed to teach combat advisor teams how to properly leverage CI resources

and identify potential insider threats. An additional focus area discussed in detail at the end of this article is the need to train intelligence advisors on report writing skills and the need to provide SFABs with a modified “Defense Strategic Debriefer Course-Lite.”

Focus Area: Intelligence, Surveillance, and Reconnaissance (ISR) and Collection Management. Regardless of COCOM employment, ISR and collection management are areas in which intelligence advisors will always be able to partner with foreign security forces. With recent MTOE adjustments designating several billets at the combat advisor team level with the additional skill identifier Q7 (ISR Manager), which requires attendance at the Information Collection Planners Course, ensuring intelligence advisors at all levels understand ISR and collection management is key. As with the Intelligence Advisor Training Course, it is not feasible for an SFAB to send nearly 50 personnel to the Information Collection Planners Course. A potential mitigation strategy is to again use the Foundry program. The ISR303 Information Collection (ISR) Integration mobile training team can provide instruction on information collection capabilities and staff integration tailored to the SFAB mission. This course of action would not replace attending the Information Collection Planners Course, but would provide some of the knowledge intelligence advisors need to be successful while waiting for formal school attendance.

Focus Area: Specialty Military Intelligence MOS Training. This focus area encompasses niche training such as Joint Counterintelligence Training Academy courses for CI personnel, HUMINT Training-Joint Center of Excellence for HUMINT personnel, and Digital Intelligence Systems Master Gunners Course for 35Ts (Military Intelligence Systems Maintainer/Integrator). One specialty area of training that the 1st SFAB is resourcing, based on lessons learned from Afghanistan, is document and media exploitation. Later in the training cycle, 1st SFAB is also receiving training on open-source intelligence, which is an invaluable tool to maintain situational awareness on multiple areas of responsibility as well as emerging security issues that may negatively affect operations.

Focus Area: Academic Partnership. Facilitated via a partnership with the Military Advisor Training Academy S-2 team at Fort Benning, the 1st SFAB is in the nascent stages of establishing a permanent academic partnership with Auburn University. This partnership will allow the 1st SFAB to tap into the knowledge base of academia to resource COCOM security symposiums while also allowing 1st SFAB members to participate in educational opportunities locally at Fort Benning and via resident opportunities on campus. The 1st SFAB is excited about this emerging partnership and the unique perspective academia can provide to intelligence advisors as they prepare to enter countries in COCOMs with diverse cultural, ethnic, religious, and security issues.

SFAB Intelligence Warfighting Function Way Ahead

Although extremely successful thus far, several areas within the SFAB intelligence warfighting function require additional attention and modification. Aside from the aforementioned intelligence architecture concerns, the intelligence warfighting function MTOE and billet coding are a work in progress.

USAICoE's Position on TOE/MTOE Authorizations

Historically, USAICoE maximizes the use of intelligence authorizations within MI units (e.g., the MI company) rather than the G-2/S-2 section of another proponent's headquarters and headquarters company (HHC) table of organization and equipment (TOE)/MTOE. The personnel assigned to those MI units can always support the G-2/S-2 in an operational control relationship. When the authorizations reside within another proponent's HHC TOE/MTOE, they are more at risk to become bill payers during force reductions.

Author's Rebuttal

While both positions have merit, SFABs are simply different from traditional brigade combat teams and the aforementioned conventional wisdom does not apply. Based on lessons learned and conversations with fellow SFAB S-2s, the author strongly recommends further modifying the MTOE to move the senior warrant officer SMEs for CI, HUMINT, intelligence and electronic warfare, and all-source intelligence from the MI company to the brigade S-2 section. These individuals should be at the center of planning and resourcing MOS-specific training for the SFAB intelligence warfighting function as a whole. They should also function as SME advisors to the brigade S-2, who is the senior intelligence officer for the brigade, as well as advisors to the brigade commander. Finally, as SFABs face a future in which simultaneous employment in multiple COCOMs is a fast approaching reality, these SMEs have a key liaison function with theater intelligence brigades, Army Service component commands, CI coordinating authorities, and HUMINT operations cells. Keeping these individuals in the MI company introduces unnecessary friction/bifurcation of efforts that can easily be solved with MTOE-neutral adjustments.

While highlighted as a success, the cross-training of non-35 series personnel as intelligence advisors represents a slippery slope. Courses of action that rely on cross-trained non-35 series personnel or direct recruiting of non-35 series noncommissioned officers to fill the intelligence advisor billets for the duration of a 3-year assignment will dilute the role and quality of intelligence advisors at the combat advisor team level. Going down this path will inevitably negatively affect the recruitment of 35F personnel, which is already a significant challenge. Ultimately, the foreign security force partners and COCOMs that SFABs support will suffer from a lack of actual intelligence advisors.

As alluded to earlier, the intelligence community needs to explore options to authorize SFAB intelligence personnel to draft their own intelligence information reports (IIRs) as a means to capture advisor debriefs. In Afghanistan, the 1st SFAB benefited from significant HUMINT uplift that will not always be available and has only two HUMINT billets organic to the organization. Modifying the Defense Strategic Debriefer Course into a mobile training team course and achieving consensus within the HUMINT community will allow intelligence advisors to standardize IIRs as the vehicle for capturing key observations from advising operations. This will also allow intelligence advisors to draft IIRs that operational management teams ultimately review and correct for distribution to the greater intelligence community. Such a course of action is a major paradigm shift but presents a unique opportunity for SFABs moving forward.

Finally, the MI Corps must look at how we recruit intelligence professionals, particularly 35Fs. The experience of the 1st SFAB in Afghanistan was not perfect and for some was far from what they envisioned when they volunteered in 2017. However, that is changing, and it is important to get that message out to prospective candidates. On a positive note, right now members of the 1st SFAB intelligence warfighting function are attending unique training such as Air Assault, Pathfinder, and Airborne school. Partnerships with academia, live environment training, and integration into Army Service component command intelligence warfighting function military-to-military events will present opportunities for intelligence analysts to literally see the world. Eventual COCOM alignment will provide stability and certainty to deployment rotations while also affording MI professionals numerous opportunities to advise foreign se-

curity force personnel on the intelligence warfighting function. Advertising these facts to potential volunteers is vital to improving the recruitment of future intelligence advisors at all levels.

Conclusion

Serving as the brigade S-2 of the Army's first purpose-built SFAB has been the experience of a lifetime. Although fraught with long hours, a good deal of frustration, and endless complex challenges, the opportunity to stand up the intelligence warfighting function of 1st SFAB has been exceptionally rewarding. The author is forever indebted to the exceptional sacrifice of the officers, warrant officers, and noncommissioned officers who form the intelligence warfighting function of 1st SFAB and helped make the impossible possible. The mission of advising foreign partners is truly a worthy undertaking and vital to our Nation's security objectives. Advising the intelligence warfighting function will always be a vital component of these efforts and it must continue to grow and evolve in the years to come. What the 1st SFAB accomplished is just the beginning of what will hopefully become one of the MI Corps' greatest accomplishments as senior leaders continue to leverage the SFAB's intelligence warfighting function to meet the requirements of our great Nation.



Endnote

1. Title 10 of the United States Code outlines the role of armed forces in the United States Code. It provides the legal basis for the roles, missions, and organization of each of the services as well as the Department of Defense. "Title 10 of the United States Code," Wikipedia Foundation, last modified 24 March 2019, 23:51, https://en.wikipedia.org/wiki>Title_10_of_the_United_States_Code.

LTC Todd Harkrader was the first brigade S-2 for 1st Security Force Assistance Brigade at Fort Benning, GA. He previously served as the battalion operations officer and executive officer for 2nd Military Intelligence Battalion, 66th Military Intelligence Brigade, and as the operations officer for the U.S. Army Europe G-2 Intelligence Security Cooperation Section. He is currently assigned to the Pentagon in Washington, DC.





Photo by U.S. Army MAJ Ian Fleischmann

The 2nd Security Force Assistance Brigade Command Sergeant Major and the brigade S-2 team with the U.S. Army Intelligence Center of Excellence Chief Warrant Officer and Command Sergeant Major during Joint Readiness Training Center rotation 19-03.

Establishing the Intelligence Readiness of a Security Force Assistance Brigade

by Major Aaron Bragg, Chief Warrant Officer 3 Nick Rife, and Chief Warrant Officer 2 Jay Gaines

Introduction

Establishing readiness within the intelligence warfighting function of a Security Force Assistance Brigade (SFAB) is as challenging as it is rewarding. Between April 2018 and January 2019, the newly established 2nd SFAB's intelligence warfighting function developed a manning, equipping, and training strategy in order to support the brigade's imminent deployment as an advisory element for the Combined Joint Operational Area-Afghanistan. With the assets, resources, and time available, few precedents exist for building an expeditionary advisor intelligence element. Indeed, channeling the advisor attributes of patience and keeping an open mind is the best approach when forging new paths. In that vein, the brigade S-2 leadership devised a three-pillar strategy to gain and maintain a heightened state of intelligence readiness:

- ◆ Build the team.
- ◆ Configure the architecture.
- ◆ Train the intelligence warfighting function.

Subsequent to the establishment of the strategy, intelligence advisors of the 2nd SFAB are postured to enable offensive operations where needed as a vital team member of a globally capable SFAB.

Build the Team

The intelligence advisor operates in an internal and external capacity. The internal mission of the intelligence advisor is to provide timely, relevant, accurate, and predictive intelligence to the team leader or company commander. Externally, the intelligence advisor provides doctrinally sound and operationally relevant intelligence coaching and mentorship to foreign security forces across the unified

land operations spectrum. Ultimately, the intelligence advisor's responsibility is twofold—build a foreign security force intelligence capacity and provide intelligence support to force protection/mission objectives.

Recruiting intelligence Soldiers with a potential for such depth in their craft is a critical component to the intelligence readiness paradigm. Optimally, a 35F (Intelligence Analyst) sergeant or staff sergeant fits the needs of the advisor teams and battalion S-2. A challenge to 2nd SFAB was a critical shortage in qualified 35F volunteers. To close the recruitment gap, 2nd SFAB widened the recruitment aperture to accept 35N (Signals Intelligence Analyst), 35M (Human Intelligence Collector), and 35P (Cryptologic Linguist) applicants. This adjustment to allow additional intelligence military occupational specialties was effective and ultimately contributed to a more holistic intelligence capability brigade-wide. The diversity in experience, the optimized military occupational specialties for team activity (35M and 35P), and the opportunity to cross-pollinate ideas between teams all served to strengthen intelligence warfighting function personnel competencies—building an advisor akin to an intelligence Swiss army knife.

Configure the Architecture

Diverse planning considerations and unique requirements within each combatant command footprint limit the speed at which the intelligence warfighting function can build and maintain situational understanding as conditions evolve. Although digital intelligence capabilities, such as the Distributed Common Ground System-Army (DCGS-A) Service Pack 1, are sufficient at the brigade level, they are less so for the common team level intelligence advisor. Implementing an innovative digital strategy, using software-as-a-service integration concepts, allows the 2nd SFAB to harness theater-unique data sets via unified data layers, accessible on organic communications transport. In other words, while the senior intelligence technician at brigade interacts with data through a DCGS-A multifunction workstation, intelligence advisors rely on a web browser to interact with the same data. This implementation provides user and access simplicity, limiting planning considerations in the mission planning process. Such an approach also provides options to the team as it potentially transitions between multiple combatant commands and as the variability



SSG David Smith records intelligence information at a key leader engagement during the 2nd Security Force Assistance Brigade Live Fire Exercise 2018. SSG Smith graduated the first iteration of the Intelligence Advisor Training Course.

Photo by U.S. Army SSG Josh Brown

and volume of information increases or decreases in accordance with environmental conditions. The core ethos of the advising team's intelligence advisor is “do the most with the least.”

Train the Warfighting Function

Intelligence advisor experience levels within the 2nd SFAB vary greatly. Brigade S-2 leaders implemented a training pipeline to baseline every intelligence advisor in the brigade. Deemed an intelligence reception, staging, onward movement, and integration (RSOI), the training approach took shape by observing 1st SFAB's lessons learned while in the Combined Joint Operational Area-Afghanistan and maintaining consistent contact with enablers at Fort Bragg, North Carolina. These included the Asymmetric Warfare Group, XVIII Airborne Corps G-3 home-station training, Fort Bragg Mission Training Complex, U.S. Army Intelligence and Security Command (INSCOM) Foundry, and U.S. Army Forces Command (FORSCOM) G-2. Intelligence advisor RSOI training events include, but are not limited to—

- ◆ Intelligence Advisor Training Course (FORSCOM G-2).
- ◆ Vulnerability Assessment Methodology (Asymmetric Warfare Group).
- ◆ Digital Intelligence Systems Master Gunner Course (INSCOM Foundry).
- ◆ Biometrics Operations Specialist Course (XVIII Airborne Corps G-3 Home Station Training).
- ◆ Integrated Tactical Network Workshop and Forum (Fort Bragg Mission Training Complex).

Most critically, not all intelligence advisors attended all training opportunities. Competing advisor-specific training events often require advisors to engage with brigade S-2 leadership to ascertain where opportunities exist based on that advisor's strengths and weaknesses.

Ultimately, brigade S-2 leadership could customize each intelligence advisor's RSOI training plan in accordance with training needs and additional non-intelligence training requirements. The resulting advisor competencies reveal a mix of technical and doctrinal intelligence understanding not common among their peers in more traditional career tracks.

Way Ahead

The intelligence advisor lacks organic information collection and processing capabilities at the advisor team level. Analysis of these capability gaps provides opportunities for commercial-off-the-shelf and government-off-the-shelf capability implementations, including the Engineering Link Analysis tool and eBee X small unmanned aircraft system integration.

The Engineering Link Analysis tool enables advisors with a ruggedized tablet for facilitating rapid mission planning, intelligence preparation of the battlefield, and situational awareness, all collaboratively available to foreign security force counterparts at the appropriate classification level. Rigorous and realistic collective training events accompanied by DevOps¹ counterparts allow the 2nd SFAB to evolve the Engineering Link Analysis capability in conjunction with tactics, techniques, and procedures and standard operating procedures.

Intelligence leaders within the 2nd SFAB also implemented use of the eBee X small unmanned aircraft system. Leveraging the National Geospatial-Intelligence Agency, the eBee X (platform name PROMETHEUS01) aids the advisor in collecting unclassified geospatial data to produce tactical decision aids. The eBee X payload renders three-dimensional visualizations of vertical environments in mere minutes. PROMETHEUS01 elevates the advising team's capacity and value proposition by leveraging what the intelligence advisor brings to the team, albeit through an ad hoc approach.

Classified processing capability remains a gap for advisors at the team level. The DCGS-A Capability Drop 1 is the ideal solution for intelligence advisors through its unique ability to trigger standard workflows and automate processes of the tactical user. The 2nd SFAB intelligence warfighting func-

tion has tested and proven DCGS-A Service Pack 1's ability to support brigade intelligence operations. Fielding of Capability Drop 1 will greatly enhance the organization's ability to conduct multi-echelon analysis, closing the information throughput gap that resides at the company advising team and below levels. Capability Drop 1 also builds in flexibility for the advising team leader, as it is a more versatile plug-and-play solution. Operational conditions of the near future could find a team operating independent of the brigade or battalion where the synchronicity of dataflow, the development of the common intelligence picture/common operational picture, and threat indications and warnings must be autonomous processes without a reliance on complex architectures. As currently configured, SFAB intelligence advisors do not have this luxury; however, continued operational testing, validation, and feedback with lessons learned cross-pollinated throughout the SFAB formations will get to such an end state.



2nd SFAB S-2 personnel following the first successful mission profile of PEACOCK01, the eBee X 3D imaging drone. It is the only collection platform organic to SFABs and has proven a critical enabler for tactical advise and assist efforts in Afghanistan.

Photo courtesy of SFC Bill Connolly

Conclusion

The 2nd SFAB's intelligence warfighting function three-pillar strategy (build the team, configure the architecture, and train the intelligence warfighting function) was not without flaw. It met with a truncated timeline for intelligence advisors



Photo by U.S. Army SSG Mike Randazzo

CW3 Nick Rife and CW2 Jay Gaines collaborate on the 2nd Security Force Assistance Brigade intelligence warfighting function digital strategy prior to the execution of the brigade live fire exercise and Joint Readiness Training Exercise 19-03.

to confront operational challenges of today. The intelligence warfighting function team consistently exercised advisor attributes of discipline and maturity as the ambiguity grew more acute leading up to the 2nd SFAB's latest arrival date.

The home station partnerships forged with the FORSCOM G-2, INSCOM Foundry, Fort Bragg Mission Training Complex,

National Geospatial-Intelligence Agency, and Asymmetric Warfare Group undoubtedly elevated the level of training the 2nd SFAB advisors received, and they far exceeded the 2nd SFAB S-2's technical leadership expectations. The home station-heavy approach also limits the costs incurred by the organization and, most importantly, the advisor families. As a framework, 2nd SFAB will continue to leverage the three-pillar approach with a keen eye on the future and where enabling offensive operations might be required in the next theater and beyond. **Everyone Fights!** 

Endnote

1. "DevOps (a clipped compound of "development" and "operations") is a software engineering culture and practice that aims at unifying software development (Dev) and

software operations (Ops). The main characteristic of the DevOps movement is to strongly advocate automation and monitoring at all steps of software construction, from integration, testing, releasing to deployment, and infrastructure management. DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases." D. Jeya Mala, *Integrating the Internet of Things Into Software Engineering Practices* (Hershey, PA: IGI Global, 2019), 16.

MAJ Aaron Bragg is the brigade senior intelligence officer for 2nd Security Force Assistance Brigade (SFAB). His previous assignments were G-2 planner and G-2 analysis and control element (ACE) chief at 82nd Airborne Division, as well as brigade S-2 at 1st Brigade Combat Team, 82nd Airborne Division. He most recently served as deputy ACE chief at XVIII Airborne Corps. His recent campaign support includes Operations Iraqi Freedom, Enduring Freedom, Inherent Resolve, and Freedom's Sentinel.

CW3 Nick Rife is the brigade senior all-source intelligence fusion technician for 2nd SFAB. He has previously served in various duty positions within 82nd Airborne Division where he supported Global Response Force and Operations Enduring Freedom, Inherent Resolve, and Freedom's Sentinel, implementing transformational digital strategies in support of tactical operations. He has also served in U.S. Army Forces Command G-2 as the Digital Intelligence Systems Master Gunner Course officer in charge.

CW2 Jay Gaines is the brigade intelligence support element chief for 2nd SFAB. His previous assignments were with 10th Mountain Division and 3rd Special Forces Group (Airborne). He has supported operations in Afghanistan and the African continent where he advanced his intelligence support to the intelligence, surveillance, and reconnaissance portfolio. Most recently, CW2 Gaines has been involved in implementing 2nd SFAB's global intelligence readiness strategy, which provides the brigade with maximum flexibility in support of expeditionary advising operations.



In October 1962, imagery captured by U.S. Air Force U-2 high-altitude and U.S. Navy low-altitude photo reconnaissance aircraft were key to understanding that Soviet intentions in Cuba were more threatening than previously assessed.

Knowledge Management for Small Teams

by Captain David C. Millikan and Specialist Kaitlin M. McFarlane

Introduction

In February 2018, Combat Advisor Teams 1231 and 1331 and Battalion Advisor Team 140 deployed to Forward Support Base Arena in Herat, Afghanistan. As the farthest west element of the 1st Security Force Assistance Brigade, our unit was responsible for train, advise, assist, accompany, and enable operations in a part of Afghanistan that had not seen a conventional American presence in more than 4 years. Although the original vision for combat advisor teams had been to support Afghan maneuver battalion staffs, we quickly found ourselves advising a brigade commander and a hospital staff led by a one-star officer. This was more than a challenge for a 12-person team that had stood up in July, supported by a 9-man Guardian Angel squadron from 1st Battalion, 28th Infantry Regiment. Adding to the challenge was the fact that every echelon in a Security Force Assistance Brigade serves primarily as an advising unit, rather than a headquarters responsible for

maneuvering subordinate units. While commanders at every level can imagine the problems to which this could lead, one unforeseen problem was the amount of information our team would collect and the difficulty we would have retaining, storing, and presenting the information to advisors for decision making in support of their partners. To this end, our team, along with the staff at Battalion Advisor Team 140, developed a functional knowledge management system to ensure information was shared inside the team, retained for future use, and ready for presentation to outside agencies.

Intelligence Serves as the Center of Gravity

Upon arrival at Forward Support Base Arena, all three teams found themselves under the command of Italian advisors at the North Atlantic Treaty Organization (NATO) Train Advise Assist Command-West, leading advising efforts in Herat with the Afghan National Army's 207th Corps.



Photo by U.S. Army CPT Adam Hendriks

The Afghan National Army's 207th Corps and the Afghan National Police's 606 Zone join Train Advise Assist Command-West for a three-day operational planning conference at the mission planning facility on Camp Arena, 7-9 July 2018. 1st Security Force Assistance Brigade advisors assigned to TAAC-West guide their Afghan partners through the military decision-making process. The brigade advising team from 4th Battalion, 1st SFAB showed their corps and brigade partners how to integrate a wide range of military skills like intelligence, field artillery, and logistics into a comprehensive operational plan.

While Combat Advisor Team 1331 and Battalion Advisor Team 140 were assigned to support expeditionary advising platform missions and targeting, Combat Advisor Team 1231 found itself advising at the Regional Military Training Center, where Afghan soldiers received training following graduation from basic training in Kabul. Since no American unit was available to provide us with a relief in place, critical to our success or failure on Camp Zafar, the headquarters of the 207th Corps in Herat, was the need to catalog information about training, logistics, and administration—there would be no time to ask questions twice. To handle this problem, we assigned the responsibility for knowledge management to our intelligence advisor.



SFC Jeremiah Velez, left, and CPT David Zak, center, both advisors with the 1st Security Force Assistance Brigade's 3rd Squadron, speak with their Afghan National Army counterparts during a routine fly-to-advise mission at Forward Operating Base Altimur, Afghanistan, September 19, 2018.

The intelligence warfighting function “facilitates understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment.”¹ As such, intelligence serves as the center of gravity for all advising activities. Without an understanding of the problem, advisors cannot recommend solutions; just as without tactical and technical expertise, advisors cannot expect their advice to be trusted or acted upon. Because of our limited personnel, only a small number of advisors could work with Regional Military Training Center staff during our engagements.

To ensure the sharing of information across the team, we instituted post-mission debriefs, chaired by the intelligence advisor. Meetings generally followed the same format: a detailed description of the advising engagement, along with any due-outs or requests made by our partners, followed by a discussion of atmospherics by the Guardian Angel squadron leader. As necessary, U.S. counterintelligence and countercorruption teams attended these meetings. When discussing our partners, advisors made sure to

share not only information concerning operations but also personal details about our partner’s families, frustrations, likes, and dislikes. We’re not recommending that you reduce your partners to a set of data points to collect. We are however recommending that forging a personal relationship with your partner is as important to building trust as it is to demonstrating technical and tactical competence. At the conclusion of the meeting, the intelligence advisor compiled the report and collected any documents brought back for translation, while the operations advisor added due-outs to the task tracker for execution and follow-up. The remainder of the advisors then began scheduling their next engagements. Given the fast pace of daily advising operations, this was the only regular meeting attended by all members of the team, and as such was never skipped or rescheduled.

The Advisor Network Report

At this point, the intelligence advisor began building the Advisor Network (ANET) report. This was our primary touch-point with higher-level Train Advise Assist Command-West advisors, and after each mission, the Battalion Advisor Team 140 reviewed the report. Although we could have simply dumped the debrief into ANET, the intelligence advisor took the time to rewrite the report. This ensured

important information was clearly identified to other agencies on ANET and avoided confusion for any non-English speakers reading the report. A reality of coalition warfare is the need to communicate complex ideas as simply as possible—there’s no room for nondoctrinal terms or huge blocks of text. Once approved, the reports posted to ANET became available to users for review, and we began to receive requests for information from a variety of agencies. These requests came from the Joint Expeditionary Team asking to join us during follow-up engagements, the National Geospatial-Intelligence Agency requesting refined coordinates to different locations, and planning staffs at Resolute Support Mission asking for updates on programs they were running from Kabul. In short, we found ourselves in the position of the primary American information-gathering unit to the 207th Corps. These requests for information were assigned to advisors to answer during later engagements.

Managing Translation Tasks

The intelligence advisor’s next task was to translate documents gathered during the engagement. Very quickly,

we learned two things: first, any documents not digitally scanned and saved would eventually disappear; and second, each translator was best suited for a different type of translation. Local nationals were more skilled at understanding slang and military terms; category III linguists worked well translating formal letters; and military occupational specialty 35L (Counterintelligence Agent) linguists handled data entry and word processing. As mundane as this sounds, there was nothing more embarrassing or detrimental to our partners' trust as having to ask for copies of documents they had already provided us. On the positive side, having a quick turnaround on document translation allowed us to ask more meaningful questions and to better understand the problems our partners faced.

Eventually, we taught our 35L to re-create the translated documents in Microsoft Word, rather than returning the document to us with a handwritten translation. This decreased the time it took to get these documents in front of decision makers and helped to eliminate some of the translation errors we were seeing. With regard to translation work, we recommend—

- ◆ Use a standard format for translators' notes, which will help you to know when a translator is unclear on the meaning of a word, or if there is a cultural nuance to the translation that you might miss.
- ◆ Make it clear to translators what your priority is.
- ◆ Identify how much time the translators should spend on a document.
- ◆ Develop a system to track which documents they are translating.
- ◆ Provide direct guidance to your translators on your intent.

Relief-in-Place Planning

From here, the team had enough information to answer requests for information, seek guidance from supporting agencies (especially Finance and the Joint Engineering Cell), and move forward to support our partners. After a couple months of advising, the process became self-sustaining, and we began to have more questions than we could answer. Working closely with the corps-levels helped us to determine which questions would be the most productive

to spend our time on. At this point, the team began compiling our own relief-in-place guidebook, detailing on-post and off-post agencies, and including everything we had come to know about our partners using Train Advise Assist Command-West's baseball card format. More than being an introduction to Herat, it was our hope that a well-done re-



SFC Christopher Davis, an advisor with 1st Security Force Assistance Brigade, teaches a map reading class to Afghan soldiers September 18, 2018. In his first advising role, Davis built up an artillery leader's course and a land navigation and reporting course for Afghan soldiers. He has also taught them on their communications systems as part of the brigade's advising efforts.

U.S. Army photo by Sean Kimmons

lief-in-place guide would allow any follow-on units to avoid the slow start we had gone through. It would also allow the team to continue the mission in the event an advisor was needed to support a mission in a different area of operations. The sooner relief-in-place planning begins, the better. We cannot stress enough the value of having every advisor and Guardian Angel write down anything they do not know—the incoming unit will have the same questions. Do not wait until you know everything, because by then, you will have forgotten what it was like to know nothing.

Knowledge Management

While the intelligence advisor managed the knowledge management process of our team, other team members were responsible for different parts of the system. To begin, the team leader was responsible for designing the overall framework for the system and ensuring quality control of the outputs. Supporting this was the signal advisor, who was responsible for building the technical parts of the system. Ensuring someone on your team is able to build an online repository for the information and transfer information across domains is extremely useful. During our deployment, we found SharePoint to be an effective system, especially when working with other U.S. units, although it can be

difficult to transfer information to non-U.S. domains used by NATO partners.

Having developed a system to collect, retain, and use information, what can a small team do to improve on this system? As useful as it would be to use a Microsoft Access database to record information on our engagements, knowledge management systems are only useful if they outlive their creators—if the unit replacing you is unable or unwilling to use your system, you have wasted your time creating it. As long as ANET is the system of record for collecting engagement reports, small teams use simple systems that reinforce ANET, not undermine it.

Conclusion

While knowledge management is generally thought of as something to be practiced at the battalion level and higher, teams at any level can effectively use the iterative process of assess, design, develop, pilot, and implement to guide deci-

sion making. It is especially useful when prioritizing the limited time available to small units operating without robust staff oversight. Ultimately, advising at the combat advisor team level is a people-focused profession, not a product-focused one. By processing information quickly and getting it where it needs to go, teams can spend more time developing trusting relationships with their partners, and less time stuck behind a computer. 

Endnote

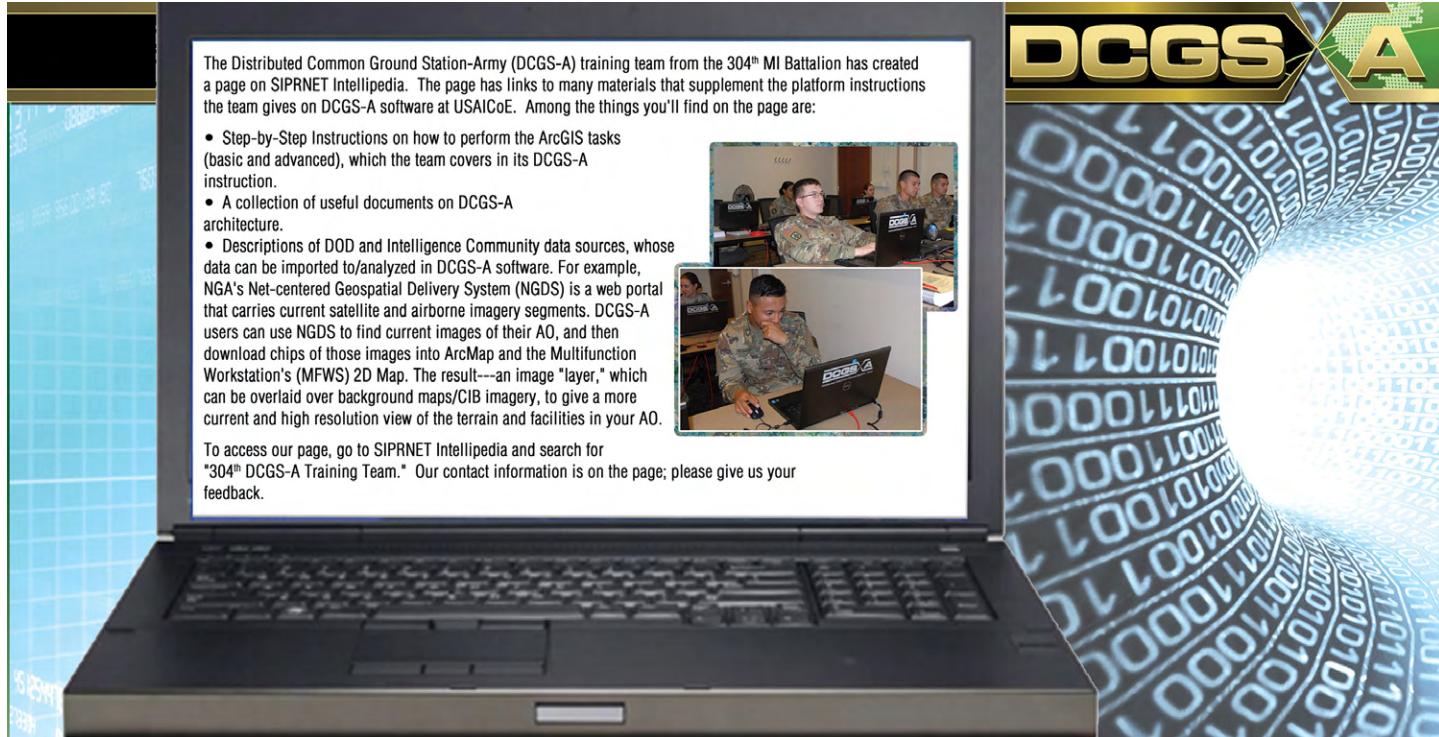
1. Department of the Army, Army Doctrine Reference Publication 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 5-4.

Reference

Department of the Army. Army Techniques Publication 6-01.1, *Techniques for Effective Knowledge Management*. Washington, DC: U.S. GPO, 6 March 2015.

CPT David Millikan currently serves as a team leader on Combat Advisor Team 1231. His previous assignments include platoon leader and executive officer at the Joint Multinational Readiness Center in Hohenfels, Germany; Deputy Branch Chief for Training Support at the Mission Command Center of Excellence in Fort Leavenworth, KS; operations officer while deployed with Special Operations Planning and Liaison Element-Afghanistan; brigade assistant operations officer with 2nd Infantry Brigade Combat Team, 4th Infantry Division, Fort Carson, CO; and Commander, Delta Company (WPN), 1st Battalion, 41st Infantry Regiment. He has deployed to Afghanistan three times.

SPC Kaitlin McFarlane currently serves as an all-source intelligence analyst with the 10th Mountain Division. She served as an intelligence advisor on Combat Advisor Team 1231 during 1st Security Force Assistance Brigade's inaugural deployment to Afghanistan, where she managed intelligence targeting collection operations in Herat.



The Distributed Common Ground Station-Army (DCGS-A) training team from the 304th MI Battalion has created a page on SIPRNET Intellipedia. The page has links to many materials that supplement the platform instructions the team gives on DCGS-A software at USAICoE. Among the things you'll find on the page are:

- Step-by-Step Instructions on how to perform the ArcGIS tasks (basic and advanced), which the team covers in its DCGS-A instruction.
- A collection of useful documents on DCGS-A architecture.
- Descriptions of DOD and Intelligence Community data sources, whose data can be imported/analyzed in DCGS-A software. For example, NGA's Net-centered Geospatial Delivery System (NGDS) is a web portal that carries current satellite and airborne imagery segments. DCGS-A users can use NGDS to find current images of their AO, and then download chips of those images into ArcMap and the Mifunction Workstation's (MFWS) 2D Map. The result—an image "layer," which can be overlaid over background maps/CIB imagery, to give a more current and high resolution view of the terrain and facilities in your AO.

To access our page, go to SIPRNET Intellipedia and search for "304th DCGS-A Training Team." Our contact information is on the page; please give us your feedback.

DCGS A

Interesting Things Happen at Intersections

by Captain William J. George

Introduction

Since the inception of the 1st Security Force Assistance Brigade (SFAB), people have asked me, “What is it like to be in the SFAB?” My reply vaguely describes the unit’s accomplishments over the past 18 months. The more difficult question to answer is, “What is it like being an S-2 in the SFAB?” My experience as a squadron S-2 leads me to respond by highlighting the advising aspects of the job or the traditional intelligence support. In many ways, the newness of the SFAB seems to cloud people’s perspective of the SFAB’s original purpose, which typecasts its members in the role of advisor or support personnel.¹ Neither fully embodies the essence of an intelligence advisor, and during deployments the reality lies somewhere in between. One of the greatest challenges that an SFAB S-2 faces is balancing the role and responsibilities of senior intelligence advisor and primary staff member. If I had one phrase to describe my experience in navigating these challenges, it would be that “interesting things happen at intersections.”²

This article describes various aspects of being an SFAB intelligence advisor, and it highlights experiences from the 1st SFAB’s recent deployment to Afghanistan. The article—

- ◆ Illustrates how doctrinal tasks affect the intelligence professional.
- ◆ Describes the difference between an intelligence advisor’s internal and external functions.
- ◆ Illustrates how the intelligence advisor’s internal and external functions can directly affect one another in relation to the operational environment influences.
- ◆ Describes how to assess a foreign security force and establish advising goals.
- ◆ Discusses the intelligence advisor’s role in the intelligence community.

Internal and External Functions of an Advising Team Member

ATP 3-96.1, *Security Forces Assistance Brigade*, divides the functions of an advising team member into two



Advisors from 3rd Squadron, 1st Security Force Assistance Brigade alongside their partners from the Afghan National Army’s 4th Brigade, 203rd Corps in front of their Persistent Threat Detection System, in Logar Province, Afghanistan.

subcategories: internal and external, as shown in Figure 1.³ The internal functions are recognizable to any primary staff member, and the external functions are primarily advisor centric.

Operational Environment's Influence

The impact of the operational environment and its ability to alter the distribution of an SFAB S-2's internal and external advising functions cannot be overstated. *Balancing the internal and external advising functions in the SFAB is not only a requirement but also an essential aspect of advising for the intelligence warfighting function.* In a permissive environment, intelligence advisors may find they are only required to conduct external advising functions, with some internal functions not being applicable.⁴ For example, at larger bases in Afghanistan, the preexisting infrastructure provides many of the internal functions of intelligence advisors, limiting their need to complete these tasks themselves. In a less permissive environment or in situations where the advising team is responsible for the majority of the internal functions, like at the smaller manned forward operating bases, the execution of internal functions may be

the higher priority for the intelligence advisor. Figure 2, on the next page, shows the balancing of functions in permissive, semi-permissive, and hostile environments.

As we deployed to Afghanistan, it became apparent that we would be heavily involved with both sides of the spectrum. I found myself filling the role of senior intelligence officer for a forward operating base that grew from 400 to 1,200 service members. It can be frustrating to find yourself working on these internal functions because it is easy to inaccurately view these functions as contradictory to your role of advisor. Despite the frustration, *it is imperative to view these functions as complementary to improving your ability to advise security forces in the region.* All the efforts in base defense, construction of a targeting process, and management of intelligence, surveillance, and reconnaissance are key to understanding the environment. This understanding allows advisors to provide their partners with guidance that is not constructed in a vacuum.

As a minimally manned intelligence section consisting of one 35F (Intelligence Analyst) and one 35D (All-Source Intelligence Officer) responsible for an entire squadron of

Intelligence Advisor Functions	
Internal	External
<ul style="list-style-type: none">• Advises the team leader on intelligence.• Monitors routine situational updates (weather, road conditions, and recent activities).• Provides reach back capability to leverage multidiscipline, multi-echelon intelligence enablers in support of advising team operations.• Maintains the cultural calendar and advises the team of key dates and significant activities.• Trains and advises the team in the use of biometric and forensic equipment used in tactical site exploitation.• Advises on the intelligence preparation of the operational environment to support operations.• Advises on the preparation of the information collection plan.• Assists the team with collecting information for required reports during missions.• Coordinates through higher headquarters for counterintelligence support for insider threat, antiterrorism, and force protection assessments.• Provides input for training assessments.• Assists with monitoring the accountability for, and welfare of, interpreters.	<ul style="list-style-type: none">• Advises the foreign security forces' (FSF) intelligence section.• Advises the FSF on using intelligence assets.• Advises the FSF on processing tactical information into predictive analysis.• Supports intelligence for the FSF combat operations.• Supports intelligence briefings to the FSF commander.• Integrates intelligence reporting with joint, interagency, intergovernmental, and multinational partners' intelligence enterprises, where allowed.• Shares intelligence and information with joint, interagency, intergovernmental, and multinational partners according to foreign disclosure officer approval when allowed.• Adheres to the principles and tactics, techniques, and procedures of effective cross-cultural communication, problem solving, and conflict resolution.

Figure 1. Intelligence Advisor Functions

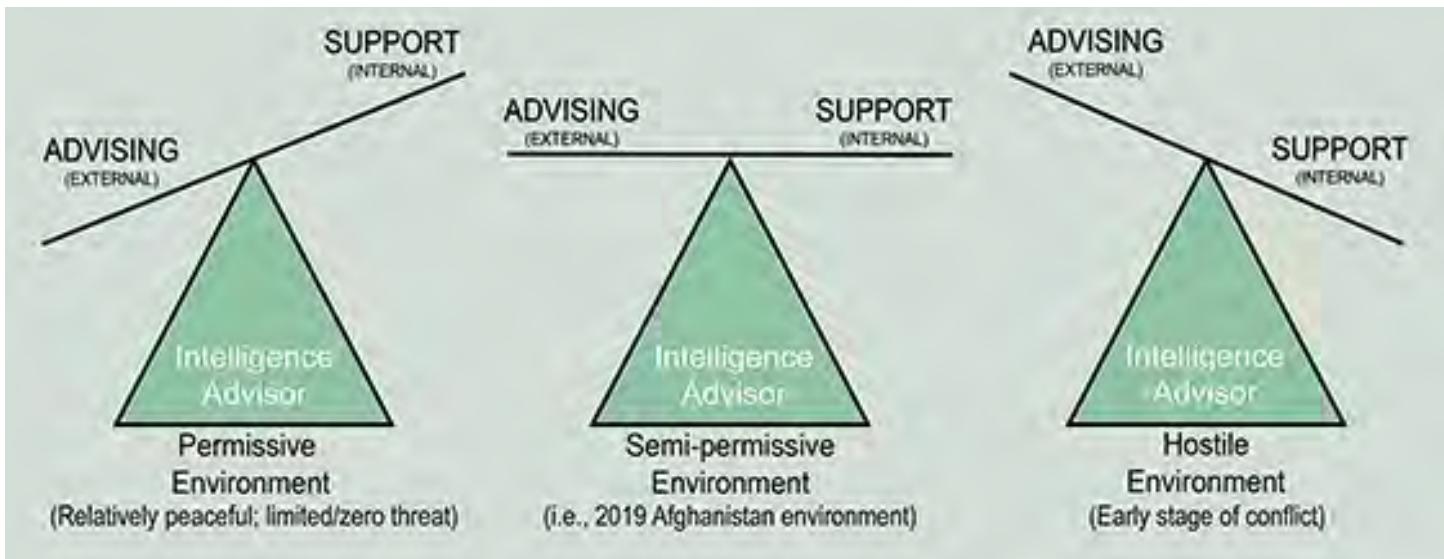


Figure 2. Operational Environment's Influence on the Intelligence Advising Functions

advisors, it was critical for us to find ways to increase proficiency while eliminating the need for additional manpower. The best way for us to achieve this was to understand that *every task we completed had to result directly in an advising effort*. Many of the ways we improved proficiency were simple and in many cases just required a mindset change. One way we accomplished our goal was by creating a team at our base, merging three conventional units into a makeshift intelligence section that could incorporate several civilian advisors, and coordinating with collocated special operations forces. Creating this team helped our future advising efforts.

The most tangible example of this was our effort in improving base defense. As everyone understood, force protection came first and was a prerequisite to accomplish our advising efforts. As we arrived in Afghanistan, an indirect fire threat commandeered a lot of our time, and until we built our base-wide intelligence team, the responsibility fell to my small shop of two to address the problem. Instead of viewing this as an obstacle to achieving our advising mission, we had to develop ways of addressing the various threats in our area while maximizing effectiveness. By harnessing several core advisor imperatives,⁵ we were able to capitalize on the resources and personnel around us to accomplish our advising mission.

A lesson learned about balancing the internal support functions and the external advising functions is to *leverage the work accomplished in your internal functions against your advising efforts*. One example is understanding the threat in your operational environment, specifically in terms of what you expect to be your most likely/dangerous course of action. Execute your normal duties, build your most likely/dangerous course of action, and once completed instruct a

class on how to execute your methodology. By doing so, you develop a rubric with which to compare your counterpart's end product. This process will be mutually beneficial by allowing collaborative work to improve force protection for both forces, and it will achieve both your internal and your external functions.

Assessing Your Partner and Establishing Goals

Assessing your partner and establishing your advising goals should be the first thing you do when entering a theater. Advisors cannot undervalue the importance of this initial assessment. It is the foundation for everything you will achieve during the deployment. You must synchronize assessing your partner and establishing goals because completing these tasks independently of one another will only impede progress and you will find yourself having to start again after having wasted precious time. Understanding your partner's capabilities and priorities is integral to developing your priorities. Doing so will allow for greater success in working with your partner because your investment in their goals bolsters their confidence in you (their advisor) and subsequently their confidence in the advising relationship. Key to establishing your goals is not to overreach your counterpart's capabilities. If you take a simple task for granted, your goals may not be feasible.

A piece of advice that I can offer a future intelligence advisor is to understand your partner's culture and its effect on their decision-making process. Understanding the Afghans' desire to reciprocate gifts and favors provided me the opportunity to share intelligence with my partner and get a response in kind. This sharing of intelligence became crucial to our understanding of the environment. In some cases, the intelligence provided led to our successful interdiction of several indirect fire attacks on our forward operating base.

One of the greatest lessons learned that I can offer an advisor as he/she sets advising goals is to “find the easy win.” It is critical to approach advising with realistic expectations about how you can assist your counterpart. Identifying your counterpart’s priority project will increase their buy-in to your advising relationship. An example of an easy win that we experienced while assisting our Afghan brigade counterparts was in improving the functionality of their Persistent Threat Detection System. This example illustrates an advising effort that was simple for us to influence and provided immediate positive feedback. It instilled a lasting resource for our counterpart.

Find the Easy Win

Our Afghan counterparts were proficient in maintaining and operating the Persistent Threat Detection System but lacked the ability to monitor and sync this capability with their operations center. As a joint advising effort with intelligence, operations, and signals advisors, they located the problem and determined that a technical issue with the information feed prevented the transmission into the operations center. With little effort, this slight technical problem was corrected and our partners had live video feed in their operations center. Within a week of the fix and with some minimal guidance on collection management, the brigade tracked five individuals as they emplaced a daisy chain of three improvised explosive devices (IEDs) at a school and voter registration site. The Afghan S-2 section monitored the individuals’ movements from emplacement back to their production site. They also coordinated efforts in their joint operations center to deploy their quick reaction force and explosive ordnance disposal element. All five individuals were detained along with the components at their production site, and the IEDs were disarmed with no casualties. This example illustrates an advising effort that was simple for us to influence. It also provided immediate positive feedback and instilled a lasting resource for our counterpart.⁶

In working toward assisting my counterpart in collection management, I found myself back-peddling and reestablishing goals because I looked at the basic aspects of my profession, like understanding the importance of leveraging multiple intelligence disciplines, and assumed my counterpart was proficient. Collection management became a long-term goal, and the focus shifted to establishing systems that allowed for the simple management of two intelligence disciplines rather than one. Understanding your counterpart’s historic effectiveness in the unit is also important in order to assess your partner correctly. An example of this existed in our partner’s chain of command, which prevented the staff from providing assessments. Therefore, setting an advising goal of getting my partner to develop multiple courses of

action for future operations would have been futile because his leadership would not have accepted his recommendations. Instead, we set our goals on increasing their ability to analyze and assess the environment to better disseminate intelligence to his battalions.

The Intelligence Advisor’s Role in the Intelligence Community

I want to highlight an aspect of the SFAB that has not been fully explored, which is codifying the intelligence advisor’s role in the intelligence community. In many ways, the intelligence advisors in the SFABs are like a new piece of hardware available to the intelligence community. In some cases, *these advisors may be the only intelligence professionals with access to a particular foreign security force*, giving them a unique ability to answer priority intelligence requirements and specific information requirements with regard to their host nation’s capability.

The recent deployment to Afghanistan revealed intelligence gaps left in the wake of the 2014 troop drawdown. In many ways, we were filling intelligence gaps that no other intelligence discipline or organization had the ability to do. This proved crucial in assisting our partners across eastern Afghanistan to synchronize efforts in preparing the environment for successful parliamentary elections. An intelligence advisor can greatly influence the intelligence community by fully using opportunities to communicate up and down the Advising Network.⁷ This allows intelligence advisors at the kandak (battalion), brigade, and corps levels to verify information as it travels inside the Afghan chain of command.

At the core of this problem is establishing the level of output the intelligence community reasonably should expect intelligence advisors to provide in terms of synthesized intelligence without overwhelming the advisor’s ability to fulfill the primary role of assessing, advising, supporting, and liaising with the foreign security force. It would be a misappropriation for the intelligence advisor to rely completely on the existing intelligence apparatus in their area of operations for analysis. I argue that there are aspects of collated intelligence production which the advisors themselves should produce because they are the lone subject matter experts. By doing so, the intelligence advisor acts as a force multiplier freeing up intelligence support in the area for other mission sets. In an environment where the theater has personnel constraints, the intelligence advisor’s unique ability to advise their counterparts, while simultaneously producing intelligence, provides an additional capacity and flexibility to the regional command and to the Department of Defense as a whole.

Conclusion

Balancing the internal and external advising functions in the SFAB is not only a requirement but also an essential aspect of advising for the intelligence warfighting function. It is imperative to view the internal advisor functions as complementary to the advising mission set. These functions can produce a hectic environment, but with the application of the right tools, systems, and processes, these issues transform from challenges into opportunities. Although the operational environment influences the distribution of these functions, understand that the division of these functions is not set. The operational environment shifts the focus and at times blurs the line between the internal and external functions. If you see everything as an advising effort, the frustration that may result from attempting to balance these functions will be limited.

Future mission sets will contribute to the ever-shifting life of an SFAB advisor and will provide additional context and lessons to continue to shape both doctrine and best practices that intelligence advisors use. The broad yet focused experiences of being an SFAB S-2 will continue to shape my effectiveness as an intelligence professional, and I am looking forward to the next mission set because “interesting things happen at intersections.”



Endnotes

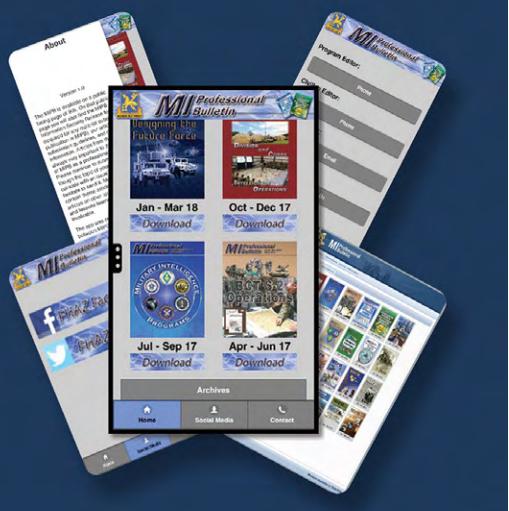
1. For the purpose of this discussion, *support* refers to the members of the Security Force Assistance Brigade who focus more on support than advising.
2. In a conversation with the author, in Logar, Afghanistan, 2018, Kyle Oman (U.S. contractor) used the phrase “interesting things happen at intersections.”
3. Department of the Army, Army Techniques Publication (ATP) 3-96.1, *Security Force Assistance Brigade* (Washington, DC: U.S. Government Publishing Office [GPO], 2 May 2018), 1-22–1-23.
4. Ibid., 3-7.
5. Department of the Army, ATP 3-07.10, *Advising Multi-Service Tactics, Techniques, and Procedures for Advising Foreign Security Forces* (Washington, DC: U.S. GPO, 13 November 2017), 33.
6. Matt Fontaine, “Afghan Army Captures IED Maker, Prevents Attack on School, Voting Center,” Resolute Support Afghanistan, North Atlantic Treaty Organization, 19 July 2018, <https://rs.nato.int/news-center/feature-stories/2018-feature-stories/afghan-army-captures-ied-maker--prevents-attack-on-school--voting-center.aspx>.
7. The *Advising Network* is an established hierarchy, in which advisors complete their external advising functions at multiple echelons, providing the ability for communication and solution of problems at echelon. For example, in Afghanistan the network consists of the kandak (battalion), brigade, and corps level.

CPT William George is currently the S-2/Intelligence Advisor for 3rd Squadron, 1st Security Force Assistance Brigade, at Fort Benning, GA. Previous assignments include 2nd Brigade Combat Team, 1st Infantry Division, S-4, and company executive officer. He has a bachelor of arts in history from the University of Florida and a master of arts in military history from Norwich University.

Military Intelligence Professional Bulletin (MIPB) presents information designed to keep intelligence professionals informed of current and emerging developments within intelligence.

MIPB mobile APP is now AVAILABLE for Android and iPhone

The APP can be accessed by going to <https://play.google.com> (for Android) or the Apple App Store (for iPhone) and searching for MIPB.





U.S. Army photo by MAJ Matt Fontaine, 1st Security Force Assistance Brigade Public Affairs

Leaders from Train Advise Assist Command (TAAC)-Capitol, TAAC-East, and Task Force Southeast, receive an operations and intelligence overview brief from the Task Force Southeast intelligence and operations staff at Advisor Platform Lightning, Paktiya Province, Afghanistan, in June 2018. The leaders from Turkey and the United States discussed common strategies to train, advise, assist Afghan National Defense Security Forces in their three geographic areas of responsibility.

SFAB Geospatial Intelligence Support: Advising the Afghan National Army

by Chief Warrant Officer 3 Jason A. Schelte

Introduction

The U.S. Army's 1st Security Force Assistance Brigade (SFAB) G-2 geospatial intelligence (GEOINT) section conducted a train, advise, and assist mission with the Afghan National Army (ANA) G-2 from March to October 2018. The section was assigned to Afghanistan's Task Force Southeast area of operation. The initial focus was to provide mission command to the ANA 203rd Corps Headquarters; however, the team also found an opportunity to train, advise, and assist the topographic section within the 203rd Corps G-2, which consisted of one officer and one noncommissioned officer. The objective was to assess the topographic section's processes and capabilities in the following areas and to recommend improvements:

- ◆ Software programs.
- ◆ Data management for intelligence reports.

- ◆ Requests for information.

- ◆ Computer hardware and printers.

- ◆ Expendable supply requests.

The team also conducted engagements with the ANA G-2's targeting, plans, and analysis sections, eventually integrating with those same sections in the military intelligence kandak (battalion) of the ANA 203rd Corps.

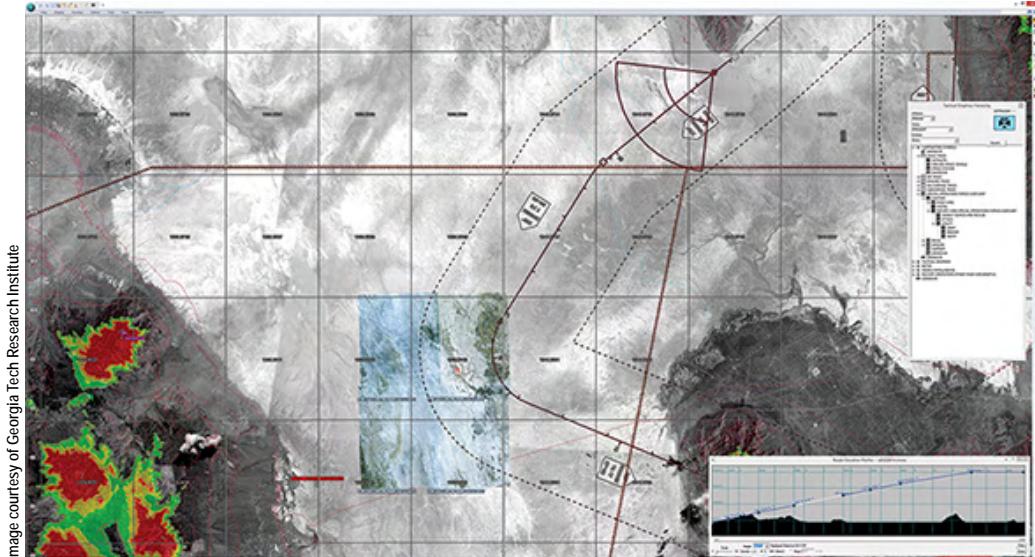
During the deployment, mission command requirements at times conflicted with the SFAB advisors' scheduled activities with the ANA, prompting the question of how best to prioritize the SFAB's advising responsibilities.

FalconView

After completing some of the initial evaluation of the ANA, advisors began more in-depth training on systems. The topographic section had a rudimentary understanding

of FalconView, which was their only source of mapping software. It was built into all the 203rd Corps G-2 section's baseline computers; however, the section used old digital map data using Russian text within FalconView. All the sections within the ANA G-2 wanted to learn new techniques for building their products so that they could meet their mission requirements. Most of the ANA G-2 enlisted soldiers and a few officers attended the training. The G-2 advisor team encouraged the ANA to practice using the software to be able to train future G-2 soldiers.

By the end of the deployment, it was clear that the number and quality of products the ANA G-2 were producing had increased significantly. The targeting section created quality products that supported air strikes, and the analysis section built products that displayed friendly and enemy disposition. The plans section created products that were far better than the hand-drawn scheme of maneuver templates they were previously using.



FalconView provides pilots with maps that help them anticipate what they will find as they carry out a mission. In addition to topographical information, the maps include obstacles, enemy positions, and other changing information.

Google Earth

The topographic section had no knowledge of Google Earth or typical mapping software such as ArcGIS or QGIS, and it was clear the ANA needed a common operational picture. The ANA Corps' joint operations center had no practical way to view, update, or display current, or historical, enemy and friendly activity. They needed a better way to have situational awareness of the battlefield. The method had to be able to display enemy and friendly locations, as well as show unit boundaries. The joint operations center also needed to be able to share their common operational picture so that other echelons could use the same information. The previous method was to use a large, wall-size, hardcopy map and a ladder. They rarely updated the

large overview map, other than the major military facility locations. That method also created a problem with finding precise coordinates because it was difficult to get anything more accurate than a six-digit military grid reference system (MGRS) grid from the large wall map.

The SFAB G-2 GEOINT advisors suggested Google Earth as the best possible solution to fulfill their needs for a common operational picture. The introduction of Google Earth led to several new tactics, techniques, and procedures that the ANA began to use to keep up with and maintain current and historical situational awareness.

SFAB advisors were able to locate a version of Google Earth that was usable on stand-alone computers. This was helpful for ANA soldiers who had no internet capability. The drawback to the offline version was that the ANA would not be able to share the information or products they created unless they had CD/DVD burning capability or a USB hard drive. Google Earth later became part of the basic build for the computer workstations. Using an internet connection with Google Earth meant we could update the program and use it in Dari.

Now that some members of the ANA use Google Earth to create their products, commanders are getting a better picture of where the significant activities (SIGACTs) are taking place in their battlespace. At the time of the SFAB's redeployment in November 2018, the ANA were creating a SIGACTs report plotting the top three or four SIGACTs for discussion. The preferred method is to plot all

SIGACTs on Google Earth to give the commander a better understanding of activities in the area of operation. The joint operations center's floor officer in charge could still discuss the three or four main points but also display all activity. This would lead to a greater understanding of activities in the area of operations. Then, once records are kept over time, the ANA could potentially see patterns, historical information, and trends, thereby enhancing predictive analysis.

The 203rd Corps G-2 is responsible for enemy and friendly location updates on Google Earth. The near-term goal was for the G-2 to be responsible for updating enemy activity and for the G-3 to be responsible for updating friendly activity. The long-term goal is to have the four brigade S-2s

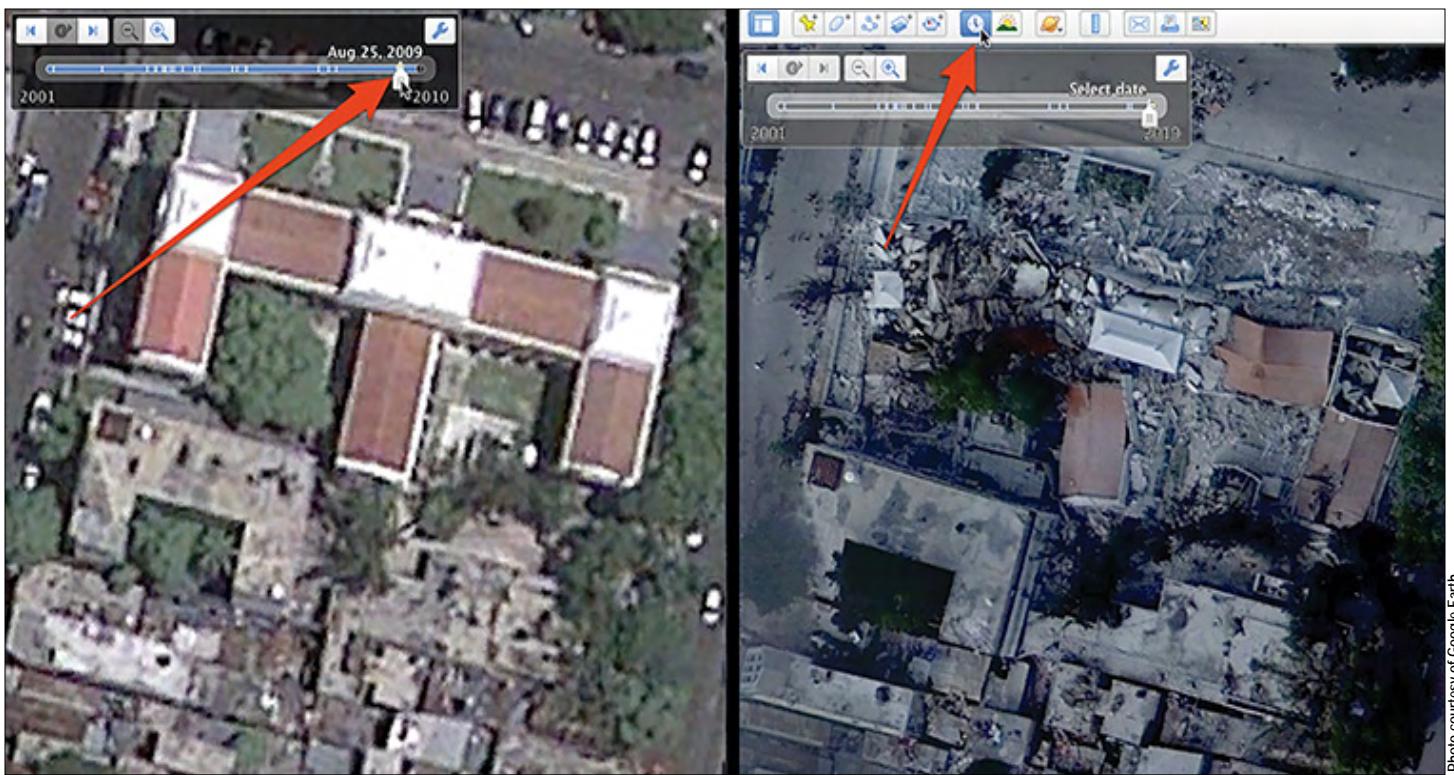


Photo courtesy of Google Earth

"Before and after" imagery depicting earthquake damage to the Haiti National Palace. The "before" image is from August 25, 2009, while the "after" image was taken on January 22, 2010. Change detection through "historic imagery" is one feature of Google Earth.¹

create the SIGACTs for their areas, and then through the liaison officers, pass the information to the Corps G-2 to consolidate the information. Similarly, the brigades can send their operations and friendly information to the Corps G-3.

The SFAB GEOINT advisor recommended that Google Earth become the main tool for the Corps ANA's common operational picture. The ANA should also distribute Google Earth to the brigades and kandaks. The program will allow the ANA to display enemy and friendly disposition, giving commanders a better understanding of their areas. Google Earth is much more precise because it can deliver ten-digit grids rather than the typical six collected from the wall map. This simple-to-use program provides data that is easy to share among multiple echelons and will modernize the ANA's common operational picture by upgrading from the use of analog mapping. It will help them to visualize intelligence reports, see patterns and trends of enemy operations, and conduct predictive analysis.

Unclassified Map Dataset

While going through transition training to get settled in Afghanistan, 1st SFAB G-2 topographic advisors learned of an unclassified hard drive, which contains an imagery dataset from the National Geospatial-Intelligence Agency. The hard drive contains map data—Buckeye imagery, orthoimagery, and a few pieces of vector data—in a 1.5 terabyte external hard drive. It runs an internal virtual machine on

the computer that allows all the data to be visible. It does not need an internet connection to work, and it is small, light, compact, and portable. The user can capture images to create products in support of mission requirements, pull the images into PowerPoint, and then easily modify them for mission-specific needs. The hard drive can create a KML² that Google Earth uses, which will give users the flexibility of viewing multiple layers. The hard drive is usable in a stand-alone version of Google Earth and can support operations with no connectivity. The hard drive also creates web services that can be pulled into programs like FalconView, ArcGIS, and QGIS, and can display all visible map and imagery layers.

We were excited to show how this relatively new tool worked because it contained unclassified imagery of Afghanistan that we could share with our ANA partners. The hard drive class was popular among the ANA G-2 section, and the topographic, targeting, plans, and analysis sections could use what they learned to create products that supported their mission requirements with the latest imagery. However, the advisors had only one hard drive to give to the ANA, so the SFAB advisors requested more drives through the National Geospatial-Intelligence Agency for further distribution. The primary SFAB G-2 GEOINT advisor created a PowerPoint presentation to support the hard drive training and had it translated into Dari for the ANA to use in future train-the-trainer situations.

This drive is versatile for multiple applications, but the data size of 1.5 terabytes is difficult to store on most computers. This means the user will need either an external hard drive or a connection to a server that can support the large data size. The ability to get more drives is a supply issue that the ANA is working to resolve. Other sections, such as the G-3 and the G-5, could use the drive when they have a requirement to create or display any type of visualization product.

Afghan National Army Data Management for Intelligence Reports

Currently the ANA maintains no recorded history of enemy SIGACTs, other than dated Microsoft Word documents that discuss information gathered from intelligence reports. No type of intelligence data management is in place at the Corps level. The Afghan National Directorate of Security emails intelligence reports in a Word document that contains reports from the previous day. Each morning, a few of the reports are chosen at random and briefed to the Corps Commander.

Now with the use of Google Earth in the ANA joint operations center, the Afghan Corps Commander needs a data management system to help maintain intelligence reports that can filter, sort, and ultimately help visualize enemy and friendly activity on the battlefield. Currently, with written reports in a Word document, there is no way to sort the reports by time, date, type of incident, province, district, or reporter name. Word documents do not have anything other than the rudimentary search capability of the “CTRL+F” (find) function, which means users must know exactly what they are looking for, and on which date something occurred, for the documents to be helpful. It is likely that the National Directorate of Security level may be facing the same problems with data management and battlefield visualization; however, the issue of data management starts at the top of an organization and the Directorate is best suited to drive this change.

If intelligence reports were compiled and maintained in a Microsoft Excel spreadsheet, they could be sorted and filtered, and a user could modify the document to better understand SIGACTs by type or dates. At a minimum, the Excel spreadsheet would need to have the following details: report ID, date, time, activity, enemy type, MGRS, province,

district, corps, brigade, kandak, today, and description of activity. Maintaining the data in an Excel format could help analysts to see enemy patterns, understand trends, use historical information for predictive analysis, and plan for future missions.



An Afghan National Army (ANA) officer teaches Soldiers of the ANA 203rd Corps about filling electronic warfare equipment under supervision of United States Army SSG Justin Hood, electronic warfare specialist for the Military Advisor Team of Task Force Southeast, during electronic warfare training July 6, 2017.

Requests for Information

Processing requests for information is time-consuming. These requests go through a series of checks before they reach the ANA G-2 topographic section. For example, when a person at an infantry kandak wants a map, the request must first go through their chain of command, up to the Corps level. Then it is assigned to the ANA G-2, and the G-2 tasks the topographic section. All personnel along the way must approve and sign the routing sheet before the next section receives the request for information. If a request is time-sensitive, or is submitted before a mission, this complicated process could hinder the troops on the ground.

The GEOINT advisor believes that the ANA soldier, with his first line supervisor, should be able to submit a request for information directly to the topographic section. This would also help the topographic section understand the required output or the effect the requester is trying to achieve.

Computer Hardware and Printers

The topographic section had a couple of Dell laptop computers, varying in age and software capabilities. The section also had four Hewlett-Packard (HP) plotters for printing large maps. Two of the four plotters were functional. One inoperable plotter had no ink and could not continue through the initialization process to show its status. The second

inoperable plotter had a problem with its printhead, requiring the section to order a new printhead (a slow process that came with its own issues). The third plotter worked, but the operating language was Chinese; fortunately, this was a simple fix, which involved reinstalling drivers on the computer and changing the operating language to English.

Supply Requests

Obtaining supplies, such as printer ink and external hard drives, was a cumbersome process. Supply requests became an issue for the ANA G-2 section when advisors and the ANA tried to order supplies for the HP plotters and external hard drives to support data sharing. Once advisors identified the need for ink and printheads, these expendable items should have been easy to order because they wear out regularly or they dry out through lack of use. When the ANA submitted the request, they found that not only did it have to go through the ANA G-2 chain of command, but it also had to go to the G-6 and the Ministry of Defense for approval. By the time we left, they were still waiting for the parts to arrive.

Similarly, advisors tried to help the ANA topographic section order a couple of external hard drives to support the sharing of data among several sections. This was more challenging than ordering printer supplies because the external hard drives were more expensive. The topographic section created the request form. The form went through the same approval process as the print supplies and again, by the time we left, the parts had not arrived.

The process is inefficient and needs to be streamlined. Once the staff primary approves a request, the G-4 should be able to action the request and order the needed parts, rather than having to route the request through several different sections.

Mission Priority—Mission Command or Advising?

The 1st SFAB's mission to advise host nation militaries is one of the U.S. Army's priorities. The SFAB is set up as a minimally manned brigade combat team to support small teams. When working with the ANA, we sometimes

wondered, "What is the priority—mission command or advising?"

Although the SFAB's priority should be advising, the advisors have the ability to flex and help the mission command team that is in place. The SFAB team can help fill requests for information and increase mission command capacity during crisis or changeover of personnel. Additionally, since SFAB personnel have potentially already been in this position, they could give advice or standard operating procedures to the junior person in the mission command position. With this structure, the SFAB could focus fully on the train, advise, liaison, and support mission with the Afghans. Eventually, the SFAB G-2 GEOINT advisors could see the SFAB team and ANA G-2 topographic sections working hand in hand on mission requirements. A commander may have to assume risk because advisors focus primarily on their advising responsibilities and may not be able to meet unexpected mission command requirements.

Conclusion

Before the SFAB G-2 GEOINT section arrived in Afghanistan to train, advise, and assist, the topographic section would typically respond to a request for information by pulling a standard pre-made map from a warehouse and taping it together as necessary, rather than actually creating a product within the section. After working with the GEOINT team, the topographic section made significant improvements to this and other processes. As a result, they and other sections were able to more effectively support requests for information and provide better products. 

Endnotes

1. Danny Sullivan, "Satellite Images Of Haiti Earthquake From Google & Bing Maps," *Search Engine Land*, January 22, 2010, <https://searchengineland.com/satellite-images-of-haiti-earthquake-from-google-bing-maps-34270>.
2. KML or Keyhole Markup Language is a file format used to display geographic data in an Earth browser such as Google Earth. You can create KML files to pinpoint locations, add image overlays, and expose rich data in new ways. *KML* is an international standard maintained by the Open Geospatial Consortium, Inc. (OGC). "Keyhole Markup Language," Google Developers, <https://developers.google.com/kml/>.

CW3 Jason Schelte is a 125D (Geospatial Engineering Technician) and has been in the Army for 19 years. He serves as the geospatial intelligence (GEOINT) officer in charge for the 1st Security Force Assistance Brigade. He deployed to Advising Platform Lightning, Afghanistan, in Task Force Southeast (TF-SE). He was the TF-SE GEOINT officer in charge and an advisor. He advised the 203rd Corps G-2 topographic section and other sections in the Afghan National Army G-2. He also advised the military intelligence kandak, the military intelligence battalion equivalent.



During the Civil War (1861-1865), the Union Army used both free and tethered balloons to watch over enemy dispositions in the early stages of the conflict.

The S303 Enemy Observation Report

by Chief Warrant Officer 2 Clyde A. Hunter and Chief Warrant Officer 2 Aaron A. Johnson

Introduction

In July 2018, the 25th Infantry Division (25th ID) executed Exercise Lightning Forge 18-03 (LF 18-03). The event was a brigade-level decisive action training exercise to prepare the unit for combat, to exercise mission command, and to evaluate operational readiness prior to a Joint Readiness Training Center rotation. During the exercise, the intelligence warfighting function within the 2nd Infantry Brigade Combat Team (2IBCT) and the 25th ID simulated operations in a degraded, intermittent, and limited communication environment while maintaining mission command and intelligence sharing between echelons.

The exercise simulated two aspects of human intelligence (HUMINT) operations:

- ◆ **Interrogation of enemy prisoners of war.** The prisoner role players were nested with opposing force elements and captured by battalions on the battlefield, forcing the brigade combat team (BCT) to exercise detainee operations.

- ◆ **The incorporation of adjacent and higher unit HUMINT reporting.** The division G-2X disseminated reports obtained from other subordinate BCTs that pertained to the 2IBCT's area of operation to stimulate reactions against pre-established master scenario events list activities.

The Current Human Intelligence Reporting System

The Army HUMINT enterprise currently reports intelligence using the intelligence information report (IIR) and its associated Defense Intelligence Agency (DIA)-mandated architecture. The report is an unstructured format that does not feed Army mission command systems and resides in DIA's databases. This HUMINT reporting architecture requires analysts to generate entities in the database manually, hindering timely situational awareness in a decisive action environment.

Other single-source intelligence disciplines, such as signals intelligence and geospatial intelligence, maintain systems



Photo by U.S. Army 1LT Ryan DeBooy

U.S. Army Soldiers assigned to 1st Battalion, 27th Infantry Regiment "Wolfhounds," 2nd Infantry Brigade Combat Team, 25th Infantry Division, provide fire suppression after the breach at a local support-by-fire position during a combined arms live-fire exercise at Schofield Barracks, Hawaii, August 3, 2018.

that use United States message text format (USMTF) reports and are interoperable with Distributed Common Ground System-Army (DCGS-A) and mission command systems. This allows these intelligence disciplines to immediately action and cross-queue intelligence information, using automated systems and tools within DCGS-A. HUMINT has never had the capability to rapidly send information to mission command systems, such as the Advanced Field Artillery Tactical Data System and Command Post of the Future, without manual entity generation. For this reason, 2IBCT S-2X and 25th ID G-2X used the S303 Enemy Observation Report (EOBSREP)¹ for HUMINT dissemination during LF 18-03 to address these deficiencies.

S303 Enemy Observation Report—A Different Form of Intelligence Reporting

For the first time, the 25th ID HUMINT enterprise experimented with a different form of intelligence reporting in place of the IIR. The division G-2X and BCT S-2X replaced the IIR with a USMTF report—the S303 EOBSREP—to disseminate HUMINT information. The 25th ID HUMINT enterprise had determined that the S303 EOBSREP better met the needs of the division's intelligence warfighting function while operating at the speed of the decisive action environment. None of the current capabilities within the DCGS-A enterprise allow for the rapid, organized, object-based production of an unstructured HUMINT IIR. During LF 18-03, the S303 report provided an innovative tactical solution for HUMINT dissemination in a decisive action training environment never before attempted.

Object-Based Production

According to DIA, “Object-based production [OBP] is a concept being implemented as a whole-of-community initiative that fundamentally changes the way the [intelligence community] IC organizes information and intelligence. Reduced to its simplest terms, OBP creates a conceptual “object” for people, places, and things and then uses that object as a “bucket” to store all information and intelligence produced about those people, places, and things.”²

To create the report, the 2IBCT S-2X, the operational management team, and the HUMINT collection teams used the Common Message Processor, a message creation tool found within the baseline version of the Portable Multi-Function Workstation (P-MFWS). The Counterintelligence and HUMINT Automated Reporting and Collection System, the Army's HUMINT program of record for HUMINT information, does not currently have the Common Message Processor on the image baseline. To bridge this gap, the 25th ID command, control, communications, computers, and in-

telligence (C4I) technician, in collaboration with the 25th ID G-2X HUMINT analysis cell officer in charge, developed a Java application called Sync, Modify, Transfer (SMT), which is capable of simultaneously generating and disseminating an S303 message and an IIR, allowing for the use of both reports. The Java application enables 25th ID HUMINT Soldiers and managers to disseminate S303 reports quickly to the unit's Tactical Entity Database.

Using the S303 Report for LF 18-03

During LF 18-03, the HUMINT collection teams reported all information using the S303 report to the operational management team. Once the team received the S303 report and reviewed it, the team populated the brigade's Tactical Entity Database with the S303 message, generated a HUMINT source entity,³ and associated the S303-generated entities with the source. This allowed the brigade intelligence support element fusion cell to visualize all HUMINT reporting on their Tactical Entity Database and on two-dimensional maps in near real time simultaneously with intelligence information populated from other intelligence disciplines. The HUMINT collection teams and operational management team used the Common Message Processor on a P-MFWS. The 25th ID HUMINT analysis cell injected S303 reports from adjacent and higher using the SMT software application. The 2IBCT S-2X and the 25th ID G-2X used the upper-tactical internet and lower-tactical internet as a means to transport the S303 report to each echelon.

During LF 18-03, the division G-2X simultaneously tested and validated SMT by creating and disseminating S303 EOBSREP messages directly to the 2IBCT S-2X and division G-2 Intelligence Fusion Server (IFS). The intent of testing both routes of creating S303 EOBSREP messages was to identify which method better enabled HUMINT collectors to rapidly learn and employ the message creation software in a decisive action training environment using upper-tactical internet and lower-tactical internet primary, alternate, contingency, and emergency (PACE) plans. In the end, the Common Message Processor software seemed to best fit the tactical needs of the HUMINT collection teams and operational management team, while the SMT better suited the division-level management needs for rapid dissemination across the battlefield.

The S303 report format allowed all echelons to have direct input into their respective IFS and Tactical Entity Database. The division G-2X used this validating event to better understand how publication authority would work if the S303 report were used in an actual decisive action fight. To achieve this, the division G-2X coordinated with the 25th ID C4I technician and the lead technology integrator for the U.S. Army

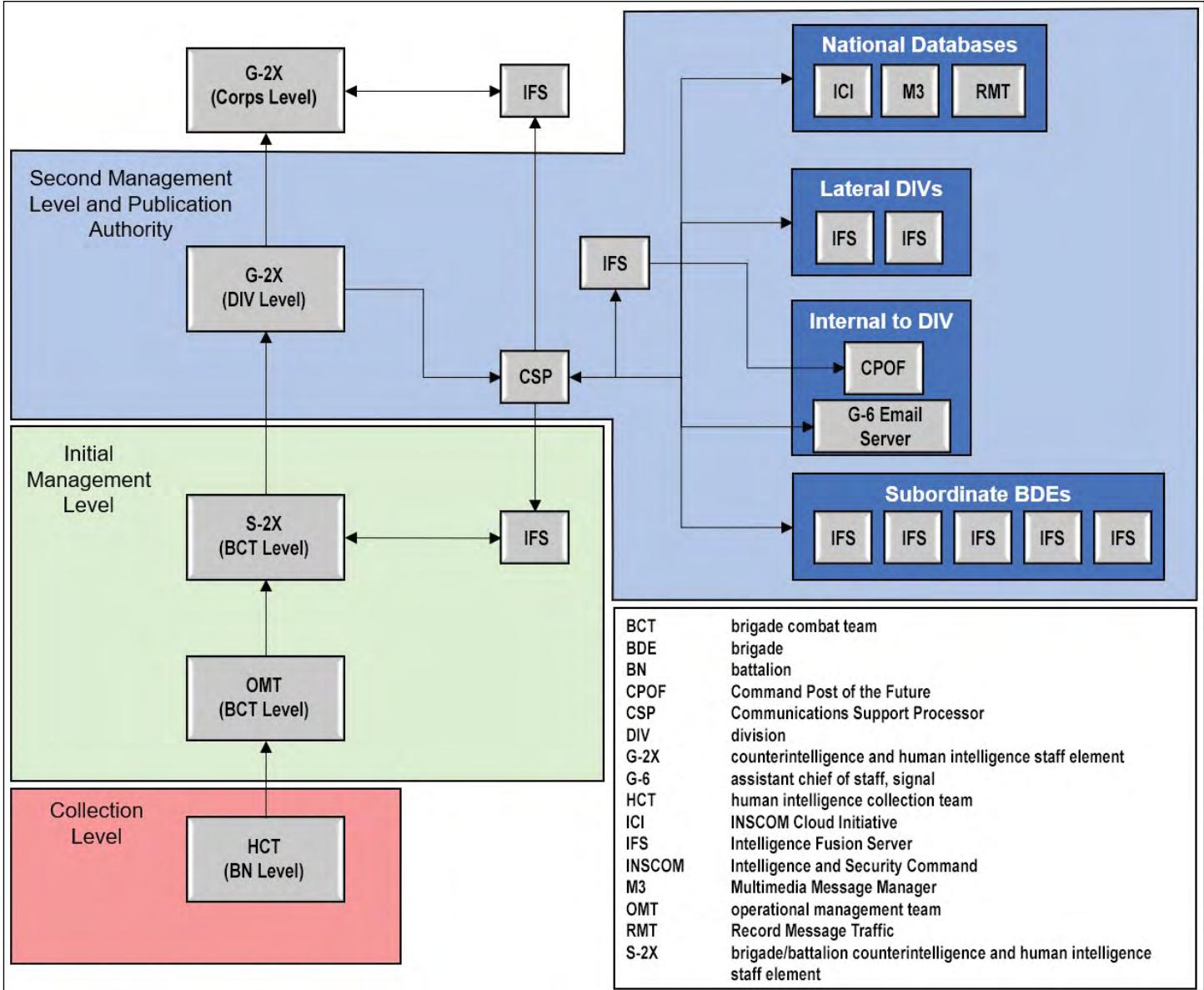


Figure 1. HUMINT S303 Report Flow

Intelligence and Security Command (INSCOM) to employ a “one-button push solution” to disseminate EOBSREPs at the division G-2X level. They considered two key factors as the intelligence architecture was built to support the EOBSREP dissemination. The first was that the reports must be discoverable by the greater intelligence community on the SECRET Internet Protocol Router (SIPR) and the Joint Worldwide Intelligence Communications System (JWICS). The second was that attachments must be transmitted with reports if reporting was related to captured enemy media or documents. Figure 1 shows the report flow, from the collection level to the publication authority.

Of note, all outlined solutions use current programs of record capabilities to facilitate EOBSREP dissemination. The 25th ID G-2X can now press one button to disseminate the EOBSREP to—

- ◆ All subordinate BCT IFSs.
- ◆ Division IFS.
- ◆ I Corps’ IFS.
- ◆ Multimedia Message Manager on SIPR and JWICS.
- ◆ Record Message Traffic on JWICS.
- ◆ INSCOM Cloud Initiative (ICI).
- ◆ 25th ID Tactical Exchange Server for a mass email to key leadership.

To enable attachments to the EOBSREP, the 25th ID G-2X created an account to upload to the 25th ID and 500th Military Intelligence Brigade-Theater (MIB-T) DCGS Integration Backbones (DIBs). Once these accounts are created, one can simply upload any type of file related to pocket litter, for example, or any other report attachment directly to the DCGS-A DIB. Intelligence community members will find an

attachment link in the EOBSREP that points them to the DIB website where they may download the associated attachment. When operating in a degraded, intermittent, and limited communication environment, the SIPR intranet established within the tactical operations center allowed the division to upload attachments locally to the 25th ID DIB. Once the upper-tactical internet was established, the 25th ID DIB federated with the 500th MIB-T DIB, ensuring that the information was readily available for all outside consumers.

The division G-2X also identified several key uses of the P-MFWS software to manage and distribute HUMINT information rapidly. Since the EOBSREP automatically extracted entities into the Tactical Entity Database, once they entered that database, division G-2X managers were able to set up filters in the Journal Message Entry viewer to filter all HUMINT reports that the IFS received. This allowed a manager to conduct a quick visualization of only HUMINT reporting to identify trends in reporting and facilitate collection management needs for the development of priority intelligence requirements. The division G-2X manager was also able to set up alerts to notify the managers when new HUMINT EOBSREPs entered the IFS. As these messages enter the IFS, HUMINT managers across echelons can automatically send the generated enemy entities directly to mission command

systems, such as the Advanced Field Artillery Tactical Data System and Command Post of the Future, for action by maneuver and fires elements when warranted.

Many believe that HUMINT has no part in the fires process or integration with the Advanced Field Artillery Tactical Data System because of information validation concerns; however, after using the S303 report during LF 18-03, 25th ID realized a significant potential to increase the overall effectiveness of HUMINT reporting. According to ATP 3-60, *Targeting*, “Target selection standards are criteria applied to enemy activity (acquisitions and battlefield information) and used in deciding whether the activity is a target. Target selection standards put nominations into two categories: targets and suspected targets. Targets meet accuracy and timeliness requirements for engagement. Suspected targets must be confirmed before any engagement.”⁴

During exercise LF 18-03, 2IBCT successfully identified how to use a HUMINT S303 report to relay HUMINT information

to the brigade fires section through the DCGS-A infrastructure. The targeting process showed HUMINT S303-derived targets as suspected targets until a confirmation of the target location error and dwell time could be established.⁵ Field artillery intelligence officers at the division and corps level or the BCT targeting officer at the BCT level must verify accurate information from a reliable source before declaring it a target if the elapsed time exceeds dwell time. The dwell time of the target determines whether to engage based on the likelihood of the target moving.⁶

Over the course of the exercise, the 2IBCT S-2X and operational management team assisted in the execution of approximately four lethal fire missions as a direct result of HUMINT S303s. Figure 2 shows the data that typically feeds into the fire mission execution function. During each fire mission, the 2IBCT S-2X was able to send the entities derived from the HUMINT S303 report directly to the

fires section. Immediately upon receipt, the fires section began an assessment of the suspected target. To confirm targets derived from HUMINT reporting, the fires section cross-queued geospatial intelligence and full motion video platforms, almost instantaneous to the receipt of the HUMINT S303 report to verify the targets at the reported locations. Once the 2IBCT S-2X had received the report, the process of disseminating the HUMINT S303 information to execution of fire mission was 4 minutes. The overall process from point of collection to execution of fire mission was 15 minutes.

Lastly, the division G-2X established a data pipe directly to the ICI for EOBSREP analytic efforts. The ICI allowed the EOBSREP to pass through text analytic software and be correlated against multiple other intelligence reports. This also allowed the greater intelligence community to visualize in real time the 25th ID HUMINT common operational picture and common intelligence picture. This validation proved that personnel across the intelligence community would have access to the reporting that the HUMINT S303 report provided, in raw report format and in extracted entity format. After pushing the HUMINT S303 entities to the ICI, HUMINT managers within the division G-2X could use the Unified Video Dissemination System overlay on the ICI to watch real-time geospatial intelligence full motion video feeds of the constructed and virtual environment within the



Figure 2. Fire Mission Execution⁷

Lower-Tactical Internet Plan					
	P	A	C	E1	E2
	JCR	Point 2 Point FM	ANW2	TACSAT - Data	TACSAT - Voice
P	SMDL S303	PDA-184 S303 file transmit	CMP on P-MFWS	PDA-184 S303 file transmit	Voice S303
A	Free message S303	PDA-184 S303 chat transmit	CMP/SMT on CHARCS	PDA-184 S303 chat transmit	
C	Chat S303	Voice S303 relay	CHARCS free text message	Voice S303 relay	
E			Sharedrive		
Upper-Tactical Internet Plan					
	P	A	C	E	
	JNN	TDN-1	TDN-3	TDN-2	
P	Direct CSP/IFS SMTP MSG	CHARCS GENADMIN	Direct CSP SMTP MSG	Direct CSP SMTP MSG	
A	Exchange email	Direct IFS SMTP MSG	Sharepoint	Sharepoint	
C	Jabber/Transverse file transfer	Sharepoint	Sharedrive	Sharedrive	
E	Sharedrive	Sharedrive			

ANW2	adaptive networking wideband waveform	JNN	joint network node
CHARCS	Counterintelligence and Human Intelligence Automated Reporting and Collection System	MSG	message
CMP	Common Message Processor	P-MFWS	Portable Multi-Function Workstation
CSP	Communications Support Processor	SMDL	semantic model definition language
FM	frequency modulation	SMT	Sync, Modify, Transfer
GENADMIN	general administration (message)	SMTP	Simple Mail Transfer Protocol
IFS	Intelligence Fusion Server	TACSAT	tactical satellite
JCR	Joint Capabilities Release	TDN	Tactical Data Network

Figure 3. Lower- and Upper-Tactical Internet HUMINT PACE Plan

scenario. This allowed the division G-2X to quickly attempt to validate HUMINT reporting as it came in against what was being pushed via the ICI.

The Importance of a Well-Developed PACE Plan

To ensure successful dissemination of the S303, 25th ID needed a well-developed PACE plan. During LF 18-03, the G-2X and S-2X employed a diversified lower-tactical internet and upper-tactical internet PACE plan to disseminate the S303 EOBSREP. Figure 3 provides a snapshot of the designed and implemented PACE plan used during LF 18-03.

The PACE plan ensured the G-2X and S-2X remained synchronized on all S303 messages, but more importantly, it allowed the analysis and control element and the brigade intelligence support element to communicate while in degraded, intermittent, and limited communication environments.

During LF 18-03, 25th ID successfully used the S303 report as the HUMINT solution to assist in providing object-based

production to the 25th ID's all-source analysts operating in a decisive action training environment. This, combined with the capability to integrate other intelligence disciplines' object-based production, allowed 2IBCT to initiate fire missions based on initial HUMINT reporting. The reporting had to be vetted, cross-queued, and verified before it could be actioned; however, because of the 2IBCT HUMINT's ability to execute object-based production for its analysts, the HUMINT section was capable of increasing overall HUMINT effectiveness in a decisive action environment.

The use of the P-MFWS for HUMINT operations greatly increased throughout the duration of LF 18-03. The G-2X and S-2X identified the following key capabilities that DCGS-A can offer HUMINT operations if implemented in conjunction with a well-thought-out PACE plan and use of the S303 report in a decisive action environment:

- ◆ HUMINT teams employing a DCGS-A Multi-Function Workstation are able to visualize the current common

operational picture and common intelligence picture in real time.

- ◆ Using historical data from the Tactical Entity Database, real-time source-directed requirement generation supports collection operations.
- ◆ Object-based production facilitates standardized reporting and visualization of intelligence across the brigade intelligence warfighting function and mission command systems.
- ◆ P-MFWS are able to visualize HUMINT source entities, which facilitates management and intuitive analyst actions in support of HUMINT operations.
- ◆ HUMINT teams can see real-time data input from the Intelligence and Electronic Warfare Tactical Proficiency Trainer and other intelligence disciplines, which facilitates the real-time generation of source-directed requirements and priority intelligence requirements.
- ◆ Management sections can execute past mission analysis against enemy prisoners of war levied against additional intelligence disciplines in real time.

Subsequent Training Exercise

In the first quarter of fiscal year 2019, 2IBCT deployed to the Joint Readiness Training Center. During the rotation, they once again employed the S303 as the primary tool for reporting intelligence information at the tactical level. They benefited from the use of structured data tools at the training center. For example, the teams were able to report information in less than 10 minutes because the S303 could be generated quickly. In addition, the use of the P-MFWS to transmit structured data enabled small file sizes. The operational management team was also able to generate source-directed requirements easily because they had the brigade's visualization of information via the Tactical Entity Database.

Conclusion

During LF 18-03, the 25th ID HUMINT enterprise successfully validated the use of the S303 EOBSREP as a mecha-

nism to disseminate HUMINT information and execute object-based production at the division and brigade echelons. For the past few years, the HUMINT community has failed to adapt to the DCGS-A environment. Use of the S303 report allowed 25th ID HUMINT to better integrate into the DCGS-A infrastructure and mission command system platforms, while simultaneously using the equipment the Army provides on the modified table of organization and equipment to execute data transmission in upper-tactical internet and lower-tactical internet beyond line of sight environments. 

Endnotes

1. The S303 Enemy Observation Report (EOBSREP) is an Army specific U.S. message text format report that can be generated within mission command systems. It is used to exchange essential elements of enemy activity. Forward observers, scouts, or other forward elements use this message to report to their higher headquarters. Department of the Army, Field Manual (FM) 3-52, *Army Airspace Command and Control in a Combat Zone* (Washington, DC: Government Publishing Office [GPO], 1 August 2002 [obsolete]), A-3.
2. Catherine Johnston, Elmo C. Wright, Jr., Jessica Bice, Jennifer Almendarez, and Linwood Creekmore, "Transforming Defense Analysis," *Joint Force Quarterly* 79, 4th Quarter 2015 (October 2015): 13, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_12-18_Johnston-et-al.pdf.
3. The term *HUMINT source entity* refers to an object entity within the Portable Multi-Function Workstation. The workstation is not designed for, nor should it ever be used for, source management operations. This entity's use is primarily to visualize intelligence reporting associated to the source entity for link diagram purposes.
4. Department of the Army, Army Techniques Publication (ATP) 3-60, *Targeting* (Washington, DC: U.S. GPO, 7 May 2015), 2-4.
5. Target characteristics consist of size, accuracy, and target location error requirements for each weapon systems.
6. Department of the Army, ATP 3-60, 2-8.
7. Department of the Army, FM 6-60, *Tactics, Techniques, and Procedures for the Multiple Launch Rocket System (MLRS) Operations* (Washington, DC: U.S. GPO, 23 April 1996 [obsolete]), 5-5.

CW2 Clyde Hunter is currently the G-2X Intelligence Contingency Funds Manager, U.S. Army Central, Shaw Air Force, SC. Previously he was the G-2X, Human Intelligence (HUMINT) Analysis Cell officer in charge (OIC) at 25th Infantry Division, Schofield Barracks, HI. At 525th Military Intelligence Brigade, Fort Bragg, NC, he served as a platoon leader and operational management team (OMT) OIC in the 519th Military Intelligence Battalion HUMINT and Counterintelligence Company. He has deployed in support of Operations Enduring Freedom and Iraqi Freedom. CW2 Hunter has an associate's degree in general studies from University of Phoenix and is working toward a bachelor of science in information technology from Western Governors University.

CW2 Aaron Johnson currently serves as Architecture Chief of the Unit Engagement Team at the U.S. Army Training and Doctrine Command Capability Manager-Foundation, Fort Huachuca, AZ. Previous assignments include G-2X HUMINT Analysis Cell OIC for 25th Infantry Division; OMT OIC for 2nd Infantry Brigade Combat Team, 25th Infantry Division, Schofield Barracks, HI; and OMT OIC for 2nd Armored Brigade Combat Team, 1st Cavalry Division, Fort Hood, TX. He deployed in support of Operations Iraqi Freedom and Enduring Freedom. CW2 Johnson earned his associate of applied science in intelligence operations from Cochise College and recently received the 2019 CW5 Rex Williams Award for excellence in military intelligence.

Military Intelligence Junior Officer Development Program at the Joint Multinational Readiness Center

by Colonel James L. Snyder, Captain Ryan M. Hardin, and Captain Kent D. Homrighausen

Introduction

The Joint Multinational Readiness Center (JMRC), located at Hohenfels, Germany, is the U.S. Army's Europe-based combat training center. Like all Army combat training centers, JMRC provides—

- ◆ rotational unit trends,
- ◆ observations and lessons learned back to the operational force through center of excellence engagements,
- ◆ professional forum participation,
- ◆ leader training programs, and
- ◆ input to a multitude of newsletters and Center for Army Lessons Learned publications.

One of the most challenging missions we have is to “get left” of the rotation and influence trend reversal by driving change in unit home station training or institutional professional military education.

The Tactical Experience Gap

For many years, a troubling trend existed across the military intelligence (MI) community—a failure of battalion and brigade S-2s to perform their critical roles adequately, resulting in several S-2s being removed from their jobs. In response to this trend, the Department of the Army G-2, the Commanding General of the U.S. Army Intelligence Center of Excellence, and intelligence community leaders revamped curricula at the Intelligence Center of Excellence. They also instituted the new brigade combat team S-2 course at the Command and General Staff College and declared calendar year 2016 the “Year of the [brigade] BDE S-2” as an MI Corps focus. All these efforts have produced tangible effects and have improved the tactical proficiency of our junior field and company grade officers.

Having served in multiple nondivisional assignments, I [COL Snyder] observed a widening gap between our



Photo by U.S. Army SSG David Overson

U.S. Army Soldiers with 1st Battalion, 4th Infantry Regiment who are assigned to the Joint Multinational Readiness Center's Hohenfels Training Area, Hohenfels, Germany, practice their role in a combined arms rehearsal, prior to maneuvering into the “Box” during Allied Spirit VIII, January 25, 2018.

JMRC is a professional, adaptable, and innovative team that builds and sustains readiness of assigned European-based forces and rotational forces through premier training in order to deter adversaries and win in a complex operating environment.

junior captains who lacked the tactical experience of their peers serving in U.S. Army Forces Command (FORSCOM) brigade combat team assignments, either as branch detail or as basic MI Branch officers. While non-FORSCOM assignments are tremendously broadening to new MI lieutenants, they generally do not provide opportunities to experience the tactical operations process executed at a brigade or a battalion. This creates junior leaders with a tactical experience gap from not providing maneuver commanders with timely and relevant assessments and recommendations to win in large-scale combat operations against a peer threat.

Military Intelligence Junior Officer Development Program

To bridge this gap and effect trend reversal at the foundational level, the JMRC has implemented an MI Junior Officer Development Program to assist young officers who

personnel. Guest OCTs benefit personally and professionally while serving key roles in developing rotational training units. Building upon this model, the MI Junior Officer Development Program offers company grade MI officers the opportunity to broaden their intelligence expertise by observing tactical units in action. This program is tailored especially to those serving in units that focus on providing operational and strategic intelligence support to the European theater. During major training rotations, MI officers are exposed to—

- ◆ maneuver, fires, aviation, and engineer battalion S-2s,
- ◆ brigade intelligence cells and enablers,
- ◆ opposing forces (OPFOR) S-2, and
- ◆ division-level intelligence, surveillance, and reconnaissance asset managers.

Intelligence Ride Along – 2LTs, 1LTs, Jr. CPTs

- No tactical intelligence experience required
- Observation only
- Ride along with the OTC Team
- Flexible schedule

Full Immersion Experience – Sr. 1LTs and CPTs

- Previous tactical intelligence experience required – OR former ride along participant
- Serve as a certified JMRC Guest OCT
- Must attend complete rotation

OPFOR Assistant S-2 – 2LTs and 1LTs

- No tactical intelligence required
- Serve as the 1st Battalion, 4th Infantry Regiment assistant S-2 for an exercise
- Unique opportunity from red perspective
- Can be tailored to fit officer availability

MI Junior Officer Development Program

are not assigned to tactical formations. This crucible experience and focused mentorship with senior MI captains, majors, and lieutenant colonels serves to round out young officers' professional development and provide them with a resource for future growth. While one brief visit to a combat training center will not fully prepare a new battalion S-2 for the demands of combat, it will empower the officers to identify the gaps in their knowledge base that they need to close. This opportunity, early in their careers, will maximize their potential for career success, while capitalizing on their already diverse experiences to enhance their peers and the force.

JMRC regularly hosts premier training exercises for European-based and regionally aligned U.S. units and our multinational partners. It also frequently invites guest observer-coach-trainers (OCTs) to augment permanent party

The program offers three options:

Intelligence Ride Along. The intelligence ride along is for second lieutenants, first lieutenants, and junior captains. This program requires no prerequisite tactical intelligence experience, is observation-based, and is highly tailorable. Participants spend anywhere from 3 days to 2 weeks shadowing professional OCTs as they mentor rotational training units' battalion and brigade intelligence teams. The ride along program also includes a chance to "peer behind the enemy's curtain" and observe the OPFOR S-2 section as they prepare for operations against friendly forces.

Full Immersion Experience—Guest Observer-Coach-Trainer. The full immersion experience is specifically for senior first lieutenants and captains with previous tactical intelligence experience. Former participants in the ride along program are highly encouraged to attend. Participants

in the full immersion experience begin with a 3-day guest OCT Academy taught by JMRC's professional cadre. After certifying as a JMRC guest OCT, participants are assigned to a battalion OCT team to fill a critical intelligence OCT billet for an entire rotation.

OPFOR Assistant S-2. JMRC's OPFOR "warriors" from the 1st Battalion, 4th Infantry Regiment replicate a highly proficient peer enemy. The third developmental opportunity for junior MI officers is to serve as an OPFOR assistant S-2 for a rotation. Requiring little to no previous tactical intelligence experience, MI lieutenants benefit through on-the-job training by providing intelligence support from the enemy perspective. Participants serve within a seasoned S-2 section under the direction of a veteran MI captain for an exercise or a customized timeframe to fit the officer's availability.

Key Takeaways

The following key takeaways highlight the benefits of the program:

- ◆ Participants gain access to current and emerging intelligence trends and initiatives while learning specific intelligence processes such as intelligence preparation of the battlefield (IPB), staff planning, and current operations—all crucial aspects of being an officer.
- ◆ MI officers have opportunities to learn from OCTs of other warfighting functions, which not only broadens their leadership experience but also expands their network and provides a contextual background on specific intricacies of the various warfighting functions. These opportunities can inform intelligence officers as they support maneuver commanders throughout their careers. MI officers will take lessons learned and knowledge gained back to their home units and implement the experience into their training plans, operations, and professional development opportunities.
- ◆ Officers build a network of relationships across Europe, the MI Corps, and the U.S. Army, which will assist in coordination, information sharing, and support of future intelligence efforts in Europe and beyond.

Feedback from Participants in the Program

Since the program's inception in September 2018, JMRC has hosted five MI lieutenants for the intelligence ride along and one captain for the full immersion guest OCT experience. Some of their after action report comments highlight the program's benefits:

First lieutenant, 522nd MI Battalion, 207th Military Brigade: "The most beneficial aspect of this opportunity for me was the ability to see the S-2s/[MI company] MICO from varying warfighting functions execute IPB. The schoolhouse gives you the opportunity to plan and run through the steps of IPB, but this experience allowed me to see the execution of that plan from multiple perspectives and enabled me to learn from the experiences of varying intelligence professionals...The OPFOR S-2 had a wealth of knowledge and the time to explain the reasons behind his actions."

First lieutenant, 650th Military Group: "I found the initial planning process, the [military decision-making process] MDMP and IPB portions, to be the most beneficial for me. The fundamental refresher of these essential decision-making processes has not only shown me what I need to brush up on, before attending the [MI Captains Career Course] MICCC, but also the overwhelming importance of analytical planning prior to execution in the field."

First lieutenant, 24th MI Battalion, 66th Military Brigade: "We had the opportunity to have an impromptu [leadership professional development] LPD [session] with the JMRC [electronic warfare officer] EWO on the implementation of [electronic warfare] EW assets and the future integration of EW with [signals intelligence] SIGINT within the MICO. That was an extremely valuable opportunity."

How to Participate

Junior MI officers may participate in any of the exercises hosted at the JMRC. These exercises provide broadening opportunities for MI officers by allowing them to take part in armored, mechanized, Stryker, and airborne/light rotations and to work with North Atlantic Treaty Organization allies and U.S. partners. Units are responsible for coordinating transportation to and from the training area in Hohenfels, Germany. JMRC provides life support for the duration of exercises, making this a very low cost opportunity for units to broaden their junior MI officers. Interested participants should consult with their chain of command for support and contact usarmy.jmrc.usareur.list.sr-intel@mail.mil for additional information about JMRC programs.



"To be successful at the next level, military intelligence [MI] leaders should have a variety of experiences at all echelons, from tactical to strategic. Participating in an immersion experience at a combat training center such as the Joint Multinational Training Center is an excellent way to broaden and deepen one's craft. Lieutenants and captains will take their lessons learned back to their home units, strengthening the MI community as a whole. This program pays dividends across the board."

— MI Company Senior Trainer, JMRC

COL James Snyder is the senior intelligence officer at the Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany. He is a proud graduate of The Pennsylvania State University, with a bachelor of science in aerospace engineering, and of Webster University, with a master of arts in security management. His prior assignments include battalion S-2, brigade S-2, Deputy Division Analysis and Control Element Chief, 66th Military Intelligence (MI) Brigade-Theater S-3 and deputy commanding officer, and Commander of 522nd MI Battalion (Equalizers!). He has deployed to Kuwait, Bosnia, Afghanistan, and Iraq.

CPT Ryan Hardin is the MI company senior trainer at the JMRC, Hohenfels, Germany. He has observed, coached, and trained three U.S. battalion S-2s and five MI company commanders. He commissioned as a branch detailed infantry officer in 2010 and subsequently served as a rifle platoon leader, battalion planner, and mobile gun system platoon leader. In 2012, he deployed to Afghanistan and served as the forward logistics element platoon leader. As a MI captain, his positions include infantry battalion S-2, headquarters company commander, and brigade engineer battalion S-2 observer-coach-trainer. CPT Hardin was recently selected to attend the National Intelligence University to pursue a master of science degree in strategic intelligence.

CPT Kent Homrighausen is the brigade engineer battalion intelligence trainer for the Raptor Team at the JMRC in Hohenfels, Germany. He commissioned as a branch detailed field artillery officer in 2010 with a bachelor's degree in justice systems from Truman State University and transitioned to MI in 2014. His prior assignments include fire direction officer, fire support officer, battalion S-2, battalion S-4, and counterintelligence/human intelligence detachment commander. He has two deployments to Afghanistan, the first in Nuristan Province and the second in Kunar Province.



What is Foundry

The Foundry Intelligence Training Program is a critical enabler to Army global readiness. It provides commanders the necessary resources (funding, facilities and subject matter experts) to prepare military intelligence Soldiers, Civilians, and units to conduct intelligence operations and activities at the tactical, operational, and strategic levels.

Foundry Training Types

Foundry enhances individual and collective intelligence training for the Active and Reserve Components through –

- Resident (TDY) or at a Foundry Site
- Live Environment Training
- Mobile Training Teams



Funding

Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, may allocate Foundry resources that support unit METL, Army Service component command's intelligence warfighter function training requirements and advanced intelligence training provided by the intelligence community.

Schedules

Foundry Courses can be scheduled through the Army Training Requirements and Resources System (ATRRS). ATRRS allows units to submit training requests online and view calendars of all available, requested, and scheduled intelligence training. ATRRS also displays training objectives, prerequisites, class size, and course administrative requirements. ATRRS URL: <https://www.atrrs.army.mil>.

Points of Contact

DA G-2 TRAINING POINT OF CONTACT

Foundry Program Manager: 703-695-1268

INSCOM FOUNDRY POINT OF CONTACT

Foundry Program Administrator: 703-706-1890

INSCOM ATRRS: 703-706-2227



Security Force Assistance Lessons Learned Support

by Mr. Chet Brown, Chief, Lessons Learned Branch

Introduction

"Help me, help you." This quote from the movie *Jerry Maguire* is less memorable than Cuba Gooding Jr.'s "Show me the money!"¹ Citing a line from a 23-year-old movie can't be a good way to begin a discussion about security force assistance lessons learned. "Help me, help you" does however succinctly describe one of the dependencies of the Army's lessons learned enterprise in adding value to current training and operations. We depend upon you to share your lessons with us so that we may help others be successful, or at least avoid identified pitfalls. Those who share their hard-earned lessons with us (the lessons learned enterprise) not only help themselves improve, but they also enable us to help others. Come to think of it, a slight edit of the money quote may describe another benefit of the lessons learned enterprise. While not able to show any money, lessons learned add value to individual and unit training and increase operational performance.

Helping military intelligence (MI) professionals in the 1st Security Force Assistance Brigade (SFAB) train for impending operations was the initial focus of the U.S. Army Intelligence Center of Excellence's Directorate of Training (DoT) and its subordinate Lessons Learned Branch. The mission variables of time and troops (personnel) available limited our initial effort. While a modest endeavor constrained by existing resources, DoT's support expanded in scope and collaboration with others also seeking to help each of the SFABs as they are established.

What Can We Do To Help?

Upon learning about the creation and impending deployment of the 1st SFAB, the DoT assessed what it could do to help the unit's MI personnel plan, prepare, and perform as intelligence advisors. The DoT Deputy Director identified the unit's compressed predeployment timeline and anticipated SFAB requirements the DoT could fulfill. Similar to

intelligence collection planning, the DoT identified existing information of immediate benefit to the SFAB's MI Soldiers and leaders. DoT leaders recognized that we had to start compiling information immediately because waiting for the SFAB to request assistance would not provide enough time to furnish the highest quality response. To estimate what the SFAB may need, we looked at what similar operations required to be successful.

What Are The Lessons Learned By Those Who Have Done This Before?

While the 1st SFAB may be the first of its current organization, it is not the first of its echelon to serve in a predominantly advisory role, particularly in the current operational areas of Iraq and Afghanistan. Lessons and best practices from advising and assisting operations during the last decade of operations are readily available to the force. Adding to the repository of lessons learned knowledge are the lessons and best practices from Army advising operations worldwide. What is now described as Phase 0 (Shape) and Phase 1 (Deter) Army operations, Soldiers have been doing as a matter of routine since well into the last century—advising and assisting our multinational partners. So much information is available on advising and assisting operations that our initial task changed from identifying "what is available" to "what is most useful" in assisting SFAB MI personnel prepare for operations. We were determined that any information or products we would provide to the SFAB would be accurate, concise, and easily understood. They would also not duplicate SFAB training, either planned or underway.

What Can We Do With What We Have On Hand?

The first product we sent was simply a two-page summary of key lessons and best practices information from similarly structured conventional force elements that had accomplished advise and assist missions during Operations Enduring Freedom, Resolute Support, and Freedom's

Sentinel. By presenting the lessons and best practices in the order of the operations cycle steps of plan, prepare, execute, and assess, we hoped to draw SFAB MI leaders' attention to the pertinent items in sequential order of importance. This initial attempt was to serve as a checklist of items for the SFAB to consider when planning training and predeployment activities. We shared the product, and strengthened a collaborative relationship, with the Center for Army Lessons Learned (CALL) and U.S. Army Training and Doctrine Command's Capability Manager Security Force Assistance Brigade (TCM SFAB). A quick search of the CALL website provided several advise and assist publications of immediate utility.

DoT leaders realized there was more we could accomplish and offer to the SFAB. Using immediately available resources, the DoT could provide the SFAB with a pocket-sized reference of MI roles, functions, and techniques. The DoT Deputy Director recommended finding a copy of the 1992 (now obsolete) FM 34-8, *Combat Commander's Handbook on Intelligence*, to use as a model in developing a reference guide for SFAB MI personnel. The task of building the reference guide fell to an MI captain who in turn was supported by the combined efforts of several DoT organizations. The collaboration resulted in producing an SFAB intelligence smart book in late 2017. Keeping in mind the environment in which the reference was going to be used, the DoT printed the smart book on weather- and tear-resistant paper bound by a single ring. These features enabled SFAB advisors to rearrange the contents of the book, tailoring it to their preference or removing selected pages to keep handy in a pocket. Initial feedback from SFAB personnel who used the reference was very positive.

As the 2nd SFAB was being formed, we sent the smart book to key MI leaders of the unit. Although the book was well received, 2nd SFAB personnel recommended a few revisions tailored to the unit's mission variables. The unit also asked if we could produce a foreign language version to help SFAB linguists become conversant in describing MI actions in the host nation's vernacular. The request was definitely a lesson recorded somewhere. We focused so intently on producing a useful reference in English that we overlooked the possibility of simultaneously developing a translated version. This is now a lesson learned.

Updating the smart book's content was fairly simple and accomplished using desktop publishing software. The updated version was provided to the 2nd SFAB printed on the special weather- and tear-resistant paper. Unfortunately, the special paper required frequent troubleshooting of printer malfunctions. The constant attention of the DoT's Training

Support Division ensured the handbook was printed and sent to support the SFAB Soldiers.

Who Else Can Help?

Translating the book into the requested language required casting a wider collaboration net. Attempts to obtain translation support from several recognized authoritative organizations were unsuccessful primarily because of the limited time available. We needed to provide the translated version to the unit as it began training. The DoT senior enlisted advisor suggested asking the Army's military occupational specialty 09L (Interpreter/Translator) community to help. The senior enlisted advisor put us in touch with the Commander, 52nd Translator and Interpreter Company (TICO), 3rd Battalion, 353rd Regiment, Security Cooperation/Security Force Assistance Operations Group, Joint Readiness Training Center, Fort Polk, LA. The 52nd TICO provided an accurate translation of the entire smart book well in advance of the requested suspense. Thanks to the efforts of the 52nd TICO and the DoT Training Support Division's printing crew, the translated versions were provided to the 2nd SFAB on the special paper stock.

The Way Forward

"A vision without resources is a hallucination" is attributed to American political commentator and author Thomas Friedman. While we were successful in meeting the immediate needs of the 1st and 2nd SFABs with existing resources, the effort did have an impact on the responsibilities and budgets of every organization that contributed to the effort. 1st SFAB returned from its initial deployment with a host of lessons, best practices, and recommendations for future versions of the intelligence smart book. The establishment of the Security Force Assistance Command and additional numbered SFABs increases the number of personnel and opportunities for more collaboration and requirements. The ad hoc efforts undertaken to ensure the immediate, and perhaps minimal level of, support to the first two SFABs is neither a desirable nor a sustainable model. The MI lessons learned effort is only a small part of the Army's lessons learned enterprise responding to the requirements of the Security Force Assistance Command and SFABs. As we continue to learn from the experiences of the SFAB personnel, we are coordinating with CALL to establish an enduring lessons learned exchange and production model. A major benefit of collaborating with CALL is to leverage their extensive network of subject matter experts and publishing resources.

Helping Us Help You

The 1st SFAB personnel have provided their lessons and best practices freely and frequently. The 1st SFAB's S-2 has

provided the Lessons Learned Branch at the U.S. Army Intelligence Center of Excellence with an extraordinary level of support, access, and information sharing. In collaboration with the TCM SFAB, we've been able to—

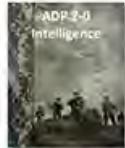
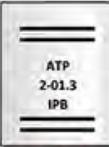
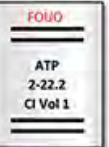
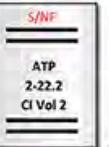
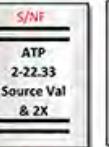
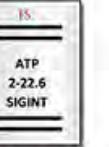
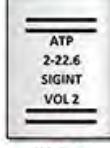
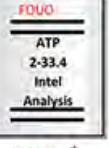
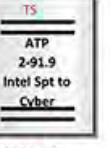
- ◆ Attend the unit's post-Joint Readiness Training Center/predeployment after action review.
- ◆ Have the S-2 brief key points from the after action review at an MI Lessons Learned Forum.
- ◆ Receive individual observations, lessons, and best practices during the unit's deployment.
- ◆ Meet with the unit's MI personnel upon their redeployment to the United States.

We've integrated key recommendations to the aforementioned smart book versions and established contact with the SFABs being organized now. The support of SFAB leaders, and all of those who contributed to their success, enabled us to provide assistance. While a number of personnel within the DoT surged to produce the intelligence smart books, I would be remiss if I did not acknowledge the support of the professionals within the 1st and 2nd SFAB S-2s, the 52nd TICO, the DoT Printing Services, and the TCM SFAB. 

Endnote

1. *Jerry Maguire*, directed by Cameron Crowe (1996; Culver City, CA: Columbia TriStar Home Video, 1997), VHS.

Are You Doctrinally Proficient?

	SEP 18 *(Change 1)		JUL 18		SEP 06																
	AUG 14*		MAR 19		DEC 15*		MAR 15		FEB 15		DEC 15		DEC 16		APR 15		SEP 16		NOV 13		DEC 15
	JUN 17		MAR 15		MAY 14		NOV 15		JUN 17 *		Final Approved Draft*		AUG 14*		JUN 15		MAY 15		AUG 17		
	DEC 13		JUN 18		OCT 16		APR 18														

Authenticated MI Doctrine can be found at:

- <https://armypubs.army.mil>, then – Publications – Doctrine and Training. Select the type of publication ADP, ATP, or FM.
- <https://ikn.army.smil.mil>, then – Resources – MI Active Doctrine. Window opens in the IKN-S Doctrine Website. Select MI Active Doctrine from the left menu.
- <https://www.ikn.army.mil>, then select the MI Doctrine icon.

For questions concerning Army intelligence doctrine, please contact the USAICoE Doctrine Division via email at:
usarmy.huachuca.icodedoctrine@mail.mil

* Key revision projects
Authenticated Draft

Doctrine Corner

Doctrine Updates



Editor's Note: The U.S. Army Combined Arms Center publishes a quarterly Doctrine Newsletter that highlights recent and upcoming changes to doctrine and provides information related to the use of doctrine. It is disseminated via email to the widest audience to maximize the understanding of doctrine. The following is an extract of information from the April 2019 newsletter.

Recently Published Army Doctrine

This article provides the operational and generating force with the most current information on recent publications. Each discussion provides a short synopsis of new Army doctrine publications (ADPs), field manuals (FMs), Army techniques publications (ATPs), and multi-Service publications. These synopses provide readers with new doctrinal changes. The Combined Arms Doctrine Directorate published each publication through the Army Publishing Directorate (APD) since October 2018. Readers can access these and other Army publications at the APD website located at <http://armypubs.army.mil/>.

ARMY DOCTRINE PUBLICATIONS

ADP 3-28, Defense Support of Civil Authorities. ADP 3-28 explains how the Army conducts defense support of civil authorities (DSCA) missions and National Guard civil support missions as part of unified land operations. It helps Army leaders understand how operations in the homeland differ from operations by forces deployed forward in other theaters. It illustrates how domestic operational areas are theaters of operations with special requirements. Moreover, ADP 3-28 recognizes that DSCA is a joint mission

that supports the national homeland security enterprise. The Department of Defense conducts DSCA under civilian control, based on U.S. law and national policy, and in cooperation with numerous civilian partners. This publication supersedes ADP 3-28, dated 26 July 2012 and ADRP 3-28, dated 14 June 2013.

ADP 3-37, Protection. ADP 3-37 provides guidance on protection and the protection warfighting function. It establishes the protection principles for commanders and staffs who are responsible for planning and executing protection in support of unified land operations. The synchronization and integration of protection tasks enable commanders to safeguard bases, secure routes, and protect forces. This publication supersedes ADP 3-37 and ADRP 3-37, dated 31 August 2012.

FIELD MANUALS

FM 1-05, Religious Support. FM 1-05 provides a cohesive understanding of the fundamentals of religious support. It is the Army's doctrinal source for religious support planning, training, and execution. This manual is a key integrating publication that links the doctrine for the Chaplain Corps with Army and joint doctrine. FM 1-05 provides operational guidance for commands and religious support personnel at all echelons and forms the foundation for all United States Army Chaplain Center and School curricula.

This publication supersedes FM 1-05, dated 5 October 2012.

FM 3-13.4, Army Support to Military Deception. FM 3-13.4 provides techniques to assist planners in planning, coordinating, executing, synchronizing, and assessing military deception. This publication guides leaders to develop deception plans that integrate into each phase and through each transition to strengthen their ability to retain initiative throughout an operation. Successfully planned deceptions enable units to act faster than the enemy can make decisions, creating positions of relative advantage.

This is a new publication.

Doctrine Corner

ARMY TECHNIQUES PUBLICATIONS

ATP 1-05.02, Religious Support to Funerals and Memorials.

ATP 1-05.02 provides fundamental doctrinal guidance on the execution of funerals and memorial events. It establishes a common understanding, foundational concepts, and methods for executing religious support during funeral services and memorial events. ATP 1-05.02 provides comprehensive doctrinal guidance on religious support techniques for chaplains and religious affairs specialists. The techniques discussed serve as a guide and are not considered prescriptive. ATP 1-05.02 nests with FM 1-05. This publication supersedes ATP 1-05.02, dated 29 March 2013.

ATP 1-05.03, Religious Support and External Advisement.

ATP 1-05.03 establishes a common understanding, foundational concepts, and methods for advising commanders on the impact of religion on operations. ATP 1-05.03 highlights the external advisement capability for chaplains and religious affairs specialists operating from battalion through echelons above corps to support the full range of military operations. ATP 1-05.03 expands upon FM 1-05, *Religious Support*, in describing external advisement as a required capability of chaplain sections and unit ministry teams. This publication supersedes ATP 1-05.03, dated 3 May 2013.

ATP 2-01.3, Intelligence Preparation of the Battlefield. ATP 2-01.3 explains how to systematically evaluate the effects of significant characteristics of an operational environment for specific missions. It describes how the commander and staff examine mission variables to understand how these variables may affect operations. It also discusses intelligence preparation of the battlefield (IPB) as a critical component of the military decision-making process, how IPB supports decision making, and the integrating processes and continuing activities. ATP 2-01.3 also facilitates a common understanding, foundational concepts, and methods of the IPB process. This publication supersedes ATP 2-01.3/MCRP 2-3A, dated 10 November 2014.

ATP 3-01.85, Patriot Battalion Techniques. ATP 3-01.85 provides doctrinal guidance and direction for Patriot units. It focuses on the functions, capabilities, and techniques shared in common by all Patriot battalions. Core capabilities require all Patriot battalions to be highly adaptive, flexible, and responsive to contingencies, globally. It also informs readers

who require an understanding of Post Deployment Build-8 software and hardware upgrades to the Patriot weapon system. This publication is complementary to Patriot technical manuals. This publication supersedes ATP 3-01.85, dated 22 March 2016.

ATP 6-02.40, Techniques for Visual Information Operations.

ATP 6-02.40 is the primary doctrine publication for visual information operations to support the Army's mission. It provides techniques associated with the components of visual information operations and establishes nonprescriptive ways or methods that combat camera Soldiers perform missions, functions, and tasks associated with visual information. It expands on the visual information foundations and tenets established in FM 6-02, *Signal Support to Operations*. Information in ATP 6-02.40 includes roles and responsibilities that enable and support the Army's mission at all echelons. It outlines the Defense Media Activity and its operating components. This publication supersedes ATP 6-02.40, dated 27 October 2014.

MULTI-SERVICE

ATP 3-34.84, Multi-Service Tactics, Techniques, and Procedures for Military Diving Operations. ATP 3-34.84 serves as a reference to ensure effective planning and integration for diving operations. It describes military dive mission areas, force structure, equipment, and primary missions each Service could provide in support of joint operations to assist commanders and staffs at all levels. This publication supersedes ATP 3-34.84/MCRP 3-35.9A/NTTP 3-07.7/AFTTP 3-2.7, CGTTP 3-95.17, dated 13 February 2015.

ATP 3-52.1, Multi-Service Tactics, Techniques, and Procedures for Airspace Control. ATP 3-52.1 is a single source, descriptive reference guide to facilitate multi-Service coordination, integration, and control of airspace during exercises, contingencies, and other operations where Service components must share airspace for operational use. It supports planners and warfighters by establishing tactics, techniques, and procedures for planning, coordinating, and executing airspace control in a multi-Service environment. This publication supersedes ATP 3-52.1/MCWP 3-25.13/NTTP 3-56.4/AFTTP 3-2.78, dated 9 April 2015.



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 Army MI professionals

Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the intelligence community. 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 of equipment and personnel. 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 consider the following:

- ◆ 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 quarterly themes, you do not need to write your article specifically to that theme. We publish non-theme articles in most issues.
- ◆ Please do not include any personally identifiable information (PII) in your article or biography.
- ◆ Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- ◆ All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

What we need from you:

- ◆ Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.

- ◆ A cover letter/email with your work or home email, telephone number, and a comment stating your desire to have your article published.
- ◆ **(Outside of USAICoE)** A release signed by your unit's information security officer stating that your article and any accompanying graphics and photos are unclassified, not sensitive, and releasable in the public domain. A sample security release format can be accessed via our webpage on the public facing Intelligence Knowledge Network website at: <https://www.ikn.army.mil/apps/MIPBW>
- ◆ **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297 or 520-533-4662) for information on how to get a security release approved for your article. A critical part of the process is providing all of the source material for the article to the information security reviewer in order to get approval of the release.
- ◆ Article in Microsoft Word; do not use special document templates.
- ◆ Pictures, graphics, crests, or logos relevant to your topic. Include complete captions (the 5 Ws), and photographer credits. Please do not send copyrighted images. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg.** Photos must be at least 300 dpi. If relevant, note where graphics and photos should appear in the article. PowerPoint (**not in .tif/.jpg format**) is acceptable for graphs, figures, etc.
- ◆ The full name of each author in the byline and a short biography for each. Biographies should include authors' 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 may contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

Submit articles and graphics to usarmy.huachuca.icoe.mbx.mipb@mail.mil. For any questions, email us at the above address or call 520-533-7836/DSN 821-7836.

MIPB (ATZS-DST-B)
Dir. of Doctrine and Intel Sys Trng
USAICoE
550 Cibeque St.
Fort Huachuca, AZ 85613-7017



1st SFAB



2nd SFAB



3rd SFAB



4th SFAB

Army Intelligence Strategies and Innovations



MIPB Professional Bulletin

July - September 2019
PB 34-19-3
Volume 45 Number 3

Army Intelligence Strategies and Innovations

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.

FEATURES

- 1 Mission Command Intelligence in Multi-Domain Operations**
by LTG Scott D. Berrier
- 7 U.S. Army Intelligence and Security Command Strategy**
by MG Gary W. Johnston and Mr. Richard A. Harfst
- 12 Fixing Echelons above Brigade Sensor Challenges in Multi-Domain Operations**
by COL William Adams, COL Mark Dotson, COL Jennifer McAfee, COL Francesca Ziemba, and Mr. Dwight DuQuesnay
- 19 Enabling Battalion S-2 Sections for the Pace of Large-Scale Ground Combat Operations**
by TRADOC Capability Manager-Foundation and Program Manager DCGS-A Team
- 21 Intelligence Policy Considerations in Large-Scale Combat Operations**
by Mr. Gregory Hatter, Mr. Scott Schultz, Mr. Craig Bell, COL Lisa Walker, and COL Bill Mangan
- 26 Aligning Intelligence Preparation of the Battlefield Doctrine with the Current Threat**
by Ms. Terri M. Lobdell
- 29 On Data Science and Intelligence Analysis**
by CPT Iain J. Cruickshank
- 33 Human Intelligence as a Deep Sensor in Multi-Domain Operations**
by COL Justin Haynes
- 40 The Military Intelligence Corps 2019 Hall of Fame Inductees**

Military Intelligence Professional Bulletin (MIPB) presents information designed to keep intelligence professionals informed of current and emerging developments within intelligence.

**MIPB mobile APP is now AVAILABLE for
Android and the iPhone**

The APP can be accessed by going to <https://play.google.com> (for Android) or the Apple App Store (for iPhone) and searching for MIPB.





Mission Command Intelligence in Multi-Domain Operations

by Lieutenant General Scott D. Berrier

Introduction

The Army's new operating concept, multi-domain operations, describes how our Service contributes to the joint force's efforts to deter and defeat near-peer and peer aggression in both competition and conflict—our primary task as defined by the 2018 National Defense Strategy. This concept signifies a seismic shift from the counter-insurgency-centric approach the Army has followed in prosecuting multiple conflicts in the Middle East and Africa over the past 17 years. In order for the Army to succeed in multi-domain operations, the Military Intelligence Corps must evolve, innovate, and modernize in order to enable the Nation's premier ground force to achieve overmatch against our Nation's adversaries and win. Mission Command Intelligence (MCI) is our framework to achieve this goal by the year 2028.

Strategic Context

Our operating environment is changing rapidly, with strategic competition between nation states now surpassing violent extremism as the central challenge to American prosperity and security. Russia has recovered from more than two decades of degraded military capability and capacity by modernizing weapon systems and reforming its armed forces while evolving niche capabilities for hybrid warfare operations. Russia has coupled this modernization with a foreign policy stance designed to control its near abroad and simultaneously re-establish Moscow's position as a global power. China, bolstered by the world's second largest economy, has extended its global influence through the Belt and Road Initiative. With this initiative, China has skillfully integrated economic, diplomatic, and informational instruments of national power while rapidly improving

its military force projection capabilities and establishing its first enduring overseas bases. These efforts now enable China to contest United States and allied power throughout East Asia, the South China Sea, and beyond. Beijing's adroit posturing of its newfound capabilities poses a significant challenge to the world order cultivated by the victors of the Second World War. In addition to Russia and China, Iran and North Korea threaten the interests of the United States and our allies by fielding forces enabled by advanced technology, backed by weapons of mass destruction, and driven by regimes whose objectives are in sharp contrast to American values. Additionally, violent extremist organizations will remain a persistent menace to U.S. interests for the foreseeable future sustained by both state and non-state actors. In order to mitigate these threats, we must accelerate our ability to understand changes in this environment, enabling commanders to outpace our adversaries' decision cycles.

Multi-Domain Operations Overview

Army forces, as an element of the Joint Force, conduct [multi-domain operations] MDO to prevail in competition; when necessary, Army forces penetrate and dis-integrate enemy anti-access and area denial systems and exploit the resultant freedom of maneuver to achieve strategic aims (win) and force a return to competition on favorable terms.

TRADOC Pamphlet 525-3-1¹

The Army's new concept of multi-domain operations described in TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*, addresses how our Service will solve the primary problem posed by near-peer and peer adversaries' standoff in all domains—space, cyberspace, air, sea, and land.

Standoff separates the joint force in time, space, and function, in both competition and conflict. Political action, operations in cyberspace, and information and influence campaigns form just some of the means our adversaries leverage to achieve this separation at the strategic level while setting advantageous conditions at the operational and tac-

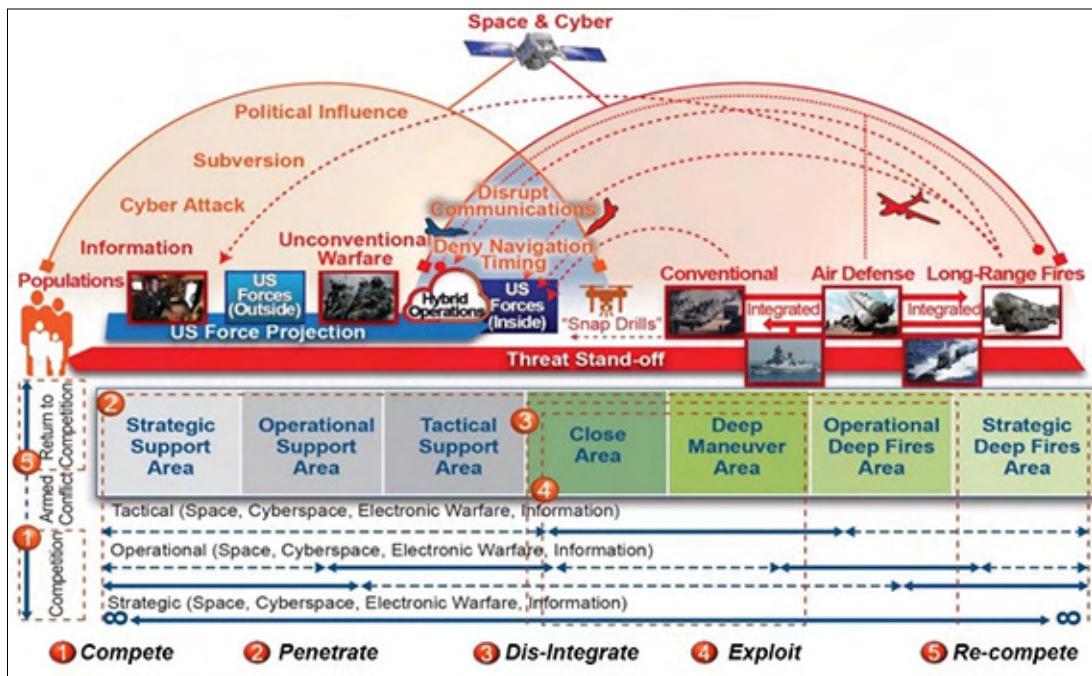


Figure 1. Threat Problems Superimposed on the Multi-Domain Operations Framework²

tical levels. Deep-sensing intelligence, surveillance, and reconnaissance (ISR) systems tied to long-range integrated air defense systems and ballistic and cruise missile forces form antiaccess and area denial (A2AD) conditions that provide standoff at the operational and tactical levels. U.S. Army forces must maintain readiness during extended periods of competition while preparing to penetrate and disintegrate threat A2AD systems early in conflict, create windows of opportunity and periods of advantage, and exploit gains in order to resolve conflicts on terms favorable to American interests. Army intelligence is vital to supporting U.S. land power and supporting the joint force in order to prevail in this environment.

Mission Command Intelligence Overview

MCI is the Army intelligence enterprise's overarching framework to achieve an end state of a ready Army intelligence team supporting mission command against all threats in multi-domain operations by 2028. It aligns intelligence requirements, planning, development, and resourcing efforts with the Army's multi-domain operations concept. MCI will enable commanders to achieve decision superiority with the speed, precision, and accuracy required to integrate and synchronize combat operations in multi-domain environments.

MCI's essential components are sensors, data, and analysis enabled by a cloud-based network architecture. These components empower intelligence professionals to execute doctrinal intelligence process functions assisted by the advantages of advanced technology and cutting-edge capabilities. Accordingly, MCI provides commanders the essential

Mission Command Intelligence is the Army intelligence enterprise's overarching framework to field a ready Army Intelligence team supporting mission command against all threats in multi-domain operations by 2028.

MCI Components Describe Characteristics Driving Our MI Modernization Priorities

Sensors

- Detect and collect advanced signatures in all domains
- Penetrate, collect, and survive in A2 / AD environments
- Collaborative capabilities across terrestrial, aerial, and space layers
- Automated sensor fusion across disciplines
- Direct sensor reporting to data architectures & fire control systems

Data

- Assured access to data at echelon and across theaters of command
- Ingest and process data from DoD, IC, commercial, open source and PAI
- Common DoD / IC standards shared throughout DoD, IC, allies and partners
- Seamless transitions from competition to conflict in all environments

Analysis

- Analyst functions integrated within COE
- High compute processing (AI / ML) automates fusion of discrete signatures
- Automated IPB and collection management processes
- Analytic workflows support dynamic modeling and forecasting
- Advanced tradecraft supported by intuitive analyst interfaces
- Rapid generation of user-based tools and applications (DevOps)

A2 antiaccess
AD area denial
AI artificial intelligence
COE common operating environment

DevOps development operations
DoD Department of Defense
IC intelligence community
IPB intelligence preparation of the battlefield



MCI Increases the Speed, Precision, and Accuracy of the Intelligence Process

MCI Mission Command Intelligence
MI military intelligence
ML machine learning
PAI publicly available information

Figure 2. Mission Command Intelligence³

means to synchronize other warfighting functions and deliver sound, timely decisions, posturing friendly forces with decisive advantage. In the context of multi-domain operations, MCI supports the Total Army's effort to achieve convergence⁴ across time, space, and in all domains.

Sensors

Army Vision 2028 calls for units from brigade through corps to possess the ability to conduct sustained ground and aerial ISR, electronic warfare, and cyberspace operations. By 2028, the Army's access to sensors must enable commanders to illuminate our adversaries' diverse array of formations and capabilities through the depth of the battlefield, exposing vulnerabilities we can exploit at the time, place, and in the domain of our choosing. MCI requires sensors and platforms adaptable to any operating domain, A2AD environments, and contested electromagnetic spectrum conditions while remaining capable of collecting against signatures generated by evolving threats. Sensors must penetrate the battlespace in greater depths than the maximum effective range of enemy A2AD systems. The robust use of human intelligence, as a deep sensor, by conventional and special operations forces will enable tipping and cueing, defeat spoofing and deception, and provide alternate collection in a contested or degraded electromagnetic environment. This framework allows the application of enterprise intelligence capabilities in mass at each echelon. These capabilities are deployable, scalable, and designed to provide commanders

with the timely, accurate, and precise situational awareness they need to fight and win.

Data

Army, joint, and national sensors will produce data in volumes and at velocities that will overwhelm cumbersome legacy processing systems. Commercial collection assets and open source information will only add to this challenge. Consistent access and discoverable data require common data configuration and reporting standards within the Army intelligence enterprise and the intelligence community. Common formatting, standards, and security protocols establish the foundation for seamless collaboration and sharing between all Services and the intelligence community, and facilitate greater forward momentum in our efforts to develop cloud-based networks. We will weave these standards into the fabric of our data technologies before integrating them into our networks. This design discipline will sustain continuity and consistency of access for all consumers operating on any platform. Army intelligence Soldiers, Civilians, and supporting contractors must leverage their access to data in order to increase the speed, precision, and accuracy of their analysis and targeting support to commanders at all echelons on the multi-domain operations battlefield. Dedicated data scientists⁵ must be integrated at echelon in order to facilitate the methods by which our forces ingest, curate, and process data into information suitable for analysis.

The key to converging capabilities across all domains, the [electromagnetic spectrum] EMS, and the information environment is high-volume analytical capability and sensor-to-shooter links enabled by artificial intelligence, which complicates enemy deception and obscuration through automatic cross-cueing and target recognition.

TRADOC Pamphlet 525-3-1⁶

Analysis

In collaboration with our joint Service partners, the Total Army intelligence enterprise must evolve processing, exploitation, and dissemination (PED) data competencies in both competition and conflict. Project Maven's integration with the Army PED enterprise at Fort Gordon, Georgia, represents one of the first steps toward this objective. By 2028, we will have integrated artificial intelligence (AI) and machine learning algorithms into our processes, reducing analytic cognitive burden. We will develop intuitive analyst-system interfaces nested with the Army's Command Post Computing Environment. Doing so will enable our Army to rapidly field tools and applications our Soldiers can configure to their specific roles and functions. These efforts are designed to enhance our analysts' efficiency and effectiveness in applying critical thinking and analytical judgment, based on training and experience, to their assessment of the multi-domain operations battlefield.

Analytic initiatives must remain responsive to the demands of a changing operational environment. They will increasingly draw upon solutions designed through the expertise of a growing talent pool of Soldiers, lessening Army reliance on commercial-sector providers. Our force must incorporate DevOps⁷ practices in order to increase the rate at which software and analytic development interacts with users to deliver actionable tools. DevOps at echelon will be instrumental in enabling intelligence professionals to employ advanced analytics at the same pace as intelligence requirements change in accordance with the unpredictable operational environments we anticipate. These actions will support the creation and management of a global integrated common intelligence picture, which also describes adversarial intelligence collection for counterintelligence purposes.

Enabling Architecture

Secure data and networks must ensure connectivity and data access appropriate to each echelon of command, with seamless transitions from home station to the forward edge of battle. By 2028, the Army intelligence warfighting function must have universal access to secure cloud-based data. Leveraging cloud architectures, our multidiscipline intelligence teams will access data for processing and ex-

ploitation, and disseminate their intelligence products with unprecedeted reach using the same architecture. In the event our network is degraded, intermittent, or limited, deployable cloud nodes will sustain our forces with data pertinent to their mission and environment.

Visualizing Mission Command Intelligence

MCI's essential components are applicable at all levels of command and throughout the depth and breadth of the multi-domain operations battlefield framework. At the tactical level, S-2s will leverage AI and data from deployable cloud nodes to expeditiously progress through the manpower-intensive steps of the intelligence preparation of the battlefield process. When describing battlefield effects, AI will assist analysts in rapidly producing an automated modified combined obstacle overlay (MCOO) while dynamically updating the product as factors change in the operational environment. This system will process weather forecasts and incorporate terrain factors such as elevation, slope, vegetation, and hydrology to automatically adjust for cross-country trafficability and anticipated rates of movement, and will refine assessed ranges of observation for both friendly and threat forces. This "live action MCOO" will allow analysts to focus time and energy on evaluating the threat and determining threat courses of action. After the S-2 develops the threat course of action, AI will identify potential changes to the course of action in real time. For example, if a destroyed bridge or other obstacle degrades a proposed enemy axis of advance, algorithms will identify alternate routes with corresponding time-phase lines. These AI-derived deviations within each threat course of action will guide named area of interest development and improve ISR collection planning. This concept is no different from the mapping and route planning applications we use on our smart phones today to account for traffic, weather, and other conditions. We use these tools in everyday life to make decisions. Using the most accurate information available to us, we then apply human experiential judgment to select the best course of action.

At both the tactical and operational level, MCI will be decisive in supporting targeting by increasing the speed, accuracy, and precision with which commanders are able to drive kill chains focused on high-value and high-payoff targets. AI will assist S-2s and targeteers by automatically correlating discreet signatures detected by multi-domain sensor systems, across all intelligence disciplines, rapidly focusing collection on named areas of interest developed through processes similar to the S-2 vignette on the next page. As analysts progress more rapidly through the intelligence preparation of the battlefield cycle and develop more

precise collection plans, modernized ISR sensors will be able to provide high-fidelity targeting information to support long-range precision fires in the deep maneuver and operational deep fires areas of the multi-domain operations framework. This capability could be employed in the following operational setting.

Artificial Intelligence Assists S-2s and Targeteers

A multi-domain task force (MDTF) commander is tasked with disintegrating an enemy A2AD network established by the threat's integrated fires command. The network is composed of long-range air defense forces and land attack missiles tied together by digital mission command systems. In order to accomplish this mission, the MDTF must sense, identify, and target the command and control assets associated with the integrated fires command headquarters, and its subordinate SS-26 short-range ballistic missile and SA-21a surface-to-air missile brigades. The MDTF S-2's collection plan specifies that the command and control vehicles associated with the integrated fires command are high-value targets, each with unique visual, electromagnetic, thermal, and cyberspace signatures.

Essential to the dis-integration effort is continuous refinement of intelligence through multiple domains to enable the Joint Force to see or stimulate and strike the enemy's remaining anti-access and area denial systems.

TRADOC Pamphlet 525-3-1⁸

Drawing from data in a deployable cloud node, AI algorithms search for multidiscipline intelligence reporting associated with these unique signatures, rapidly correlating seemingly disparate information into cohesive reports. This process significantly improves the S-2's ability to eliminate redundant reporting while allowing analysts to confirm templated enemy assets on the situation map, all with greater precision. Using this knowledge, the MDTF commander will be able to employ advanced sensors, such as drone swarms or expendable artillery-delivered unmanned aircraft systems, to collect precise locational information. This information can be injected directly into long-range precision fires delivery systems accurately conducting

near-peer and peer competitors, creating decision space for strategic leaders. In all cases, multi-domain analysis platforms, fusing all intelligence disciplines, enabled by cyberspace operations must employ AI analytics against massive quantities of data to rapidly identify, neutralize, and defeat threats to our force at home and abroad.



Photo by U.S. Navy PO1 Danica Simans

The Army's multi-domain task force operates from a tactical command post as part of Valiant Shield 2018.

kinetic or non-kinetic fires neutralizing or destroying the high-value targets. Battle damage assessment will be improved as the S-2 leverages AI analytics to rapidly correlate indicators provided by a multidiscipline array of networked sensors to confirm the long-range precision fires' effects successfully destroyed the target. Taking into account the battle damage assessment and targeting effects, AI may also assist in supporting rapid follow-up strikes by using predictive analytics to template the enemy's reaction upon the loss of critical systems or capabilities.

Long-range ground fires offer a responsive strike capability (cued by intelligence within minutes), with the capacity to overwhelm point defenses and strike targets over larger areas.

TRADOC Pamphlet 525-3-1⁹

The multi-domain operations concept is predicated upon our Nation's ability to generate and project power from the continental United States, making MCI's components vital to Army intelligence operations in the strategic and operational support areas in the competition phase as well as during conflict. Adversaries seek to acquire sensitive technologies and to disrupt supply chains and force generation/projection platforms, requiring tailored sensors to meet these threats. Adversary espionage operations and insider threats must also be subject to counterintelligence detection and neutralization in accordance with appropriate legal authorities to enable the protection of critical technologies. Special operations forces will operate throughout all areas of the multi-domain operations framework, leveraging MCI's components to counter adversary gray-zone operations by illuminating threat information campaigns, exposing covert actors, and attributing clandestine shaping operations to

The Way Forward

MCI is not only a framework; it is a call for action and must drive modernization requirements and stimulate innovation. MCI will lead us to field new equipment and systems while empowering our Soldiers and Civilians to develop creative solutions to emerging challenges. The military intelligence generating force, including the U.S. Army Intelligence Center of Excellence and our military intelligence teammates within Army Futures Command, must ardently define and drive these requirements to develop, prototype, test, and field ISR systems at a pace that ensures they will remain relevant and enable Army forces to achieve and maintain technical overmatch in comparison to our peer competitors. Technology protection is paramount to this effort. The generating force must also assess our current military intelligence organizations and modify force design to best position intelligence systems with other warfighting formations

for operations in contested environments. Institutional training and development will ensure our Soldiers and Civilians are prepared to provide a decisive human advantage during MCI-enabled multi-domain operations in both competition and conflict.

The operating force, U.S. Army Intelligence and Security Command, U.S. Army Forces Command, U.S. Army Special Operations Command, and those forces under the operational control of Army Service component commands, will employ modern capabilities to sense throughout the depth and breadth of the operational environment, in all domains, and deny the enemy's ability to do the same. MCI sensors, engaging all intelligence disciplines, will provide volumes of data that will feed the cloud-based architecture and enhance accessibility by all. Analysts will process this data into information and provide accurate and precise intelligence assessments using platform-agnostic user interfaces that are directly incorporated into the future Command Post Computing Environment.

Despite these technological advancements, no amount of technology will replace the Military Intelligence Corps' greatest resource—the experience, judgment, and intuition of highly trained men and women who make up our corps. Fundamentals-based training is vital to ensuring that doctrinal skillsets are thoroughly inculcated within our formations, at each level of professional military education. Furthermore, live, virtual, and constructive training environments called for by the Military Intelligence Training Strategy must stimulate innovation and instill critical thinking throughout our team.

Conclusion

MCI enables mission command in multi-domain operations by the year 2028 by rapidly organizing and analyzing historic and current collected data from all sources, providing relevant conclusions for commander's decision-making processes and multi-domain targeting. Our ability to leverage secure data in all formations in degraded, intermittent, and limited environments is vital to enabling analysts to develop accurate assessments for their commanders and supported forces. Sensors, capable of detecting advanced signatures throughout the depth and breadth of the multi-

domain operations battlefield framework, will feed our cloud-based architecture, allowing us to employ AI analytics. These AI tools will enable our analysts to efficiently apply their training, experience, and judgment, resulting in timely and accurate intelligence assessments. MCI will not replace the fundamental principles of the intelligence process and other doctrinal processes; rather, it will empower our team to harness technological advancements to accomplish the mission. Doing so will ensure our Army can deter, fight, and win on any battlefield, against any foe, now and into the future.



Endnotes

1. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 17; emphasis added.
2. Ibid., 16.
3. Illustration provided by COL Justin Haynes, U.S. Army, Deputy Chief of Staff, Intelligence, Initiatives Group.
4. “Convergence is rapid and continuous integration of capabilities in all domains, the [electromagnetic spectrum] EMS, and the information environment that optimizes effects to overmatch the enemy through cross domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative.” Department of the Army, TRADOC Pamphlet 525-3-1, 20.
5. Bradley M. Knopp, Sina Beagley, Aaron Frank, Rebeca Orrie, and Michael Watson, *Defining the Roles, Responsibilities, and Functions for Data Science Within the Defense Intelligence Agency* (Santa Monica, CA: RAND Corporation, 2016), 17-21.
6. Department of the Army, TRADOC Pamphlet 525-3-1, 38; emphasis added.
7. “DevOps (a clipped compound of ‘development’ and ‘operations’) is a software engineering culture and practice that aims at unifying software development (Dev) and software operations (Ops). The main characteristic of the DevOps movement is to strongly advocate automation and monitoring at all steps of software construction, from integration, testing, releasing to deployment, and infrastructure management. DevOps aims at shorter development cycles, increased deployment frequency, and more dependable releases.” D. Jeya Mala, *Integrating the Internet of Things Into Software Engineering Practices* (Hershey, PA: IGI Global, 2019), 16.
8. Department of the Army, TRADOC Pamphlet 525-3-1, 38; emphasis added.
9. Ibid., 33; emphasis added.

LTG Berrier has served as a “2” at every level in the Army from battalion through corps. He commanded military intelligence formations at Fort Ord, CA; Fort Wainwright, AK; Fort Drum, NY; the Republic of Korea; and Fort Huachuca, AZ. His joint assignments include U.S. Central Command, Special Operations Command-Central, Combined Joint Task Force-180, Combined Joint Task Force-76, Multi-National Corps-Iraq, U.S. Forces Korea, International Security Assistance Force, and Resolute Support Headquarters. He currently serves as the Army’s 46th Deputy Chief of Staff for Intelligence, G-2.

U.S. Army Intelligence and Security Command Strategy



by Major General Gary W. Johnston and Mr. Richard A. Harfst

INSCOM
United States Army
Intelligence and Security Command

Part I, Introduction

Overview

Our strategy is about preparing for the future fight—a fight that is faster and more lethal, information-centric, and globally interconnected than ever before—while building near-term readiness and executing today’s missions. For nearly a generation we’ve been engaged in the post 9/11 wars; while those wars continue and the Soldiers and Civilians in harm’s way will receive our full support, we must look ahead and shape ourselves for what’s next.

“We cannot solve our problems with the same thinking we used when we created them.”

—Albert Einstein

For many of you, this guidance only represents half of the equation, as you must also ensure you are fully nested with your supported command or agency; I understand that. I also recognize what’s reflected here represents only a small portion of what we need to accomplish. Because there are many competing requirements, it is imperative that we prioritize the investment of our resources if we hope to see measurable progress toward our most critical efforts. I look forward to a continuing dialogue as we work toward accomplishing these goals together.

Our History, Our Role

Understanding U.S. Army Intelligence and Security Command’s (INSCOM) unique value for both today and tomorrow begins with a basic understanding of our past. From World War II through Vietnam, Army intelligence was organized predominantly in single-discipline or “stovepipe” organizations. The structure evolved haphazardly, and there were serious questions about its operational and cost effectiveness. The 1974-75 Intelligence Organization and Stationing Study identified several operational intelligence deficiencies during the Vietnam War that resulted from a key gap in the Army intelligence structure. Then, and now, the Army needed a single organization to provide **unity of**

command to synchronize multidiscipline intelligence and bridge the gap between the national intelligence community (IC) and tactical forces. INSCOM exists to fill these gaps.

For much of the Cold War era, INSCOM operated almost exclusively at the “echelon above corps” level. Over time, INSCOM has extended its support, eventually reaching brigade combat teams and below. Today, both horizontal integration (i.e., across intelligence disciplines) and vertical integration (i.e., between echelons of command) are more sophisticated and interdependent, and occur across a broader range of activities than ever before. Army intelligence operates as an interdependent enterprise, and INSCOM has a central role to **“connect and deliver the enterprise.”** In a world where events and resources from one area of responsibility increasingly affect others, INSCOM helps military intelligence (MI) units and staffs at echelon leverage enterprise assets and services. This includes being responsible and able to:

- ◆ Manage the Army’s fair-share contribution to the IC.
- ◆ Bridge intelligence-related gaps/boundaries by leveraging placement, access, and interior lines of communication:
 - ◆ Between and among intelligence disciplines (multidiscipline).
 - ◆ Between national/joint and tactical levels.
 - ◆ Across areas of responsibility and domains.
 - ◆ Between multiple coalitions/partner nations and the United States.
 - ◆ Between active component and reserve component.
 - ◆ Between conventional forces and special operations forces.
 - ◆ Between institutional Army and operational forces.

What is “Enterprise”?

For the purposes of this paper, an enterprise is defined as a group of separate organizations working toward a unified objective together; an enterprise approach is a business model (or operating process) that accounts for a lack of self-sufficiency and the dependencies necessary for optimal results.

- ◆ Scale advanced or complex intelligence operations/activities and efficiently manage specialized, low-density intelligence warfighting function capabilities (including “common-user” enablers) to support (i.e., “downward reinforce”) units at echelon.
- ◆ Maintain underpinnings of Army-wide intelligence readiness for an expeditionary force:
 - ◆ Leverage global situational awareness and understanding to prevent “cold starts” and enhance responsiveness, including development of foundational intelligence and management of the associated databases and theater-specific architectures.
 - ◆ Enhance skills development through continuous engagement (e.g., live-environment training).
 - ◆ Ensure linkage of training and certification standards to MI, IC/joint levels, and Army development.
 - ◆ Support intelligence-specific readiness for reserve component MI forces.
- ◆ Support institutional intelligence requirements, including:
 - ◆ Army acquisition and design of the future force.
 - ◆ The Army’s ability to protect and secure its forces, information, technologies, and other resources.

Part II, The Strategic Context

INSCOM’s strategy reflects higher-level strategic guidance. While the totality of guidance was considered, the goals outlined below are a direct continuation of requirements derived from three key documents: *The Army Strategy*, *The U.S. Army in Multi-Domain Operations 2028*, and *The Army Intelligence Plan* (Draft). These documents, which collectively provide our long-term azimuth, should be considered required reading for INSCOM leaders.

The U.S. Army’s Mission

The U.S. Army’s mission is to deploy, fight, and win our Nation’s wars by providing ready, prompt, and sustained land dominance by Army forces across the full spectrum of conflict as part of the joint force.

The Army Vision

The Army of 2028 will be ready to deploy, fight, and win decisively against any adversary, anytime and anywhere, in a joint, multi-domain, high-intensity conflict, while simultaneously deterring others and maintaining its ability to conduct irregular warfare. The Army will do this through the employment of modern manned and unmanned ground combat vehicles, aircraft, sustainment systems, and weapons, coupled with robust combined arms formations and tactics based on modern warfighting doctrine and centered on exceptional leaders and Soldiers of unmatched lethality.

The Army Intelligence Vision

The Army intelligence vision is a ready Army intelligence team supporting mission command against all threats in multi-domain operations by 2028.

Part III, How I See INSCOM—Who We Are

Our people—military, civilians, and contractors—are the cornerstone for everything we do. As leaders, we must continually foster an environment that creates conditions for individuals to thrive. We must:

- ◆ Promote and model the Army and INSCOM values.
- ◆ Build and model trust and respect throughout the force.
- ◆ Develop and take care of people.

We are INSCOM. *We are a values-based team of professionals who are committed to contributing and evolving our individual and collective talents, skills, and abilities to nurture positive constructive relationships, build effective and sustainable partnerships, and master and leverage new technologies in order to identify, enable, and empower innovative and dynamic solutions to current, emerging, and future challenges to our Army and our Nation.*

We represent the best our Nation and our Army have to offer. We accept that the future demands that we remain dedicated to constant self-improvement, personal and professional growth, and constructive self-assessment and evaluation.

We are entrusted by our Nation, our Army, and our Soldiers to employ all the skills, capabilities, resources, and authorities we are given in order to protect our Soldiers and our Nation. We understand that we are responsible, individually and collectively, to ensure that everything we do reinforces the Nation’s willingness to place its faith and trust in our ability and judgment.

Individually, we represent many different backgrounds and skillsets. Together, we form a powerful enterprise that operates within a system of enterprises in order to protect our Nation’s vital interests. Collectively, we have the skills to use all the resources and authorities entrusted to us to deliver decisive intelligence in order to enable our leaders to anticipate and address challenges, enhance Army readiness and warfighting, protect critical capabilities, and enable decision making.

Our Values

Values help define us. The U.S. Army is a values-based organization and its values are rooted in America’s history, culture, and law. These values—loyalty, duty, respect, selfless service, honor, integrity, and personal courage—are our bedrock. Our Nation believes that certain values—including dignity and equality among all people—are universal. Commitment to these beliefs is reflected throughout our country’s history, from our founding, through the wars we’ve fought, to today—where our beliefs help shape our engagements around the world.

In addition, the following values uniquely define INSCOM:

- ◆ **Stewardship.** INSCOM has great responsibilities. We exercise stewardship in three basic areas: people, mission, and resources.
- ◆ **Collaboration.** No commander “owns” all the intelligence assets required. We recognize that a collaborative enterprise approach is necessary for anyone’s, and everyone’s, success.
- ◆ **Innovation.** Learning, adapting, and innovating amidst the backdrop of complexity and uncertainty are central themes in how the Army intends to prepare for the future. INSCOM must be a learning and adaptive organization, champion change, and both value and encourage creativity and innovation in our workforce.

Our Vision

As the premier intelligence warfighting command, we are a powerful enterprise that operates within a system of enterprises. We do this to accomplish three key purposes:

- 1) Provide ready forces to combatant commanders and the IC (this reflects our “man, train, equip” administrative control responsibilities);
- 2) Provide enabling, common-user services to Army forces globally, across all echelons (this reflects our general support to the Army responsibilities as a direct reporting unit); and
- 3) Execute multidiscipline intelligence operations in support of the Secretary of the Army’s Title 10 responsibilities (this reflects our operational control responsibilities).

When an Army intelligence Soldier picks up their comms mic—or clicks their mouse—the power of INSCOM is there!

Our Mission

INSCOM executes mission command of operational intelligence and security forces; conducts and synchronizes worldwide multidiscipline and all-source intelligence and security operations; and delivers linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities in support of Army, joint, and coalition commands and the U.S. IC.

Part IV, Our Strategy

Our strategic end state is to operate as a powerful enterprise, within a system of enterprises, in order to create decision advantage for commanders. We connect and deliver

the intelligence enterprise across the Army. Everything we do is in furtherance of this end state.

In order to achieve this strategic end state we will work along three lines of effort (LOEs) while we conduct and support current operations. These LOEs are a direct continuation of the previous LOEs, and what you, collectively, have already achieved. Figure 1 (on the next page) summarizes our approach.

LOE 1 is Readiness. This LOE began with actions to first craft, and then implement, revitalized training (e.g., annual training guidance, annual/semiannual training briefs, etc.) and readiness assessment metrics and framework to provide an integrated view of current and future readiness. We continue these actions with an understanding that building readiness—or preparedness—is a continuous process. As such, we are expanding our aperture to include other impacts on readiness, over time. Developing our workforce (previously a separate LOE), enhancing our infrastructure (i.e., our geographical footprint, facilities, and ability to “set the globe” in order to rapidly respond anywhere, anytime), securing resources (i.e., force management, program objective memorandum/budget, and contracting), and clarifying authorities and responsibilities are essential to the success of, and impacted by, everything we do. Our objective, a trained and ready Army intelligence workforce, includes the total command (Soldiers, Army Civilians, and contractors) as well as how we support Army MI readiness.

LOE 2 is Operationalize. This LOE encompasses building our mission command processes (e.g., battle update brief, commander’s update brief, collection management targeting board, etc.) and structure (e.g., Director of Enterprise Operations), combined with other actions (e.g., technical control and analysis element reconstitution and building out the new, state-of-the-art mission command center in our new building), necessary to achieve two distinct but related objectives. The first is our ability to operate the intelligence process in order to proactively conduct multidiscipline, multimodal, multifunctional intelligence operations in support of the Secretary of the Army’s Title 10 institutionally oriented responsibilities. No other organization, either in the Army or in the rest of the IC, directly supports these requirements! While our individual parts have done excellent work in the past, we have not functioned as a unified whole; an enterprise approach is necessary in order to obtain the synergy required and effectively mass on problems. As a direct reporting unit, we also have general support responsibilities: downward-reinforcing support to Army forces at echelon. Our second objective, therefore, is the ability to anticipate and rapidly respond to

The INSCOM Strategy

Connect and Deliver the Enterprise

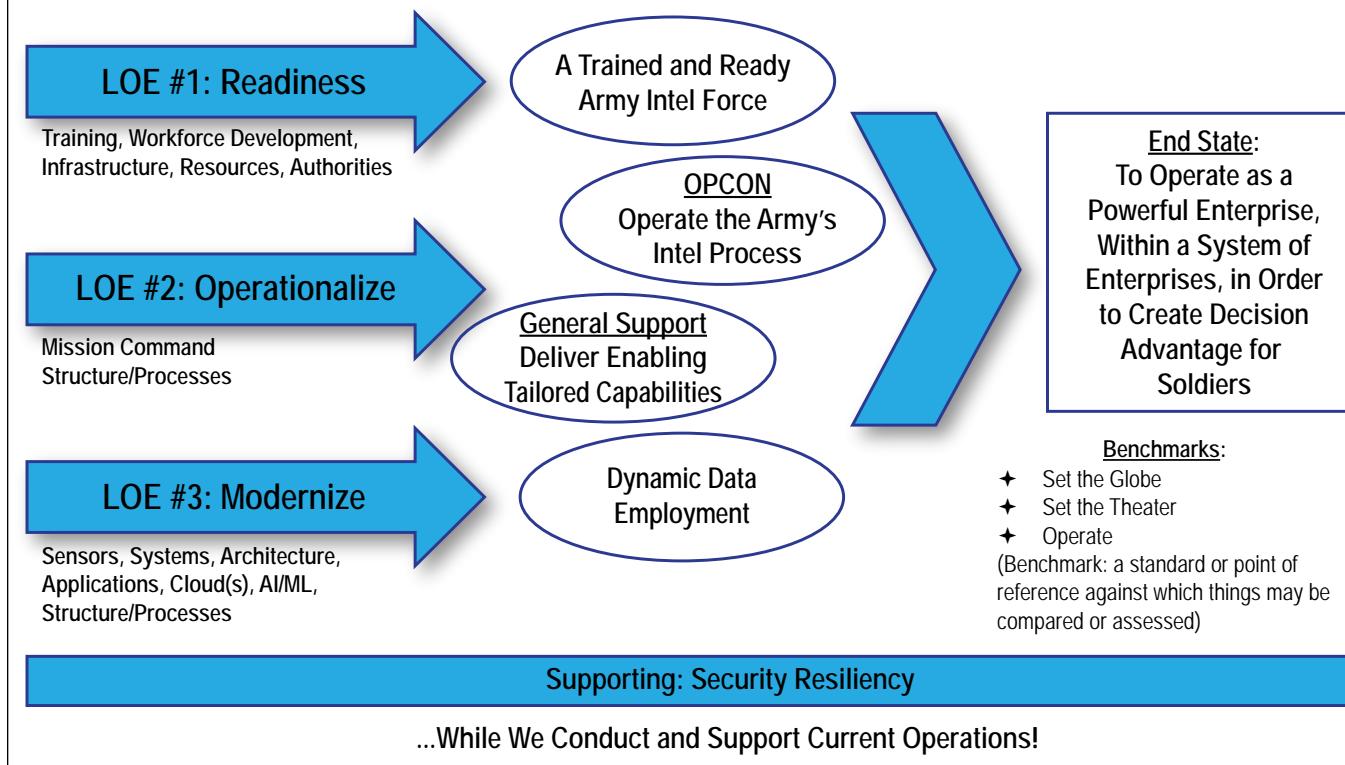


Figure 1. The INSCOM Strategy—Connect and Deliver the Enterprise

commander's requirements and deliver enabling tailored capabilities. Again, while INSCOM has done this, with great success, over the years we have not done so in a predictable, unified manner—as an enterprise. For both objectives, the start point is to see and understand ourselves and the operational environment (blue, green, and red) in all time horizons (i.e., current operations, future operations, and plans) and the guiding principle is to **“operate at the speed of trust.”**

LOE 3 is Modernize. Previously, this was focused exclusively on (and titled) building an effective and secure network architecture. While there's still work to be done in that area, building an effective and secure network architecture was an initial objective—a beachhead from which we make further advances. Today we're ready to start moving forward with other modernization efforts across the gamut of systems and sensors.

The objective is dynamic data employment. Dynamic data employment is a new conceptual framework for how we view and approach the data life cycle. In the past, our main effort was to standardize data structure, networks, processors, and user applications; we sought to optimize each component individually. Going forward we recognize that

a single commander must maneuver data—the right information—from sensor or source, in a variety of structures, through all points of processing (i.e., workspaces), used in an array of applications, to multiple end consumers, in the right format for their needs, in an assured, timely manner, and in a contested environment. The requirement is analogous to how a combined arms commander must synchronize the maneuver of infantry, armor, fire support, engineers, and logistics across any terrain, each with a variety of obstacles, and mass on the objective.

A revolution in military affairs is “based on the marriage of new technologies with organizational reforms and innovative concept of operations.”¹ Technological advances such as cloud computing, artificial intelligence/machine learning, data visualization, the Internet of things, and the proliferation of publicly available information not only make dynamic data employment realistic, but also a requirement in order to compete successfully in the information age.

A supporting effort is security. Enhancing Army security, the Army's ability to protect and secure its forces, information, technologies, and other resources, remains an essential supporting effort for the command. As it is with our intelligence activities, “operating as an enterprise” is our

mantra for the security realm. Our focus is on connecting and synchronizing disparate elements and processes that contribute to security—many of which are outside our control. Moreover, we must nest security functions with intelligence activities in a mutually supportive manner.

Underpinning all of our efforts is the need to align our business processes with our operational and mission command processes. Everybody has to look for ways to work collectively to advance these efforts within their respective areas of expertise. This includes leveraging all the capabilities and talents within INSCOM to identify, recruit, retain, and grow a workforce capable of anticipating, supporting, and driving an uncertain future. It also includes the need to ensure our facilities are designed, equipped, and positioned so that they can best anticipate and support both current and future requirements.

Part V, The Way Ahead

Work on many of these fronts has already begun. In the days ahead, we will develop specific action plans in support of these LOEs and supporting projects. We will share those as they come to fruition. We will discuss this strategy during our routine battle rhythm events and during visits to your units. I look forward to opportunities to discuss how subordinate units are incorporating applicable objectives into their routine operations and battle rhythm. I also expect this guidance to become the “language of INSCOM” and tie activities and discussion, including performance objectives in both military and civilian evaluations, back to specific aspects of this guidance. If there are any recommendations for modifications, please address them with the Enterprise Task Force.



Vigilance Always!

The INSCOM Command Team:

KEVIN G. BOUGHTON

CW5, USA

Command Chief Warrant Officer

ERIC M. SCHMITZ

Command Sergeant Major, USA

GARY W. JOHNSTON

Major General, USA

Commanding

Winning Matters!

Endnote

1. Dan Goure, “The Next Revolution In Military Affairs: How America’s Military Will Dominate,” *The National Interest*, 28 December 2017, <https://nationalinterest.org/blog/the-buzz/the-next-revolution-military-affairs-how-americas-military-23833>.

MG Gary Johnston became the Commanding General, U.S. Army Intelligence and Security Command (INSCOM), on 11 June 2018. He most recently served as Deputy Chief of Staff, Intelligence, Resolute Support Mission, North Atlantic Treaty Organization/Director, J-2, U.S. Forces-Afghanistan, Operation Freedom's Sentinel. He has commanded at every level from company through major command, and has extensive joint and operational experience. MG Johnston holds a bachelor of science in business administration from Arkansas Tech University, a master of science of strategic intelligence from the Joint Military Intelligence College, and a master's degree from the U.S. Army War College.

Mr. Richard Harfst works in the INSCOM Enterprise Task Force office.



Fixing Echelons above Brigade Sensor Challenges in Multi-Domain Operations

Graphic courtesy of the U.S. Air Force



Just like the U.S. Air Force, advanced layered sensing, command and control, and cyber technologies are anticipated to be important contributors to future U.S. Army capabilities. A family of integrated solutions and enablers that increase lethality and survivability are necessary to deliver a multi-domain operations-capable force by 2028.

by Colonel William Adams, Colonel Mark Dotson, Colonel Jennifer McAfee,
Colonel Francesca Ziemba, and Mr. Dwight DuQuesnay

Introduction

At the 2019 Intelligence Senior Leaders Conference, a combined team from the U.S. Army Intelligence Center of Excellence (USAICoE) and U.S. Army Cyber Center of Excellence (USACCoE), representing both Training and Doctrine Command and Army Futures Command, provided an overview of current modernization efforts. The desired end state is a family of integrated solutions and enablers that increase lethality and survivability at echelons above brigade (EAB) in multi-domain operations. This article summarizes the following key elements of the briefing:

- ◆ Problem framing.
- ◆ Capability gaps.

- ◆ Cross-domain initiatives:
 - ◆ Modernized force structure.
 - ◆ Tactical Intelligence Targeting Access Node (TITAN).
 - ◆ Terrestrial Layer System (TLS).
 - ◆ Multi-Domain Sensing System (MDSS).
 - ◆ Distributed Common Ground System-Army (DCGS-A) Capability Drops (CDs) 1 and 2.

Framing the Operational Problem

The Army's current intelligence, surveillance, and reconnaissance (ISR) capabilities at EAB lack the ability to effectively support large-scale ground combat operations against near-peer threats. The current expeditionary-military intelligence brigade (E-MIB) is designed to downward reinforce

to brigade combat team (BCT) level in counterinsurgency and does not provide division and corps commanders with the capabilities they require in large-scale ground combat operations. ISR issues at EAB include insufficient survivability, range, and sensing technology to collect against increasingly complex modern signatures through the entire depth of the battlefield. Near-peer threat systems in service today employ camouflage, concealment, and deception measures and emissions control, and are highly mobile, making detection and engagement difficult. As state actors continue investing in antiaccess and area denial capabilities and as the technology matures, this collection gap will become more acute. Predictable limitations include capacity constraints and ineffective data transport in denied or contested communications environments. Even our most capable theater and national ISR systems will be at risk, or unavailable, because of prioritization.

On a notional operational diagram of a large-scale ground combat battlefield in multi-domain operations, red enemy icons would represent those near-peer assets that current ISR can detect. Today, this is limited to select forces in the close fight area because the bulk of our sensing capability resides in the BCT. A majority of a near-peer adversary's remaining formations could exploit the gap in division and corps collection to exercise freedom of maneuver. This gap includes the deep maneuver and operational deep fires areas. Enemy units operating here are depicted as gray, or unseen, enemy icons.

As the USAICoE Commanding General, MG Robert P. Walters, Jr., says, the problem is we need to turn those gray icons red. The Military Intelligence (MI) Corps must modernize into a highly relevant enabler of lethality and survivability for combat forces in large-scale ground combat operations. Army ISR must be able to sense and target these adversary forces to deny the enemy's operational flexibility and preserve the initiative of friendly commanders. We must also deliver integrated signals intelligence (SIGINT), electronic warfare (EW), and cyberspace capabilities that enable situational understanding, long-range precision fires targeting, and mission command.

Fundamentally, the Army's ISR of 2028 must support the commander's ability to set the theater; enable shaping operations during competition; and facilitate the penetration, disintegration, and exploitation of threat forces.

Intelligence, Surveillance, and Reconnaissance: The Army's Number One Capability Gap in Multi-Domain Operations

After 3 years of Army Campaign of Learning exercises, wargames, experiments, studies, and field force observations, the Combined Arms Center identified a series of capability gaps in the Army's ability to fight and win in large-scale ground combat operations. Despite numerous competing and profound deficits, all warfighting functions and senior leaders unanimously agreed that the number one Army gap is a lack of ISR. More specifically, the Army has limited organic deep sensing capability at the corps and division levels. It also lacks the commensurate processing, exploitation, and dissemination (PED) capacity to exploit such collection in continuous support of target development and warnings



The Army conducts a network demonstration at Fort Bliss, TX. The Army is pursuing network modernization through cross-functional teams.

U.S. Army photo by Amy Walker, FEO CJT

intelligence in competition, and targeting and combat assessments in conflict. The primary gap in the close area at the BCT level is sensing in the electromagnetic spectrum, hence the requirement for integrated SIGINT, EW, and cyberspace formations.

Cross-Domain Initiatives to Meet the Challenges of Multi-Domain Operations

The critical gap in ISR, combined with the operational problem, has the potential to create exponential impacts across the force, given the scale, volume, and speed of

combat operations with multiple corps formations. The Army MI Corps is actively working on solutions to these challenges in partnership with enterprise stakeholders such as the Army Staff, Army Futures Command, Training and Doctrine Command Centers of Excellence, cross-functional teams (CFTs), and other proponents. Cross-domain initiatives include reorganizing the MI force structure and providing modern equipment for the space, aerial, terrestrial, and foundational layers.

Cross-Functional Teams

"The U.S. Army's modernization strategy has one focus: make Soldiers and units more lethal to win the nation's wars, and come home safely. The modernization process will leverage commercial innovations, cutting-edge science and technology, prototyping and warfighter feedback.

The Army published its modernization strategy and priorities on Oct. 3, 2017. Eight Cross-Functional Teams were created to address the six modernization priorities, with two of the priorities, *Army Network* and *Soldier Lethality*, being further divided into focus areas:¹

- ◆ Long-Range Precision Fires
- ◆ Next Generation Combat Vehicle
- ◆ Future Vertical Lift
- ◆ Army Network
 - ◆ Network Command, Control, Communications, and Intelligence
 - ◆ Assured Position Navigation, and Timing
- ◆ Air and Missile Defense
- ◆ Soldier Lethality
 - ◆ Soldier Lethality
 - ◆ Synthetic Training Environment

"The Army Directive 2017-33 published on Nov. 7, 2017, established the Army Futures Command Task Force, to explore all options to establish unity of command and unity of effort that consolidates the Army's modernization process under one roof."¹

Modernizing Military Intelligence Force Structure

Current MI formations are optimized to support a BCT-centric approach to counterinsurgency and stability operations. To achieve this, the Army accepted risk in intelligence at EAB. Specifically, corps and divisions were bill payers for capabilities and capacity in BCTs. The corps retained an MI formation (the current E-MIB) focused on counterinsurgency and downward reinforcement to the BCT. This left division without an organic MI formation.

Army MI is addressing these problems through a force structure strategy that mitigates the shortfalls at EAB. At the Army Service component command, an increase in the analytic and collection capacity of the MI brigade-theater provides dedicated theater-level intelligence sup-

port to the competition phase and during transition to armed conflict. The addition of an MI formation in the Intelligence, Information, Cyber, Electronic Warfare and Space (I2CEWS) detachment at the Multi-Domain Task Force creates an additional capacity to service theater-level targeting requirements in the conflict phase.

Current concepts call for the reorganization and repurposing of the E-MIB to better meet both corps and division operational requirements in multi-domain operations. The expeditionary MI battalions within today's E-MIBs are collection battalions focused on counterinsurgency: counterintelligence and human intelligence source operations, pattern of life-based targeting, and exploitation. The future E-MIB will feature integrated intelligence and electronic warfare formations. These units will conduct analysis and PED in support of corps and division G-2s at the main command post. They will support cross-domain targeting and ISR asset management in support of corps and division fires and effects. Integrated SIGINT and EW formations at corps and division will prove the capability to compete in the electromagnetic spectrum. The corps retains counterintelligence, human intelligence, and interrogation capabilities to deal with enemy prisoners of war in large-scale ground combat operations. However, theater, corps, and division must rely on the reserve component for surge counterintelligence and human intelligence capacity.

Not only must we reorganize and repurpose the E-MIBs, we must also equip them to support large-scale ground combat operations. A significant element of modernizing Army intelligence includes equipping solutions that can detect, identify, locate, and track the threat while surviving in a highly lethal environment. This includes deep sensing; integrated SIGINT, EW, and cyberspace capabilities; and foundational intelligence capabilities that feed both mission command and fires.

Tactical Intelligence Targeting Access Node

One of those equipment modernization efforts is the TITAN ground station. This "catcher's mitt" will provide a scalable and modular means for commanders to leverage future aerial and space ISR data feeds. TITAN will take advantage of the proliferation of commercial electro-optical and infrared satellite imagery, improvements in the national-level overhead architecture, and advancements in low Earth orbit and high-altitude technologies. TITAN will eventually replace three different ground stations currently in service: the Tactical Ground Station, the Operational Ground Station, and the Advanced Miniaturized Data Acquisition System Dissemination Vehicle. The Remote Ground Terminal, a system that leverages commercial imagery, will also help

inform future TITAN requirements. The MI community is working closely with the Assured Positioning, Navigation, and Timing CFT and the Army and joint space communities to develop this capability collaboratively.

Terrestrial Layer System

In 2017, USAICoE and USACCoE began addressing the challenges our peer adversaries pose for the Army in the electromagnetic spectrum. Since then, this collaborative effort has grown to include wider Army stakeholders, operating very much like a CFT, such as—

- ◆ Department of the Army (DA) G-2.
- ◆ DA G-3 Cyber.
- ◆ DA G-8.
- ◆ U.S. Army Intelligence and Security Command.
- ◆ U.S. Army Cyber Command.
- ◆ U.S. Army Forces Command.
- ◆ Program Executive Office for Intelligence, Electronic Warfare, and Sensors.
- ◆ Communications-Electronics Research, Development, and Engineering Center.

An essential part of working toward a solution was Chief of Staff of the Army GEN Mark Milley's direction to integrate SIGINT gathering, EW, and cyberspace operations capabilities. While the team first focused on terrestrial capabilities at the BCT, it is now—in coordination with the ISR task force—considering aerial and terrestrial capabilities at all echelons in support of multi-domain operations. Led by USAICoE and USACCoE and advised by DA G-3 and DA G-2, the team has made great strides during the past 2 years in this integration effort across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy, but especially in its organization, materiel, and training aspects.

Beginning in mid-2018, the team began a campaign plan known as the TLS demonstration, experimentation, and prototyping. Defined by a DA execute order, the plan outlines three lines of effort (organization, materiel, and training) and identifies several already planned key events the team can exploit to inform capability requirements. The events were carefully selected to provide opportunities to observe and assess the latest integrated SIGINT, EW, and cyberspace operations organizational structures and the most state-of-the-art SIGINT and EW equipment operating in a field training environment. Some of the more prominent events are the Joint Warfighting Assessment at Joint Base Lewis-McChord (JBLM), Washington, in April 2019; the Joint Operational Integration Assessment in coordination with the U.S. Marine Corps at Camp Lejeune, North Carolina, in June 2019; and the National Training Center Rotation 19-10 in September 2019. During these events, Soldiers help refine the MI and EW concept of operations, tactics, techniques, and procedures; help define the organizational structure; and outline the materiel requirements. Strong SIGINT, EW, and cyberspace operations teams from the 1st Cavalry Division have already demonstrated the value of this type of observer/user interaction at the National Training Center where they showed how tipping and cueing between SIGINT and EW teams is essential to successful operations against a peer threat. The next unit we'll observe is the 2nd Stryker Brigade at JBLM. This is the SIGINT, EW, and cyberspace operations pilot unit. Its Soldiers are organized in accordance with the latest force design updates and are already training on TLS pre-prototypes.

While the Soldiers operate as integrated SIGINT, EW, cyberspace operations elements at JBLM, Camp Lejeune, and the National Training Center, the CFT-like team will work alongside them verifying networks, staff processes and interactions, lines of communication, maintenance require-

ments² and more. All of this is to ensure we truly provide the Army a working organization. In addition to looking at platoons in the BCT, the team will look at I2CEWS detachments and their approach to operations. Part of understanding the SIGINT and EW interactions is understanding the support underpinning their operations. This support comes from the cryptologic support team and the cyberspace and



Soldiers from the 2nd Cavalry Regiment tested several electronic warfare prototypes, including the Counter-Unmanned Aircraft System Mobile Integrated Capability, a mounted system that combines electronic warfare, radar, and optic capabilities to detect, identify, and defeat unmanned aerial threats.

electromagnetic activities section, which must be examined for critical gaps as well. These essential staff elements collaboratively ensure a solid targeting process for lethal and non-lethal fires and provide critical information to the BCT commander for the rapid decision making required in multi-domain operations.

The initial focus of materiel capability development is also the BCT. However, the team is exploring the state of industry's ability to provide the long-range sensing in support of deep precision fires required at higher echelons (division, corps, and I2CEWS detachments). The CFT-like team is already equipping Soldiers today with pre-prototypes of the future TLS until it comes online as a program of record in fiscal year 2022. Their feedback will be key to developing follow-on prototypes and the TLS program of record as well as informing future materiel solutions for the Eighth U.S. Army Operational Needs Statement.

Throughout the events of the summer and fall, our observers will be looking at the organizations and equipment while keeping an eye on the training necessary to achieve success in multi-domain operations. After identifying the training requirements, the team will coordinate with the various centers' schools and determine the appropriate location for each requirement—institutional, unit, etc. This task is particularly complicated because it requires the proper nesting of training across multiple centers and schools. However, at the end state, the Army will have Soldiers and organizations trained to win multi-domain operations.

The bottom line is that the team's ongoing CFT-like activities, led by USAICoE and USACCoE, and in particular the TLS demonstration, experimentation, and prototyping effort, will validate planned SIGINT, EW, and cyberspace operations organizations at BCT, ensure the Army is building the right equipment, and confirm appropriate training is in place for the force. This is a learning effort, and Soldiers will directly inform the requirements and acquisition communities to ensure the right solutions are in place. Finally, this year's exercises will allow the BCT commanders to identify real progress in the fight in the electromagnetic spectrum and lay the groundwork for capability development at all echelons, ensuring the Army has the necessary capacity to fight and win during multi-domain operations in 2028 and beyond.



In future combat, Army units may deploy a large unmanned aerial system that can serve as a mothership capable of unleashing swarms of autonomous aircraft for various missions.

Multi-Domain Sensing System

MDSS is the vision for the modernized Army aerial ISR layer of 2028. It is not a single aerial collection platform, but rather a family of integrated flying systems that will deliver relevant sensing through the entire depth and breadth of the multi-domain operations battlefield. This layered approach leverages a variety of sensor-platform pairings by echelon. These systems will collectively operate from tree-tops to high altitude and at low Earth orbit. MDSS will collectively provide sensing capabilities from the forward line of own troops through the operational deep fires area. The first priority for MDSS development is aerial ISR support to long-range precision fires targeting. To translate the MDSS concept into specific requirements, the community of interest is simultaneously working on five closely related components of the problem.

These five elements are platforms, sensors, integration of intelligence and electronic warfare and cyberspace, PED, and data transport. Future platforms must be survivable, expendable, or attritable (i.e., affordable but not so cheap that they are expendable) at an acceptable cost and risk. These may include platforms that fly higher than current aerial ISR systems, such as high-altitude balloons and nanosatellites, or lower, such as swarms and loitering munitions. They may include future unmanned aircraft systems such as those that the Future Vertical Lift CFT is developing. The sensors carried on these platforms must employ relevant technology that can rapidly and accurately detect modern signals, emissions, and signatures. MDSS sensors will incorporate onboard artificial intelligence and machine learning

to speed processing, autonomously cross-cue other sensors, and produce low-bandwidth data streams for ease of use on constrained networks.

Nanosatellites (and Swarms)

"The term "nanosatellite" or "nanosat" is applied to an artificial satellite with a wet mass between 1 and 10 kg (2.2 and 22.0 lb). Designs and proposed designs of these types may be launched individually, or they may have multiple nanosatellites working together or in formation, in which case, sometimes the term "satellite swarm" or "fractionated spacecraft" may be applied. Some designs require a larger "mother" satellite for communication with ground controllers or for launching and docking with nanosatellites. Over 1100 nanosatellites have been launched as of January 2019."³

Loitering Munitions

"A loitering munition (also known as a suicide drone or kamikaze drone) is a weapon system category in which the munition loiters around the target area for some time, searches for targets, and attacks once a target is located. Loitering munitions enable faster reaction times against concealed or hidden targets that emerge for short periods without placing high-value platforms close to the target area, and also allow more selective targeting as the actual attack mission can be aborted."⁴

Integrated intelligence and electronic warfare and cyberspace packages will provide commanders with increased operational flexibility. These integrated aerial systems will provide options to both sense and rapidly apply non-kinetic effects. MDSS will include an aerial complement to the TLS—the ground-based SIGINT, EW, and cyberspace capability discussed earlier.

The current aerial layer PED construct relies heavily on human analysts to process immense volumes of data. In large-scale ground combat operations, the speed and intensity of operations will require much greater efficiency. MDSS envisions aerial ISR PED that leverages artificial intelligence, machine learning, and autonomous processing, both at the point of collection and at the point of analysis to reduce the burden on PED formations. This enhanced PED will deliver rapid and simultaneous situational understanding and targeting information, especially for those tactical units in contact at the forward edge.

The center of gravity for MDSS is data transport. Its communications architecture must be resilient and capable of providing relevant and timely information to the tactical edge in contested communications environments. The MI community is working closely with the Army Network CFT and the Assured Positioning, Navigation, and Timing CFT on this component. MDSS will be compatible with and mutually supportive of the future multi-domain operations network and its data standards. MDSS will rely heavily on the

TITAN ground stations and foundational DCGS-A architecture and analytics as part of this network.

As currently envisioned, MDSS comprises numerous potential future increments. These increments will capitalize on the technological advances made by the Army Network CFT, other service proponents, and industry. Because of the simultaneous requirement to both modernize and support enduring operations in the aerial layer, the MI Corps is employing an agile and adaptive strategy. This includes comprehensive management of operational risk as we transition the Army aerial ISR fleet to a multi-domain operations-capable force by 2028.

DCGS-A Capability Drops 1 and 2

DCGS-A provides the foundational layer of data storage, architecture, and analytics for Army intelligence practitioners and consumers. This foundation is modernizing to meet the demands of multi-domain operations and solve the most burdensome issues for tactical users. These issues include a lack of hardware mobility at lower tactical echelons, obsolete data storage and management, and the need for big data analytical tools. The term *capability drop* refers to the iterative approach for modernizing DCGS-A. CD1 and CD2 are the two current efforts, both focused on improving intelligence operations.

CD1 will improve battlefield mobility and ease of use for maneuver battalion S-2s. It consists of easy-to-use, commercially developed software on a ruggedized laptop computer that fits in an assault pack. A 35F (Intelligence Analyst) can operate it without any specialized support. CD1 replaces the 480-pound Intelligence Fusion Server, eliminates the need for a 35T (Military Intelligence Systems Maintainer/Integrator) to turn on the system, and automates many intelligence preparation of the battlefield and mission planning functions. The Army will field CD1 to 409 maneuver battalions in the next year.

With the increased sensors on the battlefield, the velocity and volume of data during large-scale combat operations will likely overwhelm the analyst. CD2 is the modernization effort to get ahead of this problem. CD2 focuses on identifying commercial items to upgrade or replace the current DCGS-A data architecture as well as introduce several additional analytics and system management functions. Specifically, CD2 focuses on the modernization and enhancement of the DCGS-A data fabric⁵ and analytics capabilities across multiple echelons, by providing a scalable solution with an adaptable data management architecture, automated analytics, and common core services. The end state is to improve how Army intelligence ingests, stores,

The screenshot shows a software interface for managing military equipment. On the left, there's a 'WEATHER EFFECTS' section with a legend for impact levels (No Impact, Degraded, Severely Degraded) and a grid showing these levels across various equipment categories like GROUND OPERATIONS, HALO OPERATIONS, ISR OPERATIONS, STATIC LINE OPE., and AIR ASSAULT. The grid uses colors (green, yellow, red) to represent the impact level for each category. On the right, there's a 'Properties' panel for 'VTT-323' with sections for CEILING, PRECIPITATION, MINIMUM TEMPERATURE, MAXIMUM TEMPERATURE, and VISIBILITY, each with 'Moderate' and 'Severe' settings. A large table below the weather effects shows detailed weather data for various hours from 0000-0200 to 2200-0000, including columns for Weather Product, Ceiling (m), Cloud Cover (%), Density Altitude (ft), Precipitation (mm/h), Surface Pressure (hPa), Snowfall (mm/h), Temperature (°C), Wind Direction (°), and Wind Speed (kph). The table also includes columns for HIGH, LOW, HEAT INDEX, and WIND CHILL. At the bottom right of the interface, there's a button labeled 'Forecast Applied'.

and provides information to the analyst to ensure increased speed, precision, and accuracy of intelligence during large-scale combat operations.

Conclusion

The intelligence modernization initiatives described in this article align with the strategic guidance to rapidly transform the Army into one that can fight and win against a near-peer enemy by 2028. As GEN Milley has made clear, all warfighting functions must aggressively pursue paradigm-shifting technologies and novel approaches to achieve this goal. The MI Corps remains committed to delivering world-class intelligence capabilities that enable lethality and survivability in multi-domain operations.



Endnotes

1. Office of the Chief of Public Affairs, "Army Modernization," *Stand-To*, January 16, 2018, https://www.army.mil/standto/archive_2018-01-16; and

"Army Modernization, Steps Needed to Ensure Army Futures Command Fully Applies Leading Practices," U.S. Government Accountability Office, January 2019, <https://www.gao.gov/assets/700/696537.pdf>.

2. The current force design updates address only changes required to integrate electronic warfare into existing formations. They do not account for the additional maintenance burden (specifically 35T [Military Intelligence Systems Maintainer/Integrator]) that three additional trucks will incur.
3. Wikipedia Foundation, s.v. "Small satellites," last modified 24 April 2019, 15:40, https://en.wikipedia.org/wiki/Small_satellite.
4. Wikipedia Foundation, s.v. "Loitering munition," last modified 5 March 2019, 06:15, https://en.wikipedia.org/wiki/Loitering_munition#cite_note-8.
5. "Data Fabric is an architecture and set of data services that provide consistent capabilities across a choice of endpoints spanning on-premises and multiple cloud environments." "What is Data Fabric," NetApp, accessed 25 April 2019, <https://www.netapp.com/us/info/what-is-data-fabric.aspx>.

COL William Adams, COL Mark Dotson, COL Jennifer McAfee, and COL Francesca Ziomba are respectively the U.S. Army Training and Doctrine Command Capability Managers for Foundation, Electronic Warfare, Terrestrial, and Aerial. Mr. Dwight DuQuesnay is the Director of Requirements Determination, Capability Development Integration Directorate—Intelligence, Future Concepts Center, U.S. Army Futures Command. COL Dotson is assigned to the U.S. Army Cyber Center of Excellence at Fort Gordon, GA. The remainder are assigned to the U.S. Army Intelligence Center of Excellence at Fort Huachuca, AZ.

The Army Signal Corps, first set up in 1863, posted communications troops on high ground to transmit messages by “wig-wagged” signal flags that often provided valuable field intelligence.

Enabling Battalion S-2 Sections for the Pace of Large-Scale Ground Combat Operations



DCGS-A

by TRADOC Capability Manager-Foundation and Program Manager DCGS-A Team

Introduction

The seismic shift from counterinsurgency operations to fighting a near-peer competitor in large-scale ground combat operations dictates the need to evolve and innovate to ensure the Military Intelligence Corps can provide analysis with enhanced speed, precision, and accuracy for the tactical commander. At the battalion S-2 level, this is clearly evidenced by the 480-pound server that requires a 35T (Military Intelligence System Maintainer/Integrator) to employ and will greatly reduce mobility during the speed of large-scale ground combat operations.

The Capability Drop 1 Program

A little over 2 years ago, U.S. Army Forces Command (FORSCOM) laid out their priorities necessary to outpace a near-peer threat and fix their battalion S-2 analytic challenges. FORSCOM requested an expeditionary system that could build intelligence preparation of the battlefield (IPB) and mission planning products and operate in a disconnected, intermittent, and limited (DIL) bandwidth environment. The system also needed to be simple and intuitive to use, display graphics, and provide a common intelligence and operational picture with interoperability between mission command systems.

The Military Intelligence Corps teammates at Aberdeen Proving Ground, Maryland, took on this task, Capability Drop 1 of the Distributed Common Ground System-Army. Capability Drop 1 is the first iteration in improving intelligence to meet the needs of the Mission Command Intelligence framework and preparing a tactical force to fight during large-scale ground combat operations.

This effort is the culmination of a year's worth of competition between two potential vendors, including multiple tests with Soldiers, participation in the Network Integration Evaluation (18.2), and Army Interoperability Certification testing. The Capability Drop 1 program has been a cooperative effort across the entire Army, including FORSCOM, Army Test and Evaluation Command, Communications-Electronics Command, Training and Doctrine Command, Army Futures Command, Army Special Operations Command, Department of the Army Headquarters Staff, and industry partners.

Both potential vendors delivered an initial Capability Drop 1 package to support multiple iterations of testing with intelligence Soldiers from across the Army. Soldiers provided direct feedback, enabling the vendors to determine fixes and product improvements while enabling the Army to evaluate the best solution for fielding to its tactical units. Testing focused on Soldier priorities, including intelligence planning tools, usability, interoperability, cybersecurity, and reliability. After extensive testing and Soldier involvement, a contract award was made in March 2019.

Capabilities of the System

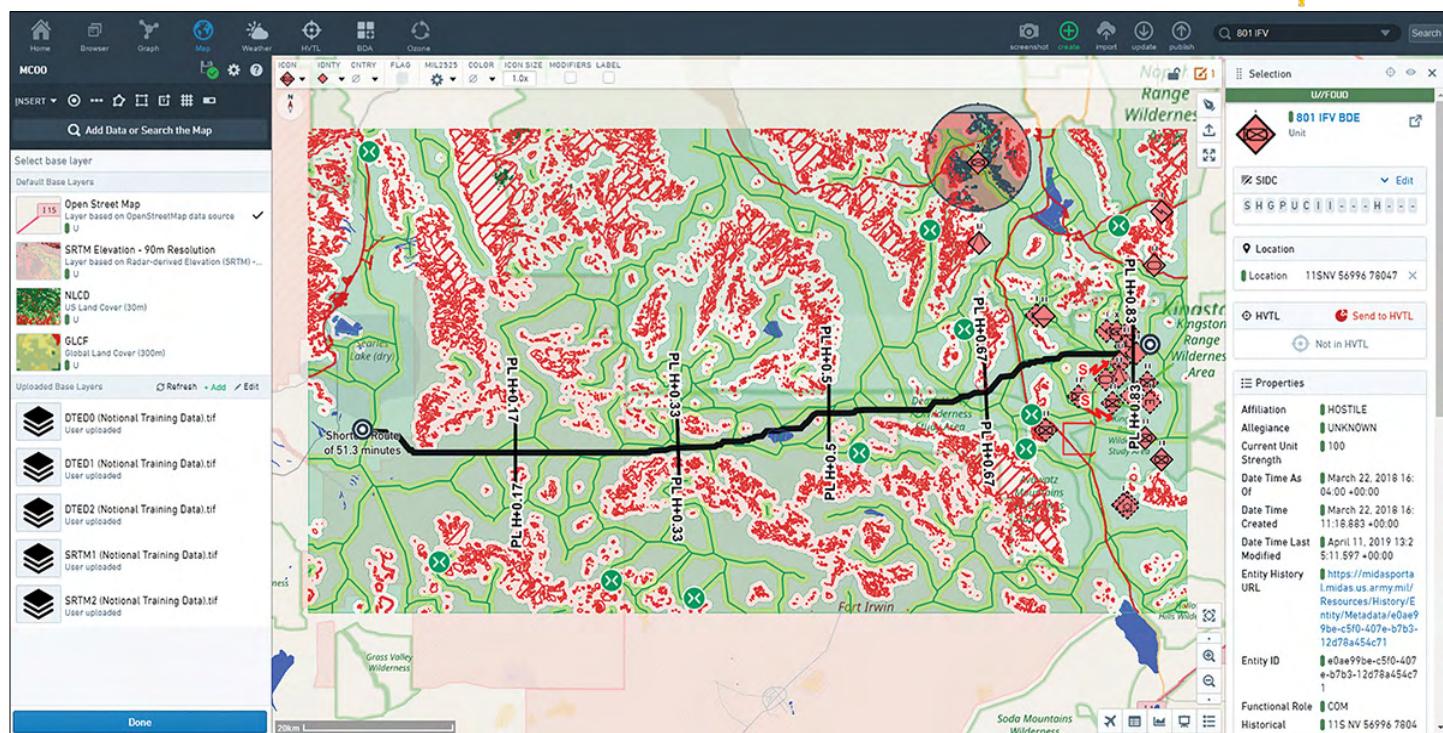
Capability Drop 1 consists of a commercial hardware and software solution to support intelligence analyst operations at the tactical echelon. Hardware solutions comprise ruggedized laptops and a displacement of the current Intelligence Fusion Server at the battalion echelon to improve expeditionary operations. Software will enable operations in a DIL bandwidth environment, enhance ease of use, and provide improved tools for IPB and processing, exploitation, and dissemination.

Capability Drop 1 enables the production of IPB and mission planning products in a DIL bandwidth environment by locally storing the digital terrain elevation data for the area of operations. This data is a uniform matrix of terrain elevation values that provides basic quantitative data for systems and applications requiring terrain elevation, slope, and/or surface roughness information. This allows the software using built-in algorithms to auto-generate IPB products. It also allows the analyst to overlay the Worldwide Equipment Guide that is contained in the software, aiding mission planning through battle tracking as well as link and nodal analysis. Analysts can use collection management applications to determine named areas of interest, build their reconnaissance and surveillance matrix, and then open a graphical display of the collection plan to determine any gaps in collection for their operation. Weather impacts to the mission readily display by equipment type and provide a forecast for the operation ahead. Once in place, the system can interface with generated reports and provide alerts to tip and queue analysts to items of interest in their area of operations. As the operation continues, another interface allows battle tracking in a very intuitive manner that links directly by system type from the Worldwide Equipment Guide.

Starting in May 2019, the U.S. Army began to field the Capability Drop 1 system to 409 maneuver battalions across the Army's Active, Reserve, and National Guard components. Initial training to battalions began in April 2019, prioritizing units based on their mission and upcoming deployments, with fielding starting in May. The training plan for FORSCOM units provides a 2-week training platform at Fort Hood, Texas, to train Soldiers as subject matter experts who will then return to train the Soldiers at battalion level. The Army plans to complete fielding and training to all battalions in less than a year.

Conclusion

This capability is designed to enhance our analysts' efficiency and effectiveness to support the tactical commander's decision making during fast-paced combat operations. Capability Drop 1 enables a pivot to next-generation intelligence capabilities to increase speed, precision, and accuracy in all functions within the intelligence cycle. Capability Drop 1 is fully aligned within the Army's overarching Mission Command Intelligence framework—to field a ready Army intelligence team supporting mission command against all threats in multi-domain operations by 2028.



Map screenshot from DCGS-A

The Program Manager DCGS-A mission is to field and sustain modernized intelligence systems through an exceptional workforce of dedicated and professional acquisition specialists and integrate best of breed solutions for the battlefield of tomorrow.

Intelligence Policy Considerations in Large-Scale Combat Operations

by Mr. Gregory Hatter, Mr. Scott Schultz,
Mr. Craig Bell, Colonel Lisa Walker,
and Colonel Bill Mangan

Introduction

The purpose of policy is to direct and assign tasks, prescribe desired capabilities, and provide guidance for ensuring the armed forces are prepared to execute operations. The *Merriam-Webster Dictionary* defines policy as “prudence of wisdom in the management of affairs.”¹

We often hear, “We need to change our policy,” but is this always a valid statement? Probably not, particularly if one considers the times we use it interchangeably with rules of engagement, authorities, roles and functions, or even doctrine. However, when considering multi-domain operations and large-scale combat operations, this statement is invaluable. It should trigger the critical thought necessary to apply “prudence of wisdom” to our intelligence policies now, so that we will be able to fight and win in the future and not be frustrated with “policies” that are not fit for purpose and are late to need.

Intelligence Policies

The problem with intelligence policy in support of multi-domain operations and large-scale combat operations should not start with a wholesale review of those “on-the-shelf” policies or the binary question of “do we have one or not?” It is more appropriate to consider the problem operationally. As an intelligence formation, we should think about our policies in terms of time, space, unity of purpose, and threat focus.

Our pacing threats operate relentlessly across a broad geographic area and in multiple domains. The Russian center of gravity in our “competition” phase is the integration of information warfare, the integration of unconventional warfare, and the application of conventional forces. During the “conflict” phase, the Russians’ center of gravity is their long- and mid-range fires. Thinking through the defeat of the Russian center of gravity by phase should trigger immediate thoughts as to policy adequacy for intelligence practitioners.

Photo by U.S. Army SPC Hubert D. Delany III



Army SGT Samuel Benton observes and mentors soldiers during the Bull Run V training exercise with Battle Group Poland in Olecko, Poland, May 22, 2018. Battle Group Poland includes United States, United Kingdom, Croatian, and Romanian soldiers who support NATO's enhanced forward presence.

Description of Terms

- **Ambiguous/unambiguous warning:** Decision makers and their staffs are likely to *ignore warning signs that remain highly ambiguous* as to what might be at stake. Warnings that are sufficiently ambiguous to allow for plausible alternative interpretations that minimize the alleged danger are *much less likely than unambiguous warnings to be put on the decision makers' agenda.*²
- **Consolidated Intelligence Guidance:** This guidance describes joint program planning between the National Intelligence Program and the Military Intelligence Program.³
- **Frozen conflict:** In international relations, a frozen conflict is a situation in which active armed conflict has been brought to an end, but no peace treaty or other political framework resolves the conflict to the satisfaction of the combatants. Therefore, legally the conflict can start again at any moment, creating an environment of insecurity and instability.⁴
- **Interior lines:** Use of interior lines is a strategy of warfare based on the fact that lines of movement and communication within an enclosed area are shorter than those on the outside. As the area held by a defensive force shrinks, the advantages increase. Using the strategy of interior lines, a partially surrounded or more centrally disposed force can more easily resupply and redeploy its units, and thus more easily mount a series of quick attacks at multiple locations.⁵
- **Late to need:** This is an action or a process that is slow, cumbersome, or unsuitable. For example, policies that are late to need may result in Soldiers arriving too late or units requiring too much time to close the equipping, manning, and training gaps.⁶
- **National Disclosure Policy-1:** The full title of the National Disclosure Policy-1 is *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*. The National Disclosure Policy Committee is the central authority for the formulation, promulgation, administration, and monitoring of NDP-1.⁷
- **Pacing threat:** Russia is the United States' current pacing threat, and China is projected to overtake Russia as the primary threat as early as 2035.⁸

The layered standoff problems of multi-domain operations center on the joint force's ability to compete so as to defeat an adversary's operations to destabilize; deter the escalation of violence; and if there is an escalation, enable a rapid transition to armed conflict. During this rapid transition, the joint force must be able to—

- ◆ penetrate antiaccess and area denial technology,
- ◆ dis-integrate antiaccess and area denial to enable friendly maneuver,
- ◆ exploit the resulting freedom of maneuver, and
- ◆ recompete to consolidate gains.

This problem set has a host of specified and implied intelligence tasks—notably, the task to ensure our intelligence policies enable our units to compete and then transition rapidly to conflict. Failure to have adequate policies in place increases the risk of being late to need. Undoubtedly, some may say, “If the fighting starts, we will be able to make the changes necessary.” This is clearly an assumption, but is this assumption valid? Given that our pacing threats are operating on interior lines, it is challenging for us to maintain the initiative on decision making when initiating conflict; to determine an acceptable end state or frozen conflict; and to enable commanders to make decisions using ambiguous rather than unambiguous warning information. Therefore, this assumption may not be valid at all.

As a formation, we should ask ourselves, what intelligence policies should we keep, get rid of, or modify? This question requires closer examination. Do these policies enable U.S. forces to keep pace in the transition between competition and conflict? Are they adequate at echelon? For those at home station and training or in exercises, rather than geographically engaged in the competition phase, are the policies adequate to allow their rapid transition into conflict?

These questions apply at echelon and across all intelligence disciplines. When asked, some common areas immediately come to mind regardless of the audience. A quick discussion of each helps to energize the thought process. These areas are—

- ◆ foreign disclosure,
- ◆ counterintelligence (CI) and human intelligence (HUMINT) operations, and
- ◆ signals intelligence (SIGINT) Soldiers and contract linguists operating in SIGINT facilities.

Foreign Disclosure

A recurring thread in our national strategy documents is the recognition that competition with near-peer threats will require us to work more closely with our allies and partners. We need to be able to share intelligence and operational information with a wide array of countries—a challenge many units already face today in myriad worldwide operations, engagements, and exercises. Foreign disclosure refers to what information a partner nation or international organization can know, in accordance with the National Disclosure Policy (NDP-1). NDP-1 establishes disclosure authorities by country, classification level, and category or type of information. Instances will always exist in which not all the same information may be disclosed to all partner nations; “writing for release” becomes paramount and must be considered as a primary planning requirement. Foreign disclosure

officers are responsible for advising units on the implementation of NDP-1 and must be involved early in the planning stage.

Several units have already included foreign disclosure guidelines in orders. The next update to FM 6-0, *Commander and Staff Organization and Operations*, should formalize this process, with an appendix dedicated to foreign disclosure and a template for a foreign disclosure annex to plans and orders. The intent of the disclosure annex is to change our mind-set and incorporate foreign disclosure throughout the planning process instead of after the fact. Many of us have experience with operation orders

written at the level of Not Releasable to Foreign Nationals (NOFORN), limiting our ability to share key operational information with allies. We need to work with personnel across the staff to ensure foreign disclosure does not have the appearance of being “just” an intelligence or security function, but rather a combat multiplier.

Outside the rule set of NDP-1, an additional challenge we often face in multinational operations is the need to share national intelligence information. This often requires detailed and sometimes lengthy coordination with the national agencies who own the information. To this end, we have proposed additional verbiage for the Director of National Intelligence’s *Consolidated Intelligence Guidance* to help emphasize the need and ways to share with our multinational partners.

NDP-1 is rules-based but includes the ability to request exceptions. The proper application of the provisions of NDP-1 facilitates the timely disclosure of classified military information to allied and partner nations. The question to consider is whether foreign disclosure policies are in place, understood, and trained at all echelons to keep pace in the transition between competition and conflict. On the surface, NDP-1 is enabling and has driven change to doctrine as well as inputs to the latest version of the *Consolidated Intelligence Guidance*, but is this enough?

Counterintelligence and Human Intelligence Operations

The challenges of working in a partnered environment carry over to discussions of CI and HUMINT in future large-scale combat operations against a near-peer threat. While the mantra of “write to release” needs to continue to be part of our training for collectors, we also need to review the policies driving the classification of our tradecraft to better facilitate partnering during the collection process, whether in CI or HUMINT operations, including intelligence interrogations.

Perhaps the biggest constraint we need to relook for CI and HUMINT are the au-

thorities that allow units and personnel to conduct CI or HUMINT operations. Some CI and HUMINT forces require the authority to conduct operations outside a theater of conflict. Successful source development requires identifying potential sources in advance of need and may involve operations in an area that has not yet transitioned into conflict. Army G-2 is looking at ways to expand CI and HUMINT collection authorities. It is encouraging increased coordination between U.S. Army Forces Command, Army Reserve, and Army National Guard Forces with organizations possessing operational authorities, such as Army Service component commands and U.S. Army Intelligence and Security Command, to maximize the use of our limited forces. This

proposed increase in utilization, combined with a more sophisticated adversary, also highlights the need for more forces to receive intermediate and advanced training and certification, to include operating

“ ‘Writing for release’ becomes paramount and must be considered as a primary planning requirement.”

“ Are we being rigorous enough to ensure our CI and HUMINT policies are adequate to achieve the end state we desire?”

in the cyberspace environment. This also requires better training of our leaders so that they understand the processes and discipline-specific authorities associated with expanded use of our CI and HUMINT personnel. While this process will take an initial investment of time and resources, it will allow us to better posture our forces to collect intelligence effectively and to protect our formations throughout the competition and conflict phases.

A number of questions persist and operational formations can best inform the necessary adjustment to policy. This may be about operating in the competition phase alongside multinational partners or regarding units conducting home station training rather than being geographically engaged in the competition phase. Simply put, are we being rigorous enough to ensure our CI and HUMINT policies are adequate to achieve the end state we desire?

SIGINT Soldiers and Contract Linguists Operating in SIGINT facilities

An everyday issue that confronts the SIGINT community centers on the reciprocity security screening process that causes a significant number of Soldiers and contract linguists to wait for access to the National Security Agency's (NSA) systems and facilities. Many of the Soldiers and contract linguists under security/background investigation by NSA's Military Affairs Division (MAD) are the best linguists available but are unable to support the mission until NSA completes their investigation. Most of the Soldiers will undergo their MAD assessment within a few weeks and be able to enter NSA facilities and access the NSA systems. However, Soldiers with significant foreign national affiliations receive a more extensive MAD assessment, which can take months longer to complete. Requiring Soldiers to await facility or systems access significantly degrades our ability to support the mission and/or train on the systems needed to support large-scale combat operations and multi-domain operations during the competition phase.

This policy challenge confronts us daily in the competition phase. The Office of the Chief of Military Intelligence is addressing this issue of MAD reciprocity process by changing DA PAM 611-21, *Military Occupational Classification and Structure*, to modify the qualifications to hold a SIGINT military occupational specialty. This policy change will reduce the number of Soldiers waiting long periods for access to facilities and systems and reduce the MAD backlog of Soldiers awaiting MAD assessments.

MAD processing has a more significant impact on the contract linguist population. Almost all the contract linguists have foreign national affiliation issues, and the MAD often requires them to undergo an extensive CI assessment that can take more than a year. This lengthy MAD assessment process can affect the ability to use contract linguists to support surge operations as well as the number of contract linguists available to support operations during the competition phase. This issue negates the use of contract linguists to provide a surge capability until we can either recruit or train more Soldiers to fill gaps in our formations and exac-

erbates our challenge of rapidly transitioning from competition to conflict. Army G-2 is working with the MAD and the NSA CI assessment team to identify efficiencies to accelerate the MAD process for contract linguists and reduce the length of time these linguists spend awaiting a favorable MAD assessment.

In the SIGINT realm, the focus has been on adapting to the policies in place rather than changing the policies themselves. This may be adequate, but is it sufficiently adequate to keep pace in the transition between competition and conflict? It is too early to tell if the policy changes we are making will reduce the number of Soldiers and contract linguists who are awaiting facility or systems access. Even if the policy changes we are making are effective, we need to consider the impact of not using our best (military and contract) linguists to support operations during the competition and the conflict phases. This is a policy issue we need to address now in order to have sufficient linguist capacity available for training and to support critical missions during the competition phase.

Conclusion

The emerging multi-domain operational environment reflects adversaries that are expanding their efforts to reduce friendly force decision-making time, operating across domains and at echelon, and engaging geographically where our allies and partners live. The lines are becoming blurrier between "below armed conflict" and conflict. The complexity and criticality of the competition phase is arguably on par with the conflict phase. Whether one is looking for changes to authorities, rules of engagement, roles and functions, or even doctrine, policy considerations are either foundational or a critical driver. A rigorous interrogation of our current policy stance across all intelligence disciplines and the prudence of wisdom in making and applying changes are as important as the material solutions with which we desire to fight and win. Intelligence policy considerations in multi-domain operations and large-scale combat operations should not be a top-down effort. The real impetus for change will come from intelligence Soldiers and their leaders—those who need us to adjust our stance so that they can compete and operate in conflict, denying our adversaries any advantage.



Endnotes

1. Merriam-Webster, s.v. "policy (n)," accessed 15 April 2019, <https://www.merriam-webster.com/dictionary/policy>.
2. Irving L. Janis, *Crucial Decisions: Leadership in Policymaking and Crisis Management* (New York: The Free Press, 1989), 235-236.

3. Janet A. McDonnell, "The Office of the Under Secretary of Defense for Intelligence: The First 10 Years," *Studies in Intelligence* 58, no.1 (March 2014): 13.
4. "Frozen Conflict," Wikipedia Foundation, last modified 12 April 2019, 07:20, https://en.wikipedia.org/wiki/Frozen_conflict.
5. "Interior lines," Wikipedia Foundation, last modified 2 November 2018, 08:49, https://en.wikipedia.org/wiki/Interior_lines.
6. Jared Serbu, "Military readiness problems can't be fixed overnight, Defense chiefs warn," *Federal News Network*, February 8, 2017, federalnewsnetwork.com/defense/2017/02/military-readiness-problems-can-t-fixed-overnight-defense-chiefs-warn/.
7. Chairman of the Joint Chiefs of Staff Manual 5230.01A, *Joint Staff Foreign Disclosure and Foreign Visits Programs*, 21 December 2017, A-2.
8. Ray Finch, "The Tenth Man—Russia's Era Military Innovation Technopark," *Mad Scientist Laboratory* (blog), August 20, 2018, <https://madsciblog.tradoc.army.mil/tag/pacing-threat/>.

Mr. Gregory Hatter is the Headquarters, Department of the Army (HQDA) G-2's Foreign Disclosure Policy Officer. He has been in his current position since 2001.

Mr. Scott Schultz is the HQDA G-2's Chief of Foreign Disclosure.

Mr. Craig Bell, a retired Army military intelligence officer, is the HQDA G-2's Foreign Language Team Chief.

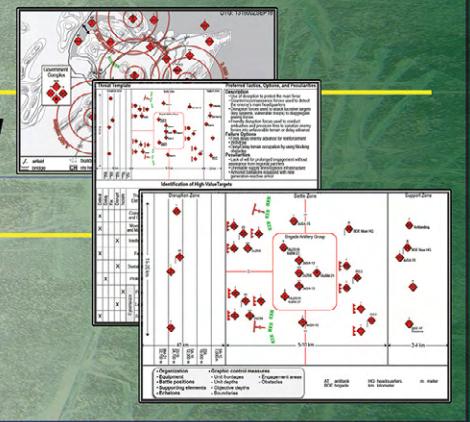
COL Lisa Walker, an Army military intelligence officer, serves as the HQDA G-2's Military Deputy to the Army G-2X.

COL Bill Mangan, an Army military intelligence officer, is the HQDA G-2's Deputy for Plans and Integration.

The image shows two screenshots of the MI Professional Bulletin website. The top screenshot displays the homepage with a banner for the 'Current Issue - Multinational Operations and Other Intelligence Challenges'. It features several news articles and a sidebar with contact information for the Foreign Disclosure Policy Officer. To the right, a large box highlights the website update with the text: 'MI Professional Bulletin Has an updated website! The current issue of MIPB is still available on the front page of our website at <https://www.ikn.army.mil/apps/MIPBW>.'. The bottom screenshot shows the 'Archive' tab, displaying a grid of thumbnail images for every issue of the bulletin from 1974 to the present. To the right of this grid, another box states: 'Now To access all of our issues back to 1974, click the archive tab. A CAC is no longer required.'

Aligning Intelligence Preparation of the Battlefield Doctrine with the Current Threat

by Ms. Terri M. Lobdell



ATP 2-01.3, *Intelligence Preparation of the Battlefield*, was officially authenticated and published on 1 March 2019. This article describes changes made through this latest revision of the publication. Intelligence preparation of the battlefield (IPB) is one of the most important processes and is critical to tactical operations. Because of this, MG Robert Walters, Jr., U.S. Army Intelligence Center of Excellence Commanding General, has directed that the October-December 2019 issue of *Military Intelligence Professional Bulletin* will focus on all aspects of the IPB process.

IPB serves as the primary framework for analysis of the battlefield during the military decision-making process (MDMP). IPB is a collaborative staff effort led by the J-2/G-2/S-2 and the intelligence staff. The entire staff participates in IPB to develop and sustain an understanding of the enemy, terrain and weather, and civil considerations. IPB helps identify options available to friendly and threat forces.¹ The IPB process is a critical staff function, as it impacts the range of military operations, is relevant across all echelons, and is a fundamental element within all planning.

This version of the IPB publication retains time-tested doctrine constructs and provides updates to align with current Army doctrine. ATP 2-01.3 preserves the steps and sub-steps of the IPB process and highlights the staff processes and products used to assist commanders and staffs in identifying when and where to leverage friendly capabilities during operations. Further, we aligned this version with the updated doctrinal constructs found within the context of ADP, ADRP, and FM 3-0 (*Operations*) as well as ADP and FM 2-0 (*Intelligence*).² We focused on conducting IPB during large-scale combat operations, multi-domain operations, and operations against a peer threat. We discussed the complex operational environment in which U.S. forces will operate across all domains (air, land, space, maritime, and cyberspace), the information environment, and the electromagnetic spectrum.

What Remained the Same—Sound Doctrine Steps

Step 1—Define the Operational Environment. The intelligence staff identifies “those significant characteristics related to the mission variables of enemy, terrain and weather, and civil considerations that are relevant to the mission. The intelligence staff evaluates significant characteristics to identify gaps and initiate information collection.” During step 1, the area of operations, area of interest, and area of influence must also be identified and established.³

Step 2—Describe Environmental Effects on Operations. “The intelligence staff describes how significant characteristics affect friendly operations. The intelligence staff also describes how terrain, weather, civil considerations, and friendly forces affect threat forces...The entire staff determines the effects of friendly and threat force actions on the population.”⁴

Step 3—Evaluate the Threat. “The purpose of evaluating the threat is to understand how a threat can affect friendly operations.” Step 3 determines threat force capabilities and the doctrinal principles and tactics, techniques, and procedures threat forces prefer to employ.⁵

Step 4—Determine Threat Courses of Action. “The intelligence staff identifies and develops possible threat [courses of action] COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat COAs to assist in developing and selecting friendly COAs during COA steps of the MDMP. Identifying and developing all valid threat COAs minimize the potential of surprise to the commander by an unanticipated threat action.”⁶

Staff Collaboration

IPB begins in planning and continues throughout the operations process. IPB products are developed to assist the commander in determining where and when to leverage

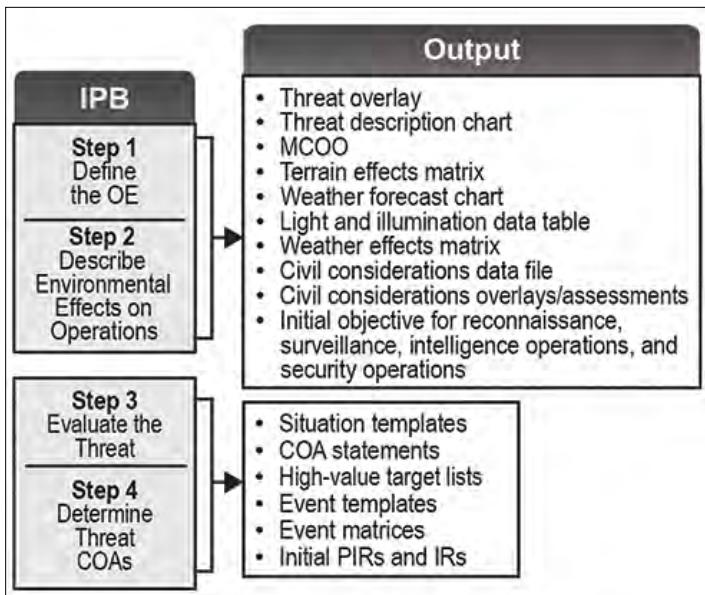


Figure 1. IPB Product Outputs⁷

friendly capabilities. Figure 1 shows the IPB product outputs that result from the MDMP.

What is New or Significantly Revised

In order to align with the current doctrinal constructs found in ADP, ADRP, and FM 3-0 and ADP and FM 2-0, this version highlights:

- ◆ **Army strategic roles.** “Operations to shape, prevent, conduct large-scale ground combat, and consolidate gains summarize the Army’s strategic roles as part of a joint force.” During shape and prevent, the IPB focus is on support for operational planning and training for large-scale combat operations. When operations shift to large-scale ground combat, time often becomes a factor. “Each echelon must effectively perform IPB to quickly generate those products that drive the rest of the military decision-making process.” Consolidation of gains is a continuous part of large-scale ground combat. However, “the IPB focus shifts to address not only the threat but also stability tasks, the local environment, and the information environment.”⁸
- ◆ **Multi-domain operations.** “The interrelationship of the air, land, maritime, space and cyberspace domains, the information environment (which includes cyberspace), and the [electromagnetic spectrum] EMS requires multi-domain situational understanding of the [operational environment] OE.”⁹ “A thorough IPB effort and intelligence analysis assists each echelon in focusing operations on all significant aspects of the OE in time and space across multiple domains.”¹⁰
- ◆ **Peer threats.** Discusses peer threats as adversaries or enemies with capabilities and capacity to oppose U.S.

forces. It provides enhanced understanding of the regular, irregular, and hybrid threats.

- ◆ **Operations and environments.** Included is an in-depth discussion (Part 3) on IPB for unified action and unique environments as well as additional considerations for multi-domain operations.
- ◆ **Scenarios.** Tailored scenarios and vignettes appear throughout the publication developed to facilitate better comprehension.
- ◆ **IPB tools appendix.** Restored an appendix on terrain, movement, and weapon data tables from the rescinded 1994 version of FM 34-130, *Intelligence Preparation of the Battlefield*.
- ◆ **Cyberspace.** Added a new appendix on IPB cyberspace considerations. While the steps of IPB remain unchanged, the considerations for cyberspace require a different perspective. As an essential part of the information environment, there is a massive global dependence on the cyberspace domain for information exchange. With this dependence and the associated inherent vulnerabilities, the cyberspace domain must be considered during each step of the IPB process:

- ◆ **“Step 1—Define the OE:** Visualize cyberspace components and threats through the three layers of cyberspace.
- ◆ **Step 2—Describe environmental effects on operations:** Use military aspects of terrain.
- ◆ **Step 3—Evaluate the threat:** Evaluate threats and [high-value targets] HVTs in cyberspace...
- ◆ **Step 4—Determine threat COAs:** Consider the threat’s historical use of cyberspace and incorporate threat COAs, determine HVT lists within the cyberspace domain, [and] assist the S-6 staff to identify friendly networks that require protection.”¹¹

Figure 2 (on the next page) is an example IPB product available within this appendix.

How to Access the Publication

Army Publishing Directorate website:

https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1006342.

Intelligence Knowledge Network:

https://ikn.army.mil/apps/IKNWMS/Home/WebSite/MILITARY_DOCTRINE_CAC2 (common access card login required).

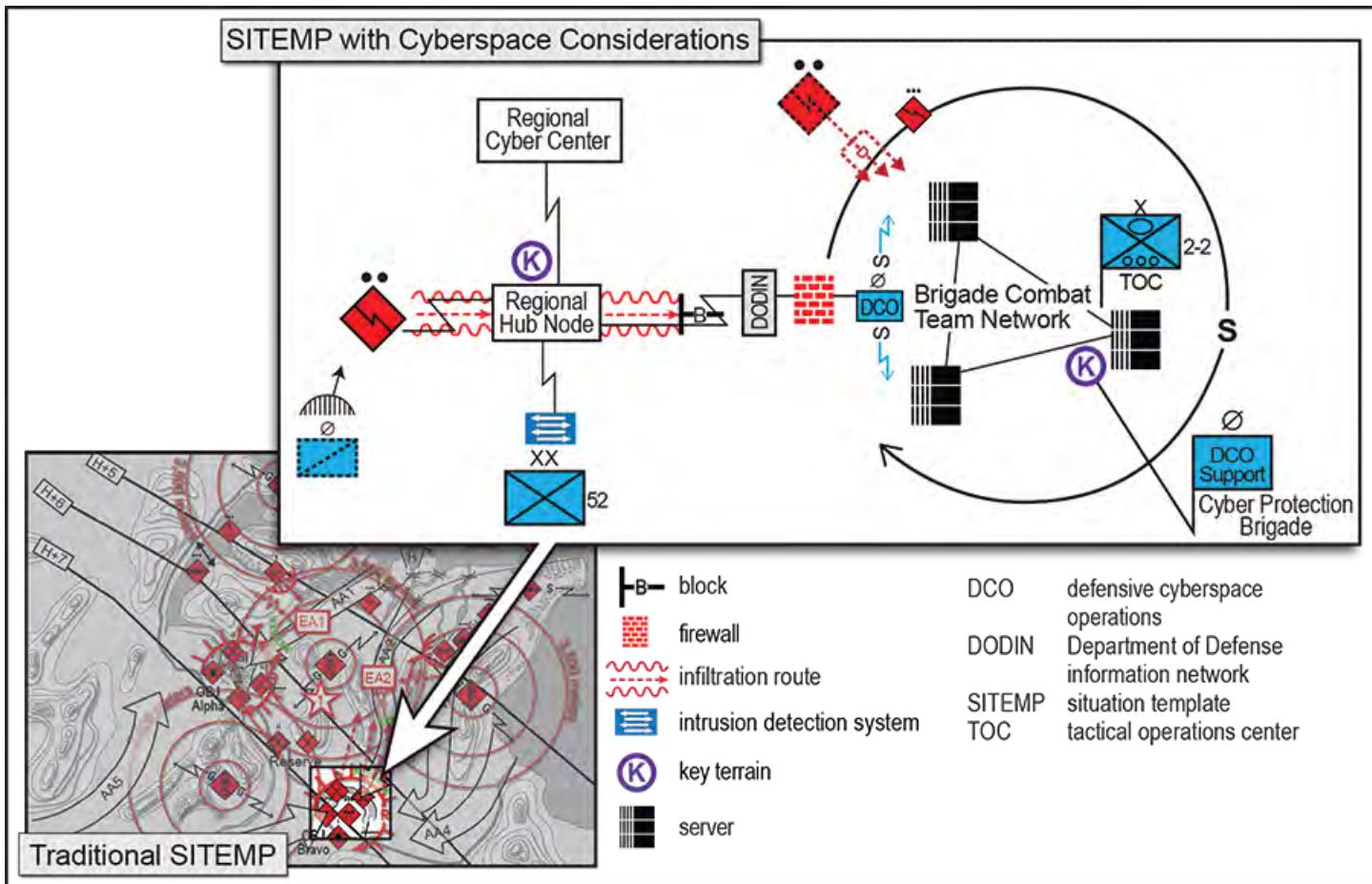


Figure 2. Threat Situation Template with Cyberspace Considerations¹²

Endnotes

1. Department of the Army, Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. Government Publishing Office [GPO], 17 May 2012).

2. Recent articles that discuss doctrinal revisions are “The Return of U.S. Army Field Manual 3-0, Operations,” *Military Intelligence Professional Bulletin* 44, no. 2 (April-June 2018): 5-11; “Doctrine Corner: Multi-Domain Operations,” *Military Intelligence Professional Bulletin* 44, no. 3 (July-September 2018): 100-101; Terri M. Lobdell, “Resetting Intelligence Doctrine,” *Military Intelligence Professional Bulletin* 44, no. 4 (October-December 2018): 9-19; and Terri M. Lobdell, “ADP 2-0 Update,” *Military Intelligence Professional Bulletin* 45, no. 1 (January-March 2019): 7-8.

3. Department of the Army, Army Techniques Publication 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. GPO, 1 March 2019), 1-3.

4. Ibid., 1-4.

5. Ibid.

6. Ibid.

7. Ibid., 2-2.

8. Ibid., 1-15-1-16.

9. Ibid., 1-12.

10. Ibid., 1-14.

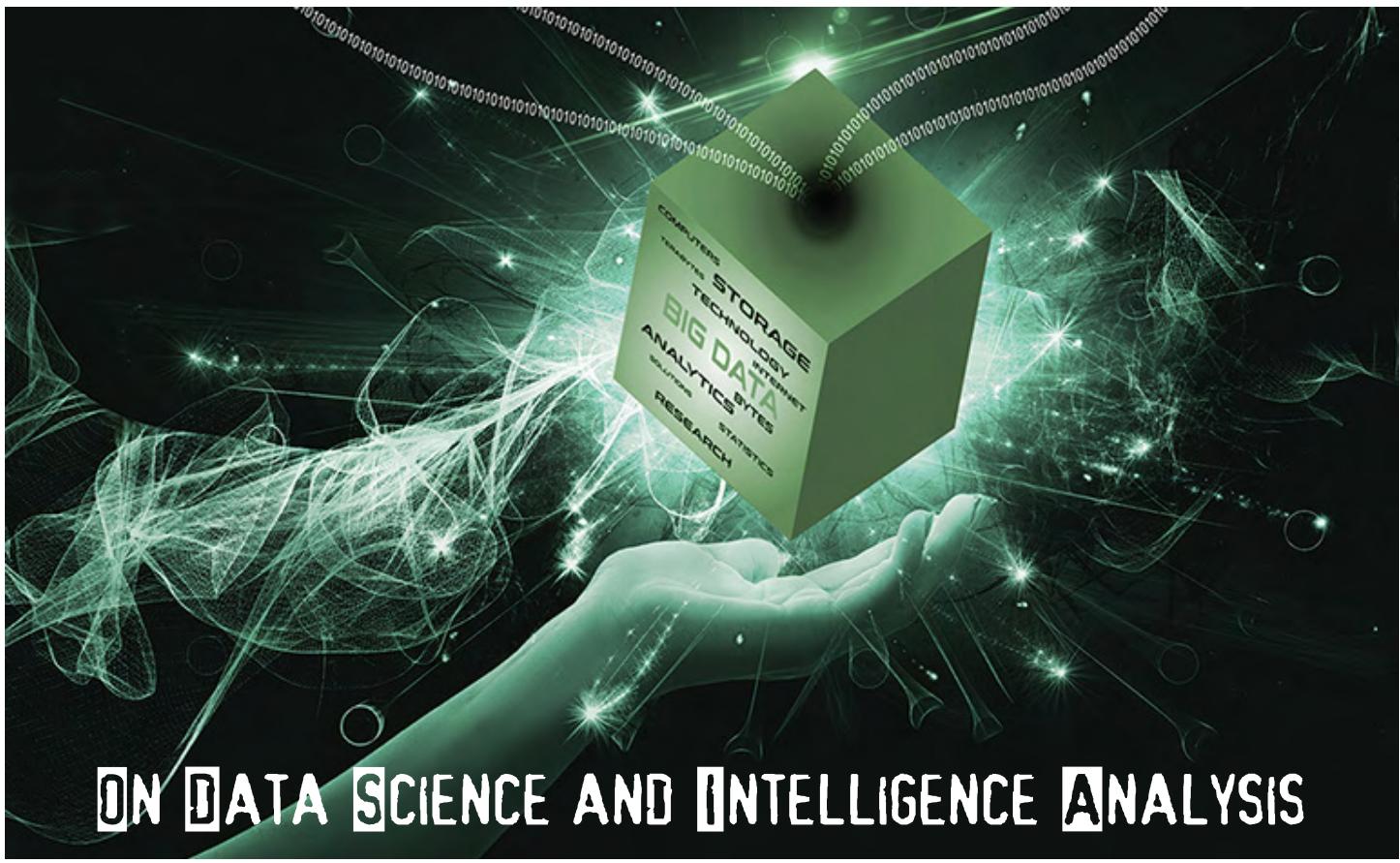
11. Ibid., D-1.

12. Ibid., D-16.

Ms. Terri Lobdell is the Chief, Keystone Doctrine and Doctrine Integration Branch, Directorate of Doctrine and Intelligence Systems Training, U.S. Army Intelligence Center of Excellence at Fort Huachuca, AZ. She is a retired military intelligence warrant officer with 24 years of active and reserve Army service. During her tenure, she served in various intelligence assignments from company to echelons above corps. She holds a master's degree in public administration from the University of Nebraska - Omaha.



The use of the newly developed military asset, the airplane, flew its first reconnaissance mission during Brigadier General Pershing’s 1916 Punitive Expedition into Mexico in pursuit of the bandit-turned-revolutionary Pancho Villa.



ON DATA SCIENCE AND INTELLIGENCE ANALYSIS

by Captain Iain J. Cruickshank

Editor's Note: This article is the first in a two-part series on data science. This first part provides a basic foundational understanding of data science and its application in the intelligence community. Part two of the series, by CPT Jason Boslaugh and Mr. Zachary Kendrick, will be published in the October-December 2019 issue. Their article discusses how the U.S. Army can apply data science lessons learned from academia and industry to modernize the intelligence warfighting function.

Introduction

There has been much hype in recent years about data science and big data—some well justified and some unwarranted. Many people see data science, and its associated disciplines of machine learning and artificial intelligence, as a panacea for the ills of modern decision making and analysis, especially those ills that plague the intelligence community.¹ However, some members of the intelligence community completely dismiss how military intelligence analysis can benefit from data science and machine learning. In this article, I will—

- ◆ clarify some of the roles of data science in intelligence analysis,
- ◆ describe conditions for its successful use, and
- ◆ promote an environment that maximizes the use of modern data science for better intelligence analysis.

Data science is a “multi-disciplinary field that uses scientific methods, processes, algorithms, and systems to extract knowledge and insights from data in various forms, both structured and unstructured.”² In simpler terms, it is the ability to distill knowledge (i.e., useful information to humans) from data (i.e., raw text, images, signals, etc.), typically using a computer. Data science often employs machine learning and other artificial intelligence techniques. As such, it is the preferred discipline for analyzing big data, online social networks, and other data sources that are simply too large, heterogeneous, and dynamic for any single human to comprehend.

Despite all the hype, data science is not a replacement for intelligence analysis. Intelligence analysis relies on much more than what data science as a discipline provides.³ Intelligence analysis relies on human intuition and experience. Rather than replace analysts, data science transforms analysts’ jobs in ways that make analysts more effective, focusing on applying human intuition. They are able to redirect the majority of their time and effort from the acquisition of information (i.e., reading reports or watching full motion video feeds) to thinking about the adversary, the environment, and trends in the battlespace.

Why Data Science?

As documented in a spate of recent articles, a trend has emerged to use more open-source and social network information for intelligence analysis.⁴ These sources of information can be invaluable but come in a deluge of constantly changing, error-prone data. Despite this, more intelligence analysts are relying on this type of data because it allows for insight that analysts cannot otherwise obtain by looking at other sources of information.⁵ Recent articles from the military intelligence community highlight several problems, including—

- ◆ A lack of interoperable and integrated data sources, and a lack of a common operational picture and ontology needed to understand information.⁶
- ◆ A lack of methods that can make information intuitive to understand and provide patterns easy to comprehend for an analyst. Furthermore, a lack of having methods that can adapt to different warfighting domains (i.e., cyberspace, counterinsurgency, etc.).⁷
- ◆ Overwhelming and contradictory reporting, as well as filtering of available information for an analyst.⁸
- ◆ A large amount of time spent monitoring full motion video feeds or sifting through volumes of reports to find a few actionable pieces of information.

These problems coalesce around intelligence analysts being able to get the “right” information and have the information presented in a way that enables their analyses. While analysts now use more and varied information for intelligence analysis, issues persist with how to process that voluminous, varied information to allow analysts to exploit it. In this situation, I would argue that data science flourishes as a discipline.

All the recent developments in industry by companies like Google, Facebook, and Microsoft have boosted interest in data science and artificial intelligence, and the Department of Defense has taken notice. The 2018 National Defense Strategy and its service-derivative documents all prominently feature artificial intelligence and modern, digital technologies.⁹ Recent advances in the Internet of things and drones have led to breakthroughs in collection technology for intelligence purposes.¹⁰ Members of the military intelligence community have also pushed to incorporate the tools of data scientists, most notably machine learning.¹¹ What these articles lack, however, is guidance on how we should implement data science and machine learning for intelligence analysis.

But there is a caveat for the use of data science and artificial intelligence—*simply buying off-the-shelf machine learn-*

ing and artificial intelligence products will be insufficient. Here’s why:

First, data science is still a new discipline. As a new discipline, many of its tools and methods are not engineered for people outside of specific applications, like the technology industry and academia. If analysts cannot understand the tools, analysts will not use them.

Second, no unique algorithms or models exist that will apply in all situations. The more complex and dynamic the data environment, the less any one given algorithm or set of tools will be applicable.

Third, off-the-shelf tools are not necessarily the solution. With the rise of adversarial machine learning, and the fact that the enemy always gets a vote in any conflict, any off-the-shelf tool will need to be adapted and changed as the enemy develops its algorithmic countermeasures. A great example of what adversarial machine learning can do are the recent studies on fooling image detection machine learning algorithms.¹² And if the tool is not open source, but rather some proprietary product, adapting it to the realities on the battlefield may be impossible. Thus, while it may be attractive to buy off-the-shelf artificial intelligence and machine learning tools, these tools will not meet the unique needs of intelligence analysis.

The Relationship

Data science can enable intelligence analysis by its ability to digest large, heterogeneous, error-prone data into humanusable information like trends, outliers, and key data points. To better illustrate this point, I will begin with a simple analogy—gold mining. The whole point of the gold-mining industry is to find gold and mine it from the earth. This gold is critical for various uses around the world. Now, a gold miner can only dig up so much earth; if he digs in the wrong places, he will fail to produce gold. A land surveyor, on the other hand, can find likely places in the earth where there is gold, but the land surveyor is not skilled in mining. Thus, a beneficial arrangement arises. The land surveyor indicates where gold is likely to exist, and the gold miner skillfully extracts it from the earth. The land surveyor’s expertise leads to the gold miner extracting more gold because he is only digging where the gold is likely to be. Now, substitute the terms *intelligence analyst* for *gold miner*, *data scientist* for *land surveyor*, and *actionable intelligence that drives commanders’ decisions* for *gold*, and you will understand how data science can significantly empower intelligence analysis. An intelligence analyst applies meaning and forms intelligence estimates based on the trends and patterns that a data scientist was able to surface.

Without diving into specific algorithms and methods, the following are some common ways data science can enable intelligence analysis:

- ◆ Allows entity detection on full motion video (i.e., Project Maven), so that analysts do not have to keep their eyes glued to just one full motion video screen for endless hours, but rather are cued to the video when something of interest happens.
- ◆ Characterizes reports, images, and other forms of information into more visual and interpretative formats for quick understanding of the intelligence environment.
- ◆ Provides predictive analytics that are constantly running, based upon key indicators of some event of interest.
- ◆ Expresses uncertainty in information available in both the information space and geographically.
- ◆ Identifies anomalies in information and in target behavior.
- ◆ Provides content recommendation to help identify more pieces of relevant information based on what analysts identify as relevant information for their intelligence analyses.

While this is not a complete list, it is important to note that at no point does data science replace intelligence analysis. None of these methods explains why an adversary might do what they do, nor do these methods negate analysts' judgments. Rather, they are tools that allow analysts to focus their effort on thinking about those key pieces of information and making informed judgments, instead of searching for information or detecting anomalies. Furthermore, removing extraneous information will allow analysts not only to spend more of their effort on actual analysis, but also to produce better intelligence.¹³

One final point about the relationship between an intelligence analyst and a data scientist. Data science uses "feature selection," which is the process of selecting variables from the information you will use in your models. A data scientist uses variables present in the data that actually relate to the phenomenon that is being analyzed. Subject-matter expertise is tremendously important in this area, and thus, it is where the intelligence analyst must play a role. When it comes to selecting attributes about the enemy, populace, or terrain, an intelligence analyst needs to be involved in that selection. So, when it comes to feature selection, the features should be a combination of what an intelligence analyst deems important and what a data scientist can meaningfully use.

Enabling Data Science for Intelligence Analysis

Data scientists occasionally say that for good data science, they need three elements:

- ◆ a good problem,
- ◆ computational resources, and
- ◆ available data.

Intelligence analysis presents the needed "good problems," but intelligence systems are generally not set up for proper computational resources and data management.

A Good Problem. In the field of intelligence analysis, there are many good problems for data scientists to resolve. What is more, as data science is incorporated into intelligence analysis, many more good problems are likely to arise.

Computational Resources. One resource that all data science methods and algorithms require is computing power. Typically, most industry and academic data scientists rely on cloud computing for this power. Cloud computing allows data scientists to create a virtual machine, from anywhere in the world, that has the exact specifications they need for the data science analyses they are going to perform, with far more computational power than can realistically be carried about. Cloud computing also enables economies of scale for computing resources, which is critical for any large-scale organization. The need for cloud computing resources is well known to the intelligence community. The community has, however, consistently failed to materialize this cloud infrastructure for a variety of reasons.¹⁴ New attention and urgency should be paid to getting a cloud architecture working to enable data science for intelligence.

There are also considerations about how data science will work in austere and electromagnetically degraded environments. For example, virtualization through things like VMware or Docker provides cheap and effective ways for data scientists to continue to use their tools on local machines, without needing additional equipment or a connection to the wider enterprise. All that is required is the ability to have virtual machines on those physical machines with access to classified networks. Finally, it is important to note that many data science tools are open source and constantly updating, and they require a programming ability in the R or Python programming languages. Therefore, closed, static data intelligence suites like the Distributed Common Ground System-Army are not suitable. They do not allow for data scientists to program and bring in their own tools to the computational environment where the data lives.

Available Data. Data management is the other major issue hampering the use of data science for intelligence analysis.

As the intelligence community has already remarked, the varied, heterogenous databases of information make getting access to any information, nonetheless the right information, exceedingly difficult.¹⁵ In essence, these problems result in having to manually search through intelligence databases or download by hand from intelligence analysis suites the information that is vital to data science. This manual labor will result in a huge loss of time for analyses and will likely be missing information. Therefore, it is critical for data science-informed intelligence analysis to have systems that have mandated programmatic access to their data from things like application programming interfaces and standard data ontologies.

Conclusion

Intelligence analysis is increasingly relying upon greater, more heterogeneous sources of information. As a result, the sheer amount of information is far exceeding what an intelligence analyst can parse while still producing actionable intelligence. Problems with inconsistent, dynamic, and erroneous information continue to plague intelligence analysis. All these problems naturally point to a solution—using data science in intelligence analysis, not as a replacement for intelligence analysts but as a means for enabling faster, better quality intelligence.

Some key conditions exist, however, like cloud computing and appropriate data management, which still must be addressed in intelligence systems in order to enable data science. Once addressed, data science will provide a distinct combat advantage to whichever force is best able to employ it as part of its intelligence analysis process. If the trends regarding greater volumes of digital information being available for intelligence continue into the future—as they almost certainly will—it is not unreasonable to expect intelligence analysts to take on many of the skills of data science, while data scientists work on core algorithmic development and specialty analyses. To get to this point, we need to establish a solid and beneficial working relationship between data scientists and intelligence analysts. 

Endnotes

1. Drew Conway, “Data Science in the U.S. Intelligence Community,” *IQT Quarterly* 2, no. 4 (Spring 2011): 24-27, https://static1.squarespace.com/static/5150aec6e4b0e340ec52710a/t/51525211e4b0e9fad0b56f9c/1364349457311/IQT-Quarterly_Spring-2011_Conway.pdf.

2. Vasant Dhar, “Data Science and Prediction,” *Communications of the ACM* 56, no. 12 (December 2013): 64-73, <https://cacm.acm.org/magazines/2013/12/169933-data-science-and-prediction/fulltext>.
3. John Coyne, “The Future of Intelligence Analysis: Computers versus the Human Brain?” *The Strategist*, Australian Strategic Policy Institute Blog, 12 September 2017, <https://aspistrategist.siteindev.com.au/future-intelligence-analysis-computers-versus-human-brain/>.
4. Paul B. Symon and Arzan Tarapore, “Defense Intelligence Analysis in the Age of Big Data,” *Joint Force Quarterly* 79, 4th Quarter (October 2015), <https://ndupress.ndu.edu/Media/News/Article/621113/defense-intelligence-analysis-in-the-age-of-big-data/>.
5. Damien Van Puyvelde, Shahriar Hossain, and Stephen Coulthart, “National security relies more and more on big data. Here’s why,” *Washington Post*, 27 September 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/27/national-security-relies-more-and-more-on-big-data-heres-why/?utm_term=.97152b2b58e9.
6. Donald Beattie and Robert Coon, “Improving Intelligence Sharing,” *Military Intelligence Professional Bulletin* 44, no. 4 (October-December 2018): 25-28.
7. Christie P. Cunningham, “Developing Analytic Capabilities in Changing Environments,” *Military Intelligence Professional Bulletin* 44, no. 4 (October-December 2018): 68-71.
8. Alex Morrow and Michael Dompierre, “Getting Intelligence to Move at the Speed of Decisive Action,” *Military Intelligence Professional Bulletin* 44, no. 4 (October-December 2018): 55-58.
9. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, n.d., <http://nssarchive.us/national-defense-strategy-2018/>.
10. Daniel C. Tuttle and Robert D. Sensenig II, “Strength Begins with Science and Technology,” *Military Intelligence Professional Bulletin* 44, no. 1 (January-March 2018): 25-30.
11. Robert Collins, Lindsay Yowell, and Greg Hartman, “The Future of Intelligence Analysis, Analytics, and Distribution,” *Military Intelligence Professional Bulletin* 44, no. 4 (October-December 2018): 35-37.
12. Drew Harwell, “Amazon facial-identification software used by police falls short on tests for accuracy and bias, new research finds,” *Washington Post*, 25 January 2019, https://www.washingtonpost.com/technology/2019/01/25/amazon-facial-identification-software-used-by-police-falls-short-tests-accuracy-bias-new-research-finds/?noredirect=on&utm_term=.4bb5999b6004.
13. Zeynep Tufekci, “Big Data and Small Decisions,” *Scientific American* 320, no. 3 (March 2019).
14. Naomi Nix, “Inside the Nasty Battle to Stop Amazon From Winning the Pentagon’s Cloud Contract,” *Bloomberg*, December 20, 2018, <https://www.bloomberg.com/news/features/2018-12-20/tech-giants-fight-over-10-billion-pentagon-cloud-contract>.
15. Beattie and Coon, “Improving.”

CPT Iain Cruickshank is currently a Ph.D. candidate in societal computing at Carnegie Mellon University as a National Science Foundation Graduate Research Fellow. His previous assignments include Company Commander for D Company, 781st Military Intelligence Battalion (Cyber), and sub-element lead for planning and analysis and production on a National Mission Team in the Cyber National Mission Force. CPT Cruickshank holds a bachelor of science from the U.S. Military Academy. He also holds a master of science in operations research from the University of Edinburgh, obtained as a Rotary Ambassadorial Fellow. He has deployed to Paktia, Afghanistan, as a member of Security Force Advise and Assist Team.



Photo courtesy of the Australian War Memorial

A wireless telegraphist operator, probably Sgt William 'Billy' Bennett, British Solomon Islands Protectorate Defence Force, operating an AWA 3BZ teleradio at the Seghe coastwatchers' station ZFJ5.

Human Intelligence as a Deep Sensor in Multi-Domain Operations: Australia's World War II Coastwatchers

by Colonel Justin Haynes

Introduction

The U.S. Army's concept of multi-domain operations addresses multiple problems posed by near-peer and peer adversaries in both competition and conflict. China, Russia, and other adversaries seek to leverage layered stand-off¹ to achieve their aims, employing kinetic and non-kinetic operations with increasing sophistication and effectiveness. This new environment requires the joint force to penetrate and disintegrate threat antiaccess and area denial systems

in order to set conditions for the United States and our allies to exploit gains and achieve operational and strategic objectives in the close and deep maneuver areas. Layered intelligence, surveillance, and reconnaissance² will be vital in enabling joint force commanders to make sound and timely decisions faster than our adversaries can respond by determining enemy force composition, disposition, and intent, as well as providing an understanding of the most critical factors shaping the operational environment.

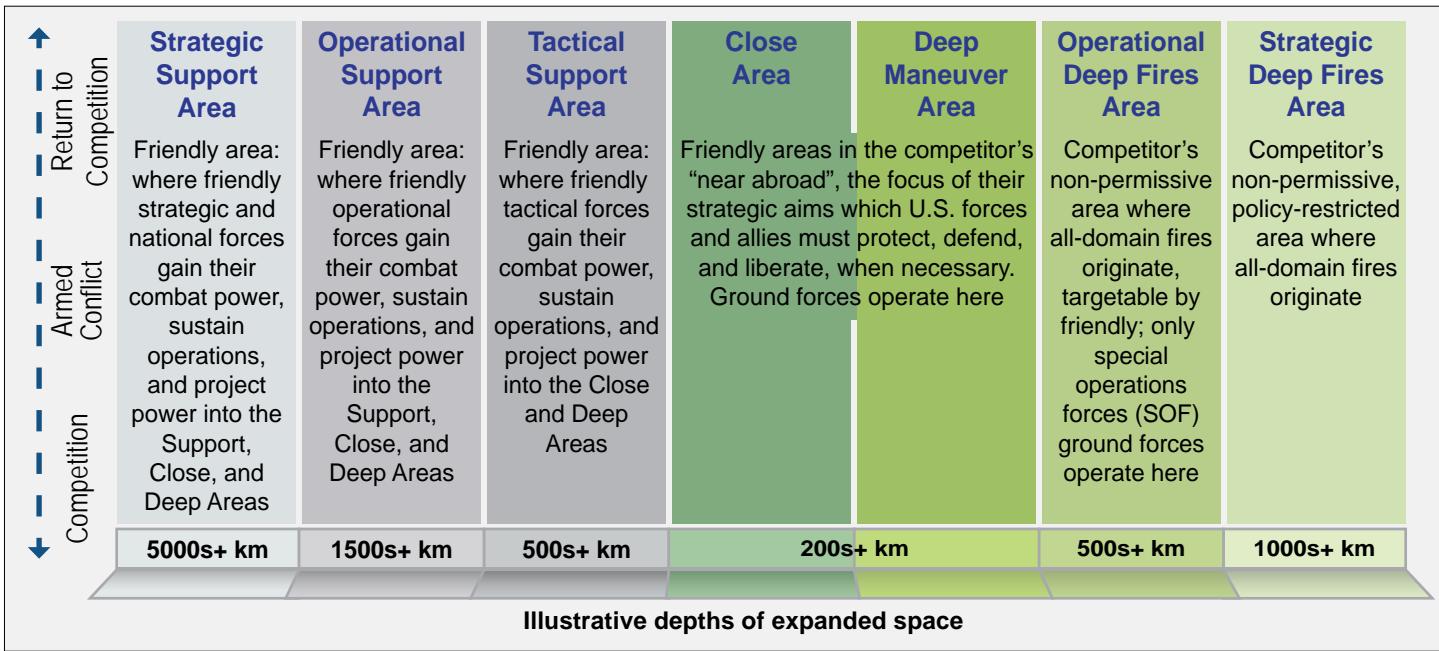


Figure 1. Multi-Domain Operations Framework³

As the Army looks to the multi-domain operations concept to guide how we use intelligence, surveillance, and reconnaissance resources in the future, it is essential to recall historical examples that may provide valuable lessons learned. Australia's employment of coastwatchers in the South Pacific Campaign during World War II provides an excellent example of human intelligence as a deep sensor in a multi-domain environment. The coastwatcher network provided tactical and operational information on enemy forces while also providing Allied commanders an understanding of the operational environment across the land, sea, and air domains. On multiple occasions, the coastwatcher network also served as an auxiliary unconventional warfare force that supported both direct action and personal recovery operations. Their activities within what we would now consider the close, deep maneuver and operational deep fires areas of the multi-domain operations framework proved invaluable to the Allies' efforts to penetrate the antiaccess and area denial system that the Empire of Japan established in early 1942.

The Coastwatchers and “Ferdinand”

Australia formed its initial coast watching organization shortly after the end of World War I in order to provide early warning of threats and activity on its northern coast. The military first established outposts in the region in September 1914, when it seized German possessions in the South Pacific and included civilian settlements in order to expand the breadth and depth of its network.⁴ In 1939, Australia's entry into World War II, as part of the British Commonwealth, increased emphasis on the importance

of this network.⁵ The Royal Australian Navy's intelligence department focused on preparing the network's more than 800 personnel for combat operations. This network came to be known by its call sign “Ferdinand,” drawing its moniker from the story of Ferdinand the Bull, as a reminder that its members were best suited for quietly observing their surroundings as opposed to engaging in direct fighting.⁶

The Story of Ferdinand

LCDR Eric Feldt, Royal Australian Navy, decided the coastwatcher organization needed a codename. He chose *Ferdinand*, from the children's classic, *The Story of Ferdinand*, about a bull who would rather smell flowers than fight in bullfights. LCDR Feldt later explained: “I chose Ferdinand...who did not fight but sat under a tree and just smelled the flowers. It was meant as a reminder to Coastwatchers that it was not their duty to fight and so draw attention to themselves, but to sit circumspectly and unobtrusively, gathering information. Of course, like their titular prototype, they could fight if they were stung.”⁷

The Ferdinand network succeeded primarily because of three fundamental factors:

- ◆ First, Australia successfully identified significant intelligence gaps following the conclusion of World War I when German colonial forces had threatened Northern Australia and its interests in the archipelagos throughout the South Pacific.
- ◆ Second, the Australian Navy then took action to establish a broad human intelligence network well before hostilities to cover these gaps with overlapping coverage and secure communications.

- ◆ Third, the coastwatchers leveraged sources who were intimately familiar with the harsh conditions found in the South Pacific and uniquely suited to survive deep behind enemy lines.

These efforts resulted in a robust and resilient system, which enabled Allied commanders to take action within Japanese decision cycles.

The operational environment encompassed a vast geographic expanse spanning from the mountainous jungles of Papua New Guinea in the west to the thousands of islands found in the Bismarck Archipelago and the Solomon Islands to the east. More than 1,200 nautical miles separated the westernmost coastwatcher in the coastal town of Aitape, on the northern coast of Papua New Guinea, and the station on San Cristobal Island located at the southeastern extent of the Solomon Islands.⁸ In order to cover this immense expanse, Australian naval intelligence established more than 85 remote locations to observe and report enemy activity and support Allied military operations.

Native islanders made up the majority of the civilian population throughout this region. These indigenous people were organized primarily as tribal cultures with widely dispersed villages of 100 to 200 people. The natives used simple tools in order to maintain a primitive, subsistence lifestyle based on fishing, hunting, and gathering, supplemented by limited crops. The islanders' primary contact with the outside world was through interaction with western men who sought the adventure of living in remote, tropical climes—men who saw profit in the natural resources found there and on occasion Chinese traders who traversed the region to barter for resources.⁹

The westerners living among the native peoples consisted of a diverse group of military personnel and civilians. These individuals, primarily white Australian men, formed the core of the group. They would report for duty as coastwatchers under the Australian naval intelligence service in the interwar years.¹⁰ Civilians greatly outnumbered military personnel and consisted of local government officials, planters,

miners, tradesmen, and sailors on small ships and boats.¹¹ Western missionaries also settled across this wide expanse to bring Christianity to the animist native population.

The Ferdinand network's preparation for conflict included training coastwatchers to use radios, basic codes, and reporting procedures. Between September and December 1939, LCDR Eric Feldt, staff director for intelligence in Port



Photo courtesy of the Australian War Memorial

LCDR E.A. Feldt, Royal Australian Navy, takes over from CDR E.H. Kincaid, U.S. Navy, as Naval Officer in Charge, Torokina, Solomon Islands.

Moresby, New Guinea, visited nearly every outpost to ensure the coastwatcher network was ready for war.¹² Feldt had extensive pre-war experience in Papua and the Solomon Islands, which gave him great credibility with the members of the organization. He would remain a vital leader in running the coastwatcher organization and linking it to the Combined Operational Intelligence Center in Townsville on Australia's northeast coast.

Small numbers of military personnel and civilian volunteers operated Feldt's coastwatcher stations; normally no more than three individuals manned each location. Frequently, local natives supported the coastwatchers, leveraging long-term relationships built before the war. Those relationships would come under significant strain as Japanese forces

invaded New Guinea in early 1942, and extended their reach throughout the Bismarck Archipelago and the Solomon Islands in the following months. On multiple occasions, the westerners found themselves isolated and harried by natives who either had turned to support the Japanese invaders or had seen opportunities to attack the coastwatchers now that they were vulnerable.¹³

The coastwatcher station's radio was its most critical item of equipment ensuring reliable reporting on Japanese activity. Radio operators sent reports on a common frequency, which stations throughout the network monitored, in order to share combat information. The stations also served as relays to distant receivers. Broad reporting criteria that Feldt had set included sightings of ships, aircraft, and floating mines; composition and disposition of ground forces; and information related to the operational environment.¹⁴

The Effectiveness of the Ferdinand Network

The coastwatchers immediately demonstrated the effectiveness of the Ferdinand network when the Japanese launched their offensive throughout the South Pacific in January 1942. The Japanese rapidly moved to secure airfields, ports, and sea lines of communication while the United States Navy was still reeling from the attack on Pearl Harbor. Tokyo's seizure of critical land features, coupled with control of both the air and maritime domains, established an antiaccess and area denial system that threatened

Island, which had the fortuitous position of being on the direct flight path between the major Japanese airbases at Rabaul and Guadalcanal.

The United States 1st Marine Division landed on Guadalcanal and several neighboring islands on 7 August 1942, initiating the Solomon Islands campaign. The following day, Read observed 45 Japanese dive bombers flying southeast from Rabaul toward the United States fleet still engaged in supporting the Marine landings more than 400 miles away. Read relayed a flash message to Port Moresby, which in

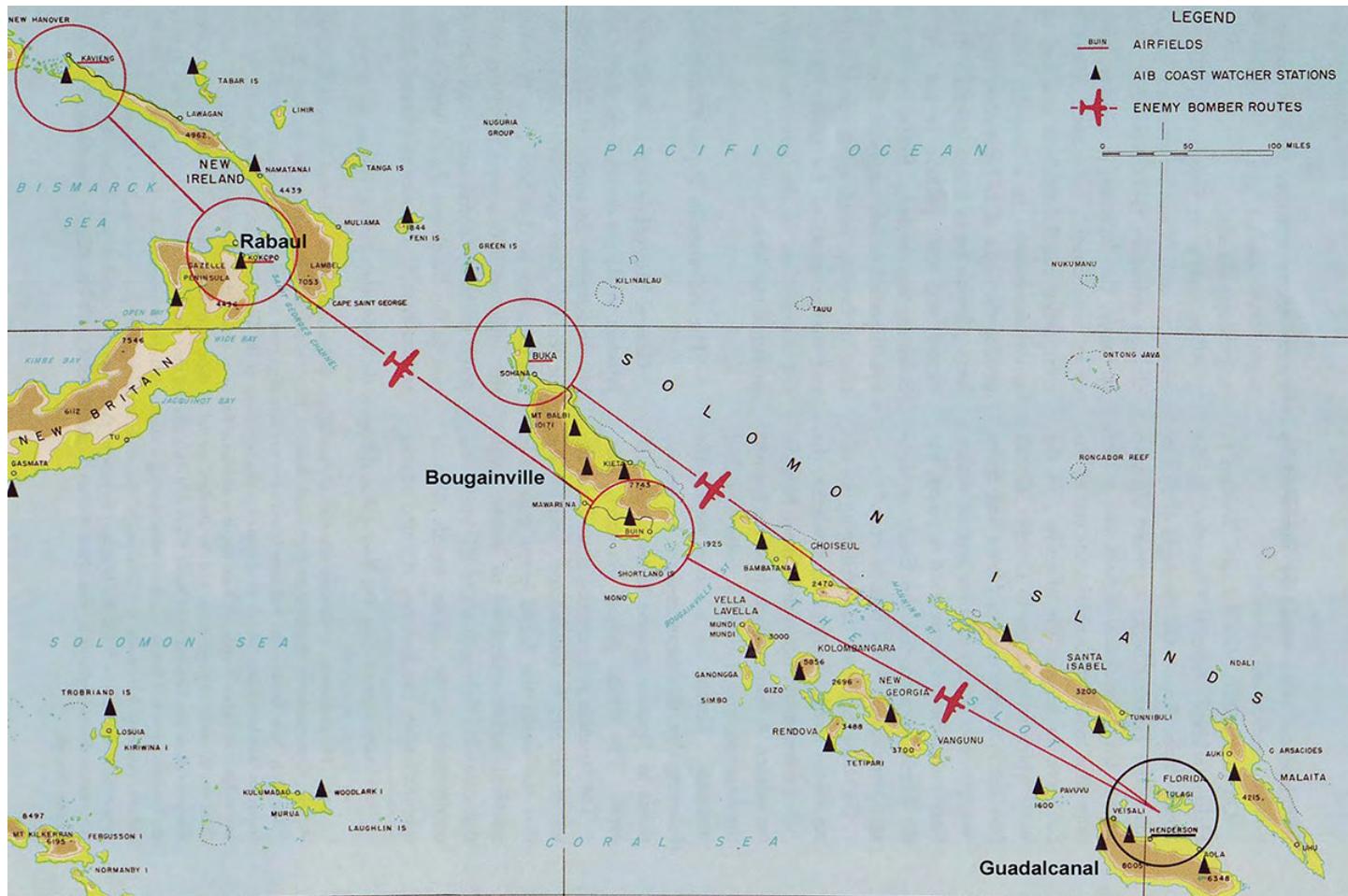


Figure 2. Coastwatchers in the Solomon Islands¹⁵

to isolate Australia from the United States at a time when the majority of her armed forces were fighting the Germans in North Africa. The coastwatchers were vital in providing intelligence on Japanese air, naval, and ground operations, allowing the Allies to focus finite resources to defend against Japanese attacks while also enabling them to exploit windows of opportunity and surprise the Japanese when they were most vulnerable.

Coastwatcher Jack Read's exploits on Bougainville Island serve as an excellent example of how the Ferdinand network provided actionable intelligence to the Allies. Read's station was located on the north end of Bougainville

turn sent the message through the Allied intelligence center in Townsville to the American fleet within 10 minutes of observing the Japanese bombers.¹⁶ This message provided the United States Navy more than 2 hours of early warning, which enabled the Navy to disperse ships, man antiaircraft weapons, and launch fighter aircraft in time to intercept the Japanese bombers. Read's rapid, accurate, and relevant intelligence reporting resulted in at least 16 Japanese aircraft shot down and prevented the disruption of United States landing operations on Guadalcanal.¹⁷

Read and other members of Ferdinand would repeat this feat on numerous occasions, providing Allied forces

critical intelligence on Japanese air, naval, and ground forces throughout the war. In addition to providing air raid warning, coastwatchers alerted Allied forces of Japanese ship movements and ground forces on the numerous islands and rugged jungles of the South Pacific. Human source networks among the local native populations and a limited number of westerners in the region provided extensive information on the enemy in addition to direct observation on Japanese forces.

Coastwatcher Keith McCarthy, located on New Britain Island, provided the Australians the first intelligence on the composition and disposition of Japanese forces at Rabaul, while also supporting the recovery of numerous Australian Soldiers who had fled into the jungle after the Japanese invasion.¹⁸ Other coastwatchers used local native sources to provide battle damage assessments of Japanese airfields after Allied air raids.¹⁹ Furthermore, Ferdinand saved the lives of more than 110 Allied fliers by either recovering or reporting the location of Allied pilots who had crashed in the region.²⁰

Ferdinand reporting on enemy ship movements throughout the Solomon Islands also enabled the Allies to interdict the “Tokyo Express” running reinforcements to Guadalcanal, resulting in the isolation of Japanese troops there. Jack Read, while evading Japanese patrols on the northern end of Bougainville Island, observed a major buildup of Japanese vessels on 6 November 1942. Understanding that this group of ships could rapidly deliver an additional division of Japanese troops to fight the United States Marines on Guadalcanal, Read took a risk by breaking from his evasion to report. On 14 November, 11 Japanese transports accompanied by 12 destroyers as escorts sailed from Bougainville to land their cargo of 15,000 Japanese soldiers on Guadalcanal, only to be interdicted by American aircraft that were ready to strike because of the intelligence that Read had provided. Only four Japanese troop transports survived, delivering just a fraction of the troops and supplies that the Japanese desperately needed on Guadalcanal, dooming a planned offensive.²¹

A Harsh Environment

Despite their numerous successes, the Ferdinand network was a costly endeavor, resulting in the loss of more than 35



LCDR W. J. (Jack) Read, Naval Intelligence Division, Royal Australian Navy, with his native scouts and other personnel at the Australian Intelligence Bureau camp, Lunga, Guadalcanal, British Solomon Islands Protectorate, March 27, 1945. Read is the European on the left.

Photo courtesy of the Australian War Memorial

coastwatcher lives.²² Jack Read, Keith McCarthy, and other coastwatchers operated deep behind enemy lines with limited resources and minimal opportunities for external support. These factors increased the risk to both personnel and their vital intelligence-gathering mission. Coastwatcher vulnerabilities included three primary threats: Japanese signals intelligence operations, human compromise, and the hostile nature of the environment itself.

Japan fielded extensive signals intelligence capabilities by leveraging naval platforms, aircraft, and ground collection systems to intercept and locate the source of coastwatchers’ transmissions. The Japanese Imperial Navy was responsible for collection in the Solomon Islands, while the Army focused on New Guinea. Naval radio direction finding units established at Rabaul and Guadalcanal provided anchor points for a collection baseline, posing the greatest threat to Australian coastwatchers.²³ The Japanese rapidly hunted down coastwatchers who did not practice disciplined communications and forced many off the air as they moved away to avoid capture and likely execution.

Despite their remote operating locations, Ferdinand’s coastwatchers were in frequent contact with native islanders. These islanders provided opportunities for sources of enemy information and logistical support, but they were also formidable adversaries when they cooperated with the Japanese. Jack Read noted that Japanese search parties were not effective in hunting for him and his compatriots

by themselves, yet when paired with a native tracker they became formidable threats.²⁴ Maintaining positive relations with the islanders became an imperative, as they provided a measure of force protection and early warning against Japanese ground movements, as well as food and other supplies to the coastwatchers when needed. Even with good relations, support of the local populace could rapidly change because of threats from the Japanese forces or in the event islanders sought to aid them through personal motivations.²⁵

The environment in which the coastwatchers lived and survived posed just as much a threat to their lives as to their Japanese enemies. Malarial fevers, dysentery, and typhus were common among the coastwatchers with limited to no medical support available.²⁶ Even small cuts and abrasions were vulnerable to infection and gangrene. Because of these conditions, only men with detailed knowledge of how to live in the jungle and survive in extreme isolation were able to remain in their posts. Medical evacuation was difficult to coordinate and exposed the extraction platform, usually a submarine, patrol torpedo boat, or amphibious plane to Japanese attack.

Applying Lessons Learned to Contemporary Environments

Studying the Australian coastwatching network provides multiple lessons learned that we might apply to contemporary environments found in numerous combatant command areas of responsibility today. This case study highlights how an operational-level human intelligence network in a coastal environment effectively supported operations in multiple domains, spanning throughout the depth and breadth of the multi-domain operations battlefield framework. Following World War I, Australia identified a significant vulnerability in its ability to maintain overwatch of the great expanse of islands and seas to its north. The Australian naval intelligence service's foresight allowed it to develop the coastwatcher network in peacetime, well before anticipated hostilities, ensuring the success of the organization. This decision ensured Ferdinand's coastwatchers were well trained, properly positioned deep within the enemy's battlespace, and experienced in their operating environment before Japan's invasion of the South Pacific. Once the Japanese seized terrain and controlled air and sea space, it would have been incredibly difficult to establish an extensive source network behind enemy lines. Additionally, Ferdinand's simple yet effective communications network ensured rapid reporting of relevant combat information in time for the Allies to counter Japanese moves. Finally, the Ferdinand network was built around individuals with an

intimate understanding of their harsh operating environment, which enabled them to operate with minimal external support for long periods of time.

The Australian Navy employed the Ferdinand network as a deep sensor to provide early warning intelligence in support of land and maritime operations in the Solomon Islands and enable targeting for air and naval operations. Similar and successful employment of Army human intelligence as a deep sensor in multi-domain operations—through identification of sources with appropriate placement and access in advance of need—will enable setting the theater through more refined intelligence preparation of the battlefield and deliver enhanced battlefield awareness to commanders. The reporting of adversary unit identifications, locations, and activity will enable effective cross-cueing of all intelligence disciplines to tip, cue, confirm, and target threat forces across all operational domains in both competition and conflict. 

Endnotes

1. Stand-off is “the physical, cognitive, and informational separation that enables freedom of action in any, some, or all domains, the electromagnetic spectrum, and information environment to achieve strategic and/or operational objectives before an adversary can adequately respond.” Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), GL-8.
2. Ibid., 33.
3. Ibid., 8.
4. “Operations against German Pacific Territories,” Australian War Memorial, accessed 5 March 2019, <https://www.awm.gov.au/collection/E84777>.
5. Peter Dunn, “Coast Watch Organisation or Combined Field Intelligence Service Section “C” of the Allied Intelligence Bureau,” Australia@War, accessed 5 March 2019, <http://www.ozatwar.com/sigint/coastwatchers.htm>.
6. Eric Feldt, *The Coast Watchers* (New York: Oxford University Press, 1946), 4.
7. Feldt, *The Coastwatchers*, 95, quoted in “Australia and the Second World War: The Coastwatchers 1941-1945,” The Anzac Portal, Australian Government, Department of Veterans’ Affairs, accessed 8 March 2019, <https://anzacportal.dva.gov.au/history/conflicts/australia-and-second-world-war/resources/coastwatchers-19411945>.
8. A. B. Feuer, ed., “Introduction: The South Pacific Coast Watching Network,” in *Coast Watching in World War II* (Mechanicsburg, PA: Stackpole Books, 1992), xvii.
9. Feldt, *The Coastwatchers*, 27-33.
10. Ibid.
11. John Brown, “Coastwatchers on New Britain,” *World War II* 13, no. 1 (May 1998): 8.

12. Ibid., 6.
13. Feldt, *The Coast Watchers*, 36.
14. Dunn, *Coast Watch Organisation*.
15. Mark Tempest, "Sunday Ship History: Coast Watchers in the South Pacific," *EagleSpeak* (blog), July 27, 2008, <http://www.eaglespeak.us/2008/07/sunday-ship-history-coast-watchers-in.html>.
16. Jack Read, "Air Battles at Guadalcanal, August 8, 1942-January 1, 1943," in *Coast Watching*, 63-64.
17. Walter Lord, *Lonely Vigil* (New York: Viking Press, 1977), 46.
18. Feldt, *The Coast Watchers*, 36.
19. Feuer, *Coast Watching*, 69.
20. Lord, *Lonely Vigil*, 292-293.
21. Ibid., 105-106.
22. "The Role of Australian Coastwatchers in the Pacific War," Battle for Australia, accessed 4 March 2019, <http://www.battleforaustralia.org/Theyalsoserved/Coastwatchers/CoastwatcherRole.html>.
23. John Prados, "Neglected Intelligence: The Japanese in the Solomons Campaign," *U.S. Naval Institute Proceedings* (August 2013): 66-71.
24. Jack Read, "Porapora Days and the U.S.S. *Nautilus* Rescue, November 4, 1942-January 1, 1943," in *Coast Watching*, 77.
25. Brown, "Coastwatchers on New Britain": 8.
26. Feldt, *The Coast Watchers*, 27.

References

- Acred, Matthew Laird, ed. "Japanese Invasion Movements Early Pacific Campaign 1942." Asisbiz. Accessed 6 March 2019. <https://asisbiz.com/>.
- Commonwealth of Australia, Department of the Navy, Supervising Intelligence Officer, North-Eastern Area. 4 May 1945. <https://recordsearch.naa.gov.au/SearchNRetrieve/Gallery151/dist/JGalleryViewer.aspx?B=410895&S=1&N=208&R=0#/SearchNRetrieve/NAAMedia>ShowImage.aspx?B=410895&T=P&S=24>.
- Hastings, Max. *Inferno: The World at War 1939-1945*. New York: Alfred A. Knopf, 2011.

COL Justin Haynes is a career military intelligence officer who has served in command and staff positions within the 82nd Airborne Division, 172nd Stryker Brigade Combat Team, 160th Special Operations Aviation Regiment (Airborne), and the 504th Battlefield Surveillance Brigade. He commanded the 502nd Military Intelligence Battalion at Joint Base Lewis-McChord, WA, and served as the G-33 Current Operations Chief for U.S. Army Intelligence and Security Command before attending the National War College. COL Haynes is currently the senior planner for the Deputy Chief of Staff, G-2 Initiatives Group, and will assume command of the Expeditionary Operations Support Group in June 2019.



Photo courtesy of the Australian War Memorial

British Capt W. F. Martin Clemens (left, with beard), Coastwatcher and District Officer on Guadalcanal, Solomon Islands, being debriefed by LTC Buckley (second from left), Commanding Officer Division 2 (Intelligence), United States 1st Marine Division on August 18, 1942. Other identified personnel are: Lieutenant F. Kidd (third from left), Division 2, United States 1st Marine Corps; Flight Lieutenant Charles Widdy (right), Royal Australian Air Force, a guide with the 1st Marine Division. Obscured on the right is a sergeant of the Division 2 staff taking notes.



The Military Intelligence Corps 2019 Hall of Fame Inductees

Colonel James A. Bartlett, U.S. Army, Retired

Following graduation from the University of Texas and Officer Candidate School, Jim Bartlett was commissioned a second lieutenant in Army intelligence. He served two combat tours in Vietnam. As an aerial reconnaissance officer with the 1st Military Intelligence (MI) Battalion, he developed a targeting program to facilitate timely provision of information to commanders. On a second tour, he served with a Military Assistance Command, Vietnam (MACV) Province Advisory Team—responsible for province and district intelligence operations. The Province Intelligence Program was designated the “model” for MACV. Between Vietnam tours, he was an instructor with the Intelligence School.

COL Bartlett commanded the 504th MI Detachment with 4th Armored Division in Germany providing intelligence support to division and subordinate elements. He was assigned to the 66th MI Brigade where he played a key role in a major reorganization initiative and led a source control branch that managed intelligence sources throughout theater.

After Command and General Staff College, he was assigned to the Pentagon. As the action officer for joint reconnaissance on the Army Staff, he ensured the Army played a key role in national policy. He implemented procedures to provide intelligence from national assets to tactical commanders. He then served at Army Personnel Command (PERSCOM) where he managed assignments for MI majors.

In January 1980, he took command of the 11th MI Battalion, the only tactical technical intelligence (TECHINT) unit in the Department of Defense (DoD). It provided TECHINT and foreign material support to defense organizations worldwide. COL Bartlett then commanded the 163rd MI Battalion at Fort Hood, Texas. This organization provided aerial reconnaissance, signals intelligence, counterintelligence, interrogation, and long-range surveillance unit support to III Corps. He initiated a training program that was named the prototype for U.S. Army Forces Command. After the War College, COL Bartlett served as the MI Branch Chief at PERSCOM, responsible for assignments and professional development for MI officers. He implemented accession standards to enhance the quality of the MI Officer Corps and ensured that MI officers filled key positions throughout the Army and DoD. He initiated a program on rating standards for MI leaders. Assigned as Chief, Combat Support Arms Division, he managed 25,000 officers in the MI, Engineer, Signal, Military Police, and Chemical Branches.



From 1987 to 1989, COL Bartlett commanded the 205th MI Brigade, providing intelligence support to V Corps in Germany. 205th elements received Armywide recognition for excellence. He successfully led the brigade on the last major Reforger exercise. Selected to be Assistant Deputy Chief of Staff, Intelligence, for U.S. Army Europe, he managed intelligence activities in theater. He played a key role in providing all-source intelligence to Operation Desert Storm.

COL Bartlett then commanded the Foreign Science and Technology Center. His organization responded to critical intelligence requirements for a variety of users. He spearheaded the effort to form the National Ground Intelligence Center (NGIC) and ensured that NGIC was a command-designated position—always led by an MI officer.

COL Bartlett concluded a distinguished career in MI in 1994. His awards include the Legion of Merit (2 Oak Leaf Clusters), Bronze Star Medal, Meritorious Service Medal (5 Oak Leaf Clusters), Air Medal, Army Commendation Medal, Defense Intelligence Director’s Medal, Army General Staff Badge, Air Crewman’s Badge, Presidential Unit Citation, and various campaign ribbons.



The Military Intelligence Corps 2019 Hall of Fame Inductees

Colonel Daniel T. Morris, U.S. Army, Retired

COL Daniel Morris began his military career as an enlisted infantryman (draftee) and was commissioned through Officer Candidate School in 1971. His earliest intelligence assignments included S-2, 1/48 Infantry, and Commander of 856th Army Security Agency Company, 3rd Armored Division, in Germany. From 1979 to 1982, he was the force modernization planner and Military Intelligence (MI) Branch professional development officer, U.S. Army Military Personnel Center. Then, following 18 months as an intelligence and targeting officer for the Commander in Chief, European Command, Airborne Command Post in England, COL Morris was selected as chief of the unit's Standardization and Evaluation Section. Subsequently, he served as Chief of the G-2 Exercise Division, XVIII Airborne Corps.

From 1987 to 1991, COL Morris served consecutively as Executive Officer and Commander of the 519th MI Battalion (Tactical Exploitation) (Airborne), which he successfully deployed during Operation Just Cause in Panama and Operation Desert Storm in Iraq. In Panama, he deployed and operated the largest tactical interrogation facility in combat since Vietnam. During Desert Storm, COL Morris validated the concepts for the Corps' long-range surveillance capability, which conducted cross-border operations with an attached attack and lift helicopter element.

After attendance at the Naval War College and a year as the G-2, 7th Infantry Division, COL Morris was selected to be the Chief of the Joint Intelligence Center (JIC) at U.S. Central Command (CENTCOM) in 1993. He led the JIC to be the model for all modernized integrated database producers, integrated an imagery analysis element into the JIC, supported combat operations in Somalia, and set the conditions to make the organization a command instead of a center.

In August 1996, COL Morris became the Deputy Chief of Staff, Intelligence, for Army Special Operations Command. His partnership with the XVIII Airborne Corps G-2 and the 525th MI Brigade gave junior officers professional development opportunities not available within their own organizations. Additionally, his senior analysts served as guest instructors with the John F. Kennedy Center for Special Warfare, providing relevant and timely instruction to maximize intelligence community support of special operations.



COL Morris's final military intelligence assignment was J-2, U.S. Special Operations Command (SOCOM). He successfully fought to reinstate 40 Defense Intelligence Agency-funded analytic billets for the SOCOM JIC that had been previously cut and worked on a select team with the Central Intelligence Agency and Joint Chiefs of Staff to identify and recommend targets for then President Bill Clinton's consideration after the 1998 terrorist bombings in Kenya.

COL Morris retired from military service in July 1999, entered private business as a program manager, and then became president and chief executive officer of a small company. After September 11, 2001, he returned to the Department of Defense as a senior executive to serve 16 additional years, initially as CENTCOM's Deputy J-2 and then Executive Director, National Ground Intelligence Center.

His military awards and decorations include the Defense Superior Service Medal, Legion of Merit, Defense Meritorious Service Medal (1 Oak Leaf Cluster), Bronze Star, Meritorious Service Medal (3 Oak Leaf Clusters), Army Commendation Medal (1 Oak Leaf Cluster), Master Parachutist Badge, Aircraft Crewman Badge, and Expert Infantry Badge.





The Military Intelligence Corps 2019 Hall of Fame Inductees

Major Rene J. Defourneaux, U.S. Army, Retired (Deceased)

Rene Defourneaux was born in France in 1921 and immigrated to the United States in 1939. He volunteered for the U.S. Army in 1943 and, because of his French language skills, he was sent to the Military Intelligence Training Center at Camp Ritchie, Maryland, to become an interrogator. On completion, he was shipped to Londonderry, Northern Ireland, and then quickly transferred to the British Army's Special Operations Executive in London. After intensive training to conduct sabotage and subversion missions, as well as organize guerilla resistance, he was assigned to the Office of Strategic Services (OSS) but under the operational control of the British.

After PVT Defourneaux was chosen for a mission within German-occupied France, he was discharged from the U.S. Army and reported to Supreme Headquarters Allied Expeditionary Forces (SHAEF), where he was commissioned a second lieutenant by SHAEF Commander GEN Dwight Eisenhower. On the night of August 8, 1944, 2LT Defourneaux was dropped into France, mistakenly some 20 miles from the intended site, but eventually joined his group of resistance organizers. Operating behind enemy lines for several months, he personally destroyed the bridge of Saint-Thibault on the Loire River and tricked the Germans into blowing up another bridge, denying their use by German tanks to attack American Soldiers. Mission completed, 2LT Defourneaux returned to the United States, where he received the Silver Star for his actions in France.

In April 1945, the OSS selected 2LT Defourneaux for an assignment in the China-Burma-India Theater. On April 31, 1945, he flew from Calcutta, India, to Kunming in the far southeast part of China. By May 16, he was second in command of the eight-member Deer Team tasked to train guerillas in French Indochina. To hide his French roots, he went by the cover name Raymond Douglas. On July 28, Defourneaux and the Deer Team parachuted into a jungle camp near Hanoi to link up with the resistance group led by Ho Chi Minh and General Vo Nguyen Giap. Their mission was to train the group for guerilla operations against the Japanese and to collect intelligence for use against the Japanese in the waning days of World War II. After the war in the Pacific



ended, Defourneaux again returned to the United States and was discharged.

In November 1947, Defourneaux was recalled to active duty and assigned to the Counter Intelligence Corps (CIC). He had assignments with the 109th CIC Detachment in Maryland, the 66th CIC Detachment in Germany, the 500th Military Intelligence Group in Japan, the 113th Intelligence Corps Group, and the Army Intelligence School at Fort Holabird, Maryland. Many of his foreign assignments in Europe and Asia, especially in the Pacific, were highly classified and are essentially unknown today.

Rene Defourneaux retired from the U.S. Army as a major in February 1965. In retirement, he wrote four books: *The Winking Fox*, *The Tracks of the Fox*, *The Raven Dropped His Cheese*, and *The Mark of the Buceros*. He passed away on April 1, 2010, and is buried in Arlington National Cemetery.





The Military Intelligence Corps 2019 Hall of Fame Inductees

Chief Warrant Officer 5 Stephen T. Kiss, U.S. Army, Retired (Deceased)

CW5 Stephen Kiss, a native of Budapest, Hungary, fought in the 1956 Hungarian uprising against the Soviet Union as a 16-year-old. After escaping Hungary, he enlisted in the U.S. Army in November 1958 under a law allowing the recruitment of foreign nationals. As a light weapons infantryman, he served with the 3rd Armored Division in Germany from 1959 to 1962.

Subsequently, CW5 Kiss put his Hungarian and Italian language skills to work for the 525th Military Intelligence (MI) Group and the 528th MI Company (Interrogation), providing interpreter-translator support to the Army and other federal agencies. After training and leading the Interrogation Prisoner of War Section of the 1st MI Company, 1st Infantry Division, at Fort Riley, Kansas, he deployed to Vietnam, where he led field interrogation teams during combat operations. He completed a Vietnamese language course and returned to Vietnam as senior interrogator for the 25th MI Company, 25th Infantry Division, and for the Combined Military Interrogation Center in Saigon.

In 1971, he served his first of several assignments at the U.S. Army Intelligence Center and School, Fort Huachuca, Arizona, where he was a senior instructor for interrogation approaches and questioning techniques. During later assignments to the schoolhouse, he revised the Basic Interrogator Course, developed the first Department of Defense Strategic Debriefer and Interrogation Course, and had overall responsibility for Intelligence Combating Terrorism, Counterdrug Analysis, Human Intelligence, and Counterintelligence courses.

CW5 Kiss's made his greatest contributions to MI during his many years in Germany. In 1973, he was attached to the 511th MI Battalion as the officer in charge of the Border Resident Office (BRO) in Cham, Germany. Under his leadership, BRO Cham became the most productive screening and collection office along the German-Czechoslovakian border. At the behest of successive battalion commanders, CW5 Kiss remained in this assignment for nearly 7 years. In 1983, CW5 Kiss served as the deputy representative to



the German Federal Agency for Recognition of Refugees for the Deputy Chief of Staff for Intelligence (DCSINT), U.S. Army Europe (USAREUR). With his mastery of the German language, culture, and bureaucracy, he developed and sustained successful relationships with German federal, state, and MI organizations for the next 10 years.

CW5 Kiss's last active duty assignment was as the counterintelligence/human intelligence advisor to the DCSINT, USAREUR, from 1996 to 2002. He provided input to every action involving counterintelligence/human intelligence collection, analysis, doctrine, policy, organization, training, and material issues. He also deployed to Bosnia, Kosovo, and Macedonia as a member of the USAREUR Intelligence Lessons Learned Team.

CW5 Kiss retired in 2002 after 43 years of active service. He then served with the MI Civilian Excepted Career Program until his death in February 2008. CW5 Kiss's military awards include the Legion of Merit, Bronze Star, Meritorious Service Medal (3 Oak Leaf Clusters), Joint Service Commendation Medal, Army Commendation Medal (5 Oak Leaf Clusters), Army Achievement Medal (1 Oak Leaf Cluster), and Good Conduct Medal (2 Oak Leaf Clusters).





The Military Intelligence Corps 2019 Hall of Fame Inductees

Mr. Maurice J. Sheley, Master Sergeant, U.S. Army, Retired, Department of the Army Civilian, Retired (Deceased)

Maurice J. Sheley enlisted in the U.S. Army in 1967 and served 10 years as a supply specialist/radar operator with two tours in Vietnam, before serving an additional 10 years as a counterintelligence (CI) agent. He retired as a master sergeant in 1987.

Mr. Sheley then became a Department of the Army Civilian and, for the next 27 years, served in various positions within the U.S. Army Foreign Counterintelligence Activity (FCA). He was first assigned as a team chief and then Chief of the Counterespionage Section in the Wurzburg, Germany, Field Office, 511th Military Intelligence (MI) Battalion, 66th MI Group. Reassigned to the Special Operations Section, he remained in Wurzburg conducting offensive counterintelligence operations (OFCO) until 1994, when the OFCO effort was consolidated in Munich as Detachment 15. Mr. Sheley then served as a case officer and assistant team chief on Detachment 15's Team Hercules, one of the most successful OFCO teams in the history of CI operations. While many of his operations remain classified, Mr. Sheley's operational exploits helped ensure the United States maintained a strategic advantage over its adversaries during and after the Cold War.

After serving as the Deputy Director of FCA from 1999 to 2001, Mr. Sheley became the operations officer of Detachment 14 at Fort Meade, Maryland. He refined the OFCO craft into a viable capability against nontraditional or asymmetric target sets. His operations and investigations were responsible for both the exploitation and/or neutralization of entire espionage networks targeting the U.S. Army and the Nation. While serving as the operations officer for the U.S. Army Special Investigations Detachment from 2009 to 2012, Mr. Sheley oversaw the successful investigation and prosecution of SPC William Millay for espionage, resulting in Millay's 16-year prison sentence. These results and his expertise in ensuring them won Mr. Sheley and his team the prestigious Department of Defense (DoD) CI Investigations Award for 2011. In his final position at FCA, Mr. Sheley's operational successes resulted in his team receiving the National Counterintelligence Executive Operations Award and two DoD CI awards in 2012.



Mr. Sheley also had significant accomplishments outside of FCA. In 1997, he managed a wide variety of critical and highly sensitive special access programs while assigned as the U.S. Army Intelligence and Security Command's Chief of the Special Programs Office. In 2004, he served as the Army G-2's liaison to the National Security Agency and was then called on to serve as a contributing agent in the Abu Ghraib Task Force. In 2007, he was tasked by Army leadership to revive the Pacific Liaison Detachment, which had been operationally shut down prior to his arrival.

Upon his retirement in 2014, Mr. Sheley was widely recognized throughout the intelligence community as one of the most successful CI case officers. In addition to the team awards already mentioned, his Civilian awards include the Meritorious Civilian Service Award, Commander's Award for Civilian Service, Achievement Medal for Civilian Service, and MI Corps Knowlton Award. Mr. Sheley passed away on August 20, 2016.



TRADOC CULTURE CENTER

TRAINING AND EDUCATION



Mission Statement: Established in 2004, TCC provides relevant and practical cross-cultural competency training and education IOT build and sustain an Army with the right blend of cross cultural competencies to facilitate the full range of military operations, now and in the future.

Culture Center
on-line @

<https://atn.army.mil>



Available Training: TCC provides training in foundational cross-cultural competencies, regional expertise and other practical topics such as cross cultural negotiations and leader engagement.

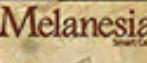
Cross-Cultural Competence Skills Topics:

- Self Awareness and Perspective Taking
- Cross-Cultural Communications
- Use of Interpreters
- Rapport Building

Regional Expertise:

- AFRICOM, CENTCOM, EUCOM, NORTHCOM, PACOM, SOUTHCOM
- Smart Cards and other Graphic Training Aids are also available

Smart Cards



60+
AOs
Covered

Pre-Deployment Training:

- SFAB/RAF deploying units
- Named Operations deploying units

Request Training

ATRRS

Course Number:
9E-F36/920-F30(CT-MTT)

The Training Circulars (TCs) for Military Intelligence Training Strategy (MITS)
Tier 3 and Tier 4 may be downloaded from—



APD | ARMY PUBLISHING
DIRECTORATE

1. The Army Publishing Directorate at <https://armypubs.army.mil/>,
then - Publications - Doctrine and Training -Training Circulars

-or-



Directorate of Training

Customer Focus | Products & Outreach | Development & Integration | Educational Design & Development | Training the Team

2. The Intelligence Knowledge Network (IKN) at <https://ikn.army.mil/apps/dot> select "MI Training Strategy (MITS)" link on the left side of the page.

Select "Links" under the MITS banner at the top of the page to access-

- MITS/USAICoE DATE 3.0 Evaluator's SmartBook
- MITS for the BCT Tier 3, TC 2-19.403
- MITS for the BCT Tier 4, TC 2-19.404

FIELDING A TRAINED AND READY ARMY INTELLIGENCE TEAM



TO SUPPORT MULTI-DOMAIN OPERATIONS