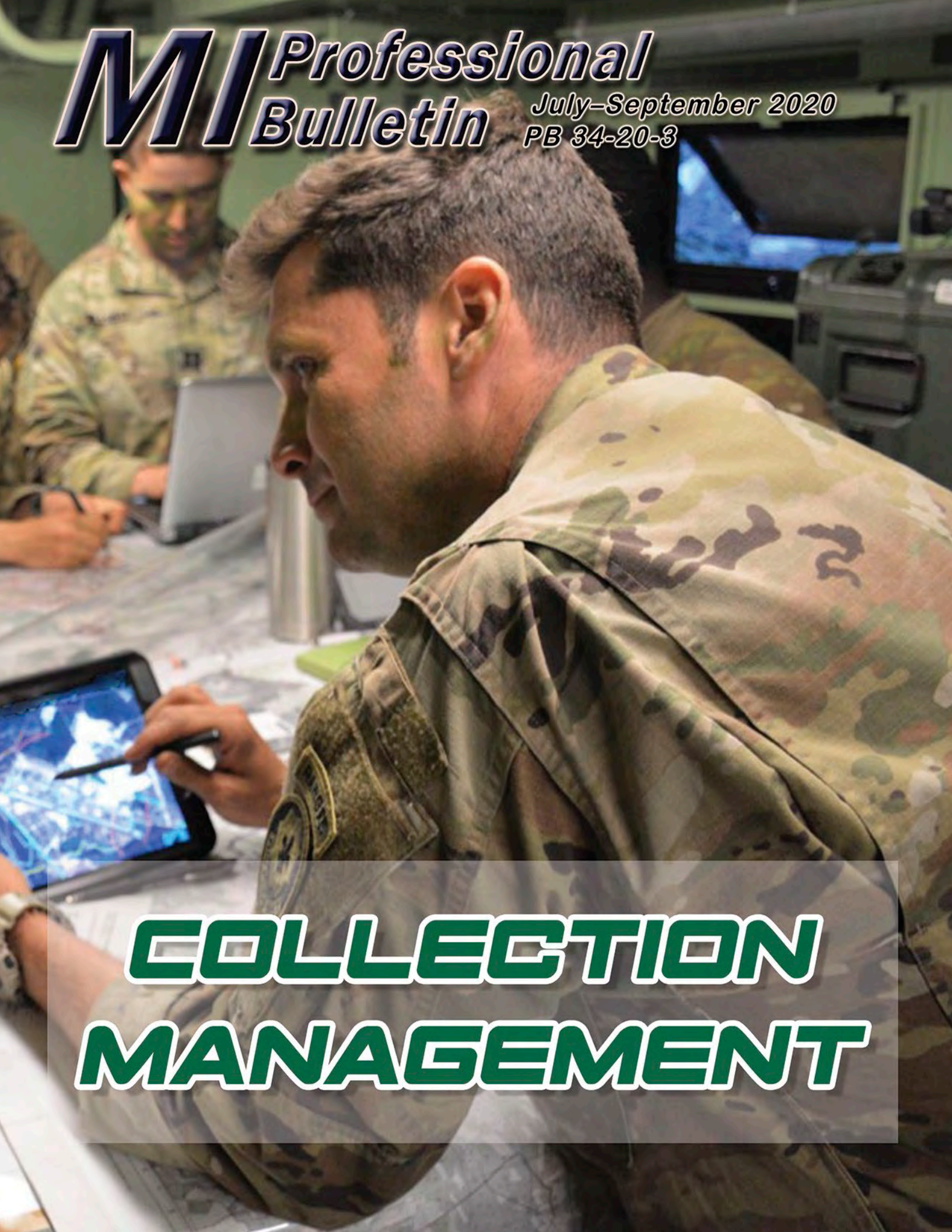
MI Professional Bulletin
July–September 2020
PB 34-20-3



COLLECTION MANAGEMENT

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

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:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
2029702

From the Editor

The following themes and deadlines are established:

April–June 2021, *Intelligence Support to Information Warfare.* This issue will focus on the intelligence operations and activities that enable windows of opportunity in the information environment and cyberspace. Deadline for article submission is 4 January 2021. **This is a change from the previously published article deadline for this quarter.**

July–September 2021, *Theater Intelligence Operations.* This issue will focus on theater army-level, regionally focused intelligence capabilities and operations supporting Army and joint forces across the specific regions. Deadline for article submission is 2 April 2021.

Although MIPB targets quarterly themes, you do not need to write an article specifically to that theme. We publish non-theme articles in most issues, and we are always in need of new articles on a variety of topics.

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

MI Professional Bulletin

July–September 2020
PB 34-20-3
Volume 46 Number 3

We would like to thank CW3 Omar DeLeon, Intelligence-Capabilities Development and Integration Directorate, U.S. Army Futures Command, for his time, knowledge, and support as this issue's "stakeholder." His assistance was key to obtaining some of this issue's diverse content.

Future of Army Intelligence

Collection Management

DEPARTMENTS

Inside back cover: Contact and Article Submission Information

Always Out Front

by Lieutenant General Laura A. Potter
Former Commanding General
U.S. Army Intelligence Center of Excellence
from 19 July 2019 to 11 August 2020

Since I took command almost a year ago, the Army Intelligence team has taken many steps to better train and prepare the Military Intelligence (MI) Corps to provide intelligence support to large-scale ground combat operations and multi-domain operations across all echelons. In the October–December 2019 issue of *Military Intelligence Professional Bulletin* (MIPB), I emphasized how our all-source intelligence training, professional military education, doctrine, and perspective must change to meet the demands of the Army's modernization efforts. Since then, we have identified and tackled many challenges across the various facets of intelligence training, support to readiness, and modernization. Our institutional training units have revised their curricula to train, evaluate, and rigorously prepare our MI Soldiers for the challenges of creating timely, relevant, accurate, and purpose-built intelligence. Now, MI Soldiers are better prepared to provide sound analytic judgments and advice to our operational commanders, operational staffs, and the larger intelligence community.

This quarter's MIPB is dual themed. The primary theme focuses on collection management, which has been another focal point for Army intelligence. As a critical part of the intelligence process, collection management underpins the intelligence warfighting function and results in answers to the commander's priority intelligence requirements. Collection management is a challenge at all echelons and involves the integration and synchronization of all reconnaissance, surveillance, intelligence operations, and security operations units and assets. This challenge will become more significant because of increasingly sophisticated peer and near-peer threat capabilities, inherently complex operational environments, and high-paced multi-domain operations.

The secondary theme for this MIPB issue concentrates on topics resulting from the 2020 Intelligence Senior Leaders Conference. The subjects focus on creating a shared vision of future operational environments, systems modernization, and human capital affecting the present and future of the MI Corps. The U.S. Army Intelligence Center of Excellence (USAICoE) plays a significant role in this by informing and ensuring development, innovation, and technological progression to meet the requirements of Army 2028 and beyond that are central to supporting this theme.

In this MIPB issue, you will read two articles by authors assigned to the U.S. Army Futures Command at USAICoE that provide a look into several possible advancements and outcomes. The first, by Mr. Mark Wallace, envisions what Army intelligence support to warfighting will look like now and through 2038. The second article, by CPT Michael Kossbiel, discusses Army, Department of Defense, and coalition initiatives related to collection management and sensor management supporting multi-domain operations capable forces.

You will also read articles filled with best practices, lessons learned, and other points to consider from organizations overcoming collection management training gaps and obstacles. For example, the article by MAJ Denn, MAJ Turner, and CPT Wojciechowski provides insight from the Joint Multinational Readiness Center and identifies several challenges that brigades must address.

MAJ Thornton's article offers a U.S. Army Forces Command perspective on the issue of collection management. MAJ Thornton describes how the Army must plan and prepare for transitions in the complex environments of multi-domain operations and large-scale ground combat operations. He illustrates how our collection managers must be able to jump main command posts while ensuring the tasking, collection, processing, exploitation, and dissemination of timely and accurate information to warn, enable decisions, and drive operations.

We are grateful for the unprecedented number of articles submitted over the past few months, which allowed us not only to develop this quarter's issue but also to provide content for a new web-based capability called Vantage Point. Scheduled to be launched in the near future, Vantage Point will offer the timely publication of articles containing practical solutions to current intelligence challenges. And unlike MIPB, it will be a venue to discuss the authors' ideas and to share experiences and recommendations.

Overall, the articles in this quarter's issue contain a number of recurring subthemes, including the challenges of collection management at echelon corps and below (ECB), challenges I can relate to on a personal level. In 2001, a month before the September 11 attacks, I arrived from the Command and General Staff College to take over as the V Corps collection manager. Shortly after 9/11, V Corps began planning the invasion of Iraq, which included a wet gap crossing of the Euphrates. Throughout that time period, I witnessed firsthand the incredible complexities of collection management. From that experience, I know that the collection manager must thoroughly understand the enemy situation and, equally important, be deeply involved in Army and joint intelligence and operational planning in order to facilitate mission accomplishment. The key to successful completion of this endeavor is rigorous preparation in a dynamic, complex environment.

In the past year, we have taken and continue to take significant steps to improve collection management across doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). For example, based on the Department of the Army G-2's bottom-up review, USAICoE and the U.S. Army Futures Command (specifically the Intelligence-Capabilities Development and Integration Directorate) conducted a deliberate DOTMLPF assessment to identify existing collection manager (Q7 billet) authorizations for retitling and recoding at ECB.

The assessment identified that only 25 percent of collection manager billets reside at the brigade combat team (BCT) MI company, division, and corps levels. In addition, the majority of Q7-coded billets at the BCT MI companies, divisions, and corps are aligned to single-source analysts, not the collection management sections. As a result, the current modified table of organization and equipment does not properly allocate and align collection managers at ECB, which affects our MI staffs' ability to conduct requirements management, align information collection capabilities with requirements, and assist the G-3/S-3 with tasking the right units and assets to conduct collection.

To address these gaps, we are pleased to report that in fiscal year 2021, collection management billets will increase within our BCT, division, and corps formations. These changes will—

- Increase the experience and expertise to leverage information collection capabilities supporting multidomain operations and large-scale ground combat operations.
- Maximize the use of MI military occupational specialties at echelon to build redundancy.
- Increase collection management interoperability and cooperation.
- Increase substantially the number of Q7 billets and corresponding institutional training.

We all know that change is constant, and we must continue to adapt and modernize the intelligence warfighting function to meet the challenges inherent with the Army's focus on large-scale ground combat operations and multidomain operations. By bridging the gaps in collection management, the MI Corps will continue to drive operations, remain effective and efficient, and strengthen our Army's lethality. However, there are myriad other challenges that together we, as the Army Intelligence team, still need to overcome. I am confident in the strength, dedication, and ingenuity of the MI Corps.

Always Out Front!

Always Out Front

by Brigadier General Anthony R. Hale
Commanding General
U.S. Army Intelligence Center of Excellence
Assumed Command on 11 August 2020

Taking command of the U.S. Army Intelligence Center of Excellence is the privilege of a lifetime, and joining the dedicated professionals currently shaping our future is an honor. My 30 years of service have focused on operationalizing intelligence for the warfighter, and I've conducted that effort at every echelon across U.S. Army Forces Command, U.S. Special Operations Command, and U.S. Army Intelligence and Security Command. Now at the U.S. Army Training and Doctrine Command, I see countless opportunities to directly influence the warfighter and our Army in a way that is inaccessible to most within Army Intelligence.

LTG Potter, thank you for your tireless dedication to the Military Intelligence Corps and Fort Huachuca. The strength of our corps is a direct reflection of your leadership and of your passionate drive for the modernization we need. Additionally, I truly appreciate how you carefully protected the health of our Soldiers and civilians during the uncertainty of the coronavirus disease 2019 pandemic. I wish you, Randy, Jack, and Rob nothing but the best as you continue your service to our great Nation.

Our priority continues to be building a stronger Army to keep our Nation safe against emerging peer threats and continued asymmetric threats. Our primary objectives to achieve this end state are to *Build Leaders* and *Drive Change* while continuing to inform our Soldiers, our Nation, and our adversaries of our abilities and prowess. I'm excited to see our Soldiers in training, to support modernization efforts, and to continue to improve our foxhole. Desert-6, signing on.

Always Out Front!

Normal Programmed Doctrinal Projects

- ATP 2-19.1, *Echelons Above Corps Intelligence,* in revised final draft staffing.
- ATP 2-19.4, *Brigade Combat Team Intelligence,* adjudicating final draft staffing comments.
- ATP 2-22.4, *Technical Intelligence,* in final draft staffing.
- ATP 2-22.6, *Signals Intelligence,* starting early stage of development.
- ATP 2-22.7, *Geospatial Intelligence,* starting early stage of development.

Surge/Critical Doctrinal Projects

- ATP 2-01, *Collection Management,* in final draft staffing.
- TC 2-19.01, *MI Company & Platoon Reference Guide,* expect publication in mid-December 2020.
- Intelligence portions of FM 3-60, *Targeting,* provided final draft comments to Fires Center of Excellence.
- Long-term following publication of FM 3-60: new ATP on Intelligence Support to Targeting.

How You Can Help

- It's your doctrine, so participate in the development process.
- Contact the Doctrine Team to provide feedback.
- Doctrine mailbox: usarmy.huachuca.icoe.mbx.doctrine@mail.mil

CSM Forum

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

Most everyone has heard that military intelligence (MI) enlisted assignments are being managed differently this year as part of a pilot program using the Assignment Satisfaction Key Enlisted Marketplace (ASKEM). The new Enlisted Manning Cycles and ASKEM will offer more predictability, transparency, and talent management into the assignment process. However, a great deal of misinformation about the program is still circulating. I hope I can untangle the discussion so that we can speak with one voice about the program.

We all knew that some form of the Marketplace and Assignment Interactive Module Version 2.0 designed for the officer cohort would eventually be implemented for the enlisted force; however, the Army will not manage officer and enlisted assignments in the same way. The ASKEM pilot program provides a chance to see what is in the realm of possibility, considering that we have a lot more enlisted personnel than the officer/warrant officer cohorts.

For now, ASKEM applies only to active component staff sergeant to master sergeant/first sergeant. These noncommissioned officers (NCOs) will receive a year and month of availability for assignment (YMAV) that is set at 36 months from the time the individuals arrive at their units. All personnel within the YMAV will be grouped into manning cycles based on that date, which will allow the impacted NCOs to see what options are available during that movement period. This YMAV will give the Soldier and units more predictability as to when individuals are eligible for assignment and should positively affect mission and career management. This does not mean that NCOs will automatically be placed on assignment at 36 months, nor does it mean that all NCOs will remain on station for 36 months, because Army requirements may dictate out-of-cycle moves. Additionally, units will maintain their ability to submit personnel requests for stabilizations, deferments, deletions, etc., just as in the past.

Once identified as movers, NCOs will be able to see, and preference, all available assignments for their military occupational specialty and grade during their movement cycle. NCOs will also be able to provide information to their branch manager for consideration during the assignment process. As part of this pilot, the Army has already identified several NCOs throughout the MI force and provided them instructions to complete their assignment selections in ASKEM. A key point is that ASKEM will not be the same process as for officers because it does not include interviews, unit input, or assignment to specific paragraph/line numbers; and Human Resources Command (HRC) will not consider by-name requests. It is also important to understand that branch managers must fill every position in their movement cycles regardless of NCO preferences. As an example, if the majority of the moving-eligible population preferences one location and no one preferences another location, branch managers will fill both locations in accordance with manning guidance and professional development models. Additionally, when an available mover is unable to proceed on assignment, the MI Branch will have to reach into their bench and possibly move someone out of cycle to fill requirements.

This program has a key pro and key con. The pro is the potential to provide continuity to a particular mission. The con is NCOs will not know exactly what position they are preferencing. They will focus only on locations rather than trying to find developmental opportunities for their career progression. Regardless, this is an opportunity for leader engagement. It will be crucial for senior leaders to assist our NCOs in understanding the overall process and the outcomes of their decisions. Lastly, please remember this is a pilot program that the Army will refine over time. For more information, HRC's video may help answer some questions: https://www.youtube.com/watch?v=bOI3exqfvzk&feature=youtu.be.

My sincere thanks to MSG Torre, MI Branch NCOIC, for assisting with the information for this column.

Always Out Front!

Technical Perspective

by Chief Warrant Officer 5 David J. Bassili
Former Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence
from 9 July 2018 to 25 June 2020

Hello again and farewell, teammates. This is my final contribution to the *Military Intelligence Professional Bulletin* (MIPB) before I fade away into retirement. I promise not to get overly sentimental or nostalgic, but instead I intend to focus on you, the cohort.

Over the last two years, our cohort (YOU) have made significant strides in ensuring the intelligence warfighting function wins in future large-scale ground combat operations. You have operationalized the Military Intelligence Training Strategy, ensuring Army commanders understand intelligence readiness needs and producing trained Soldiers and crews of intelligence professionals across the force. You contributed immeasurably to the test and evaluation and full implementation of Capability Drop 1—the first leg of our next-generation foundational layer weapon system—and you continuously seek ways to broaden its employment across echelons. You have established near-irreversible momentum for the Digital Intelligence Systems Master Gunner course by expanding the conduct of Gunner Entry Programs and exposing increasing numbers of Soldiers, noncommissioned officers (NCOs), officers, and fellow warrant officers to this key combat multiplier program. These are but a handful of the numerous efforts the cohort encountered and enabled to succeed for commanders at all echelons. In this list, I also need to include our response to the coronavirus disease of 2019 (COVID-19) pandemic. We ought to view the current COVID-19 environment in the same context as every other obstacle that stands in the way of mission accomplishment…warrant officers adapt and overcome…and this time is no different.

The future is now, and the demands will all change. You will continue to support the test and evaluation and fielding of additional future capabilities, namely the Terrestrial Layer System, Tactical Intelligence Targeting Access Node, Multi-Domain Sensing System, and Capability Drop 2. You will stand up new tactical division intelligence formations and build capacity in multi-domain task forces. You will contribute to the changing nature of how the Army will fight in large-scale ground combat operations and converge multi-domain capabilities that provide strategic advantage and create multiple dilemmas for our peer competitors. You will navigate your career and professional development in a modernized, 21st century talent management-based personnel system tailored specifically to warrant officers. You will do all of this and more, and I know you will be successful because that is exactly what generations of warrant officers before you have done. You are experts in balancing requirements with too few resources, a fact that lends itself directly to the focus of this quarter's MIPB—collection management.

ADP 2-0, *Intelligence,* tells us that our intelligence core competencies serve as the areas that all military intelligence units and Soldiers must continuously train on to maintain a high degree of proficiency. Collection management ties directly to the core competency of intelligence synchronization—the art of integrating information collection; intelligence processing, exploitation, and dissemination; and analysis with operations to effectively and efficiently fight for intelligence in support of decision making. The key word in that definition is ***art***. It takes more than systematic instructions of how to be a collection manager. It requires a deep understanding of the threat, an expert understanding of our collection systems, and a professional understanding of all Army operations. Collection management is not an individual sport, and it never has been. Our current challenge focuses most significantly at the brigade combat team, where no collection manager billet exists. But in my opinion, that is only symptomatic of the real problem. The vast majority of our mid-career NCOs, officers, and warrant officers have minimal practical experience in conducting collection

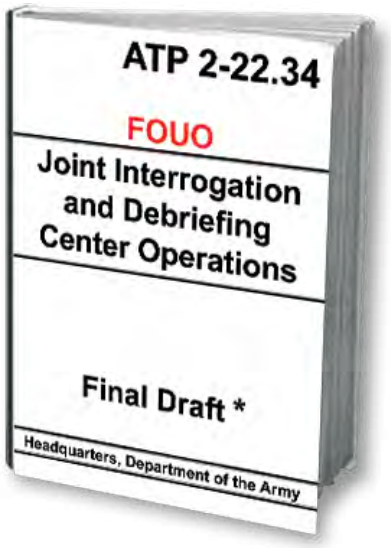
management tasks in the threat environments we currently train. We became comfortable with a "standing deck" of near-persistent intelligence, surveillance, and reconnaissance coverage that could "react to contact" instantaneously.

We, the Army, must refocus our efforts on the military decision-making process—specifically mission analysis and wargaming for large-scale ground combat operations. We have to relearn the importance of thinking in terms of time and space—latest time information is of value and phase lines—combined with the pace of operations against a peer competitor. Named areas of interest become decision points for collection managers: Which course of action is the enemy adopting? Do I need to shift focus of an asset? This is an Army-wide challenge, not unique to the Military Intelligence Corps. Being a brigade combat team centric Army in counterinsurgency/counterterrorism for the last 20 years, which focused resources on downward reinforcing, requires time to change. Change is hard, but the Army is in the midst of generational change, and the cohort will be key in ensuring its success. This is not to say we are not currently learning and improving. This quarter's MIPB contributors offer insights and tips of how you too can do just that. In addition to these articles, I encourage you all to read FM 3-55, *Information Collection,* and if you are really interested in a historical perspective, hunt down a copy of FM 34-2-1, *Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance* (1991), or FM 34-2, *Collection Management and Synchronization Planning* (1994).

In closing, I would like to reiterate my original sentiment from two long years ago. I was truly humbled to serve in this capacity and to represent the current and future interests of our cohort to Army senior leaders. We are who we are as a cohort based on the individual successes (and failures) of each one of us. CW5 Aaron Anderson will bring renewed energy, imagination, drive, and innovation to the position, further improving and taking the foxhole that is our cohort to new heights. Thank you all for the support and your individual dedication to our craft and to our Army. Stay safe, remain calm, and Soldier on!

Always Out Front!

ATP 2-22.34, *Joint Interrogation and Debriefing Center Operations*



ATP 2-22.34, *Joint Interrogation and Debriefing Center Operations,* discusses doctrinal techniques and procedures used to manage and conduct intelligence operations in a joint interrogation and debriefing center (JIDC) by Department of Defense (DoD) human intelligence (HUMINT) and other support personnel. The JIDC concept was developed to meet operational requirements while always adhering to U.S. and international legal parameters associated with interrogating detainees, as well as protecting detainees' rights, safety, health, and well-being. As the largest and primary force provider of HUMINT collectors in the DoD, the Army established the military intelligence (MI) battalion (interrogation) to conduct JIDC operations. ATP 2-22.34 supersedes TC 2-22.304, *Military Intelligence Battalion (Interrogation),* dated 3 August 2009.

ATP 2-22.34 complements existing doctrine, particularly FM 2-22.3, *Human Intelligence Collector Operations,* and incorporates lessons learned and best practices from recent operations and subject matter experts worldwide. ATP 2-22.34 is for commanders, staffs, Soldiers, and Department of the Army (DA) Civilians assigned to an MI battalion (interrogation) or Soldiers and DA Civilians augmenting or supporting a JIDC.

Technical Perspective

by Chief Warrant Officer 5 Aaron Anderson
Chief Warrant Officer of the MI Corps
U.S. Army Center of Excellence
Change of Responsibility occurred on 25 June 2020

Teammates,

What an honor and a privilege it is to serve as your 8th Chief Warrant Officer of the Military Intelligence (MI) Corps. As I consider this amazing opportunity, I would first like to thank all the great officers, warrant officers, noncommissioned officers, Soldiers, Department of the Army Civilians, and contractor partners who mentored, coached, and supported me along my journey. I look forward to driving positive change and tackling, head-on, the challenges associated with transforming the Army and our MI Corps from a force highly skilled and lethal at executing counterinsurgency operations to one trained and ready to execute large-scale combat operations in a multi-domain environment.

I would be absolutely remiss if I did not take this opportunity to publicly acknowledge my predecessor, CW5 Dave Bassili. CW5 Bassili's accomplishments and contributions to the MI warrant officer cohort are abundant. He advanced the cohort in several areas, including talent management, leader development, and warrant officer education. Dave, on behalf of the entire MI warrant officer cohort, both past and present, I offer you thanks for your leadership and service as the 7th Chief Warrant Officer of the MI Corps.

As I begin to settle into my new position, I would like to briefly address my initial goals and objectives. I will likely expand, or drill down, on several of these in future *Military Intelligence Professional Bulletin* (MIPB) columns. It is extremely important to me that my goals and objectives are nested and synchronized with those of the U.S. Army Intelligence Center of Excellence Commander. While these areas are certain to change over time, they represent an initial framework for focusing my time and energy. My intent is to build upon the strong foundation of efforts that were established over the last several years.

My initial goals and objectives fall into the following four lines of effort:

- Training/Education/Building Technical Depth
  - Build doctrinally focused, confident warrant officers capable of leading and winning in large-scale combat operations and multi-domain operations.
  - Reestablish warrant officer expertise and deep understanding of the threat.
  - Ensure warrant officer professional military education produces quality graduates who meet the needs of the force.
- Force Modernization/Force Management/Drive Change
  - Ensure MI warrant officers are at the cutting edge of testing and implementation of new systems (Capability Drop 2, Terrestrial Layer System, Multi-Domain Sensing System, and Tactical Intelligence Targeting Access Node) and technologies (artificial intelligence, machine learning, and data science).
  - Effectively engage in emerging force modernization initiatives to resolve current and future challenges.
  - Work closely with the Office of the Chief, Military Intelligence and all stakeholders to help shape future formations.
- Talent Management/Leader Development
  - Produce agile, adaptive, and innovative leaders who act with boldness and initiative.
  - Embrace and maximize opportunities afforded by Assignment Interactive Module 2.0 and mentor on its potential pitfalls.
  - Align warrant officer assignments to optimize experience and opportunity.

- Engage with the Army Talent Management Task Force on emerging and ongoing warrant officer initiatives and the Total Warrant Officer Study.

✦ Communication and Strategic Messaging

- Tell the MI warrant officer story (MIPB, public affairs office, opportunities, etc.).
- Increase the visibility of our cohort and maximize opportunities to increase recruiting.
- Build collaborative teams across all MI warrant officer specialties—across all three components.

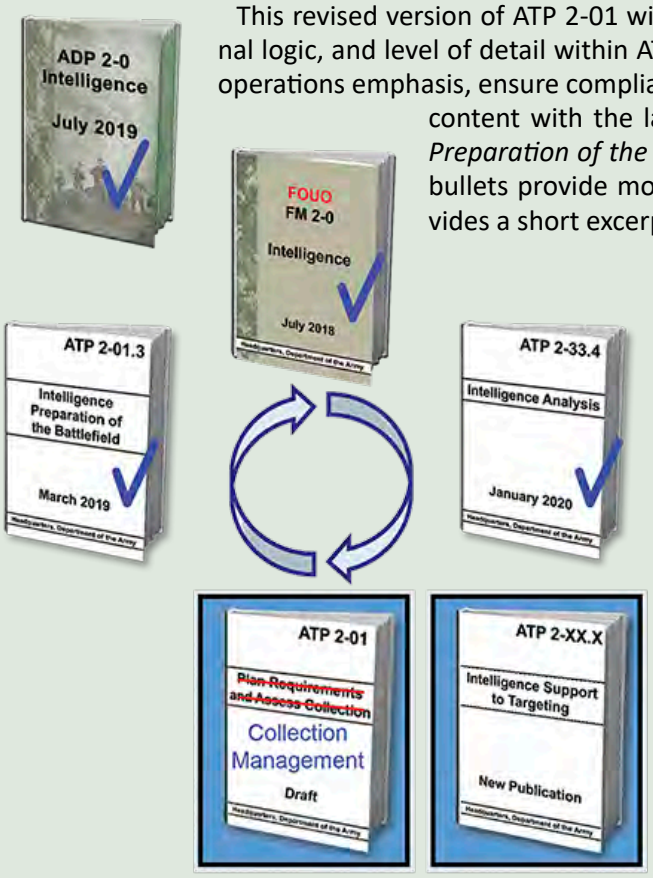
As I close out this column, I would again like to say that I am truly humbled and honored at this opportunity and the subsequent journey that awaits me. I would like to thank you and your families for your daily sacrifice, selfless service, and contributions to the Army in defense of our Nation. I wish you good health and safety as we continue to work through the impacts of this ongoing coronavirus disease 2019 pandemic.

Always Out Front! and Army Strong!

Doctrine Corner
ATP 2-01, *Collection Management*

In the last issue of *Military Intelligence Professional Bulletin,* we presented phase one of the intelligence doctrine modernization plan. The overall modernization plan will revise all Army intelligence doctrinal publications and is a result of the publication of FM 3-0, *Operations*, in October 2017. The first phase of this effort is the revision of our most fundamental publications, which includes ATP 2-01, *Collection Management*. Illustrated below is the status of phase one.

Since October 2019, the U.S. Army Intelligence Center of Excellence has been revising ATP 2-01. At the time of this article's creation (late September 2020), the writing team has initiated worldwide staffing of the final draft. The results of the staffing will drive subsequent timelines, but the intent is to publish the Army techniques publication in 2020 or as early thereafter as possible.



This revised version of ATP 2-01 will be significantly different. Beyond improving the clarity, internal logic, and level of detail within ATP 2-01, the writing team will add a large-scale ground combat operations emphasis, ensure compliance with current combined arms doctrine, and synchronize the content with the latest doctrine in FM 2-0, *Intelligence*; ATP 2-01.3, *Intelligence Preparation of the Battlefield*; and ATP 2-33.4, *Intelligence Analysis*. The following bullets provide more details on the revision of ATP 2-01, and the next page provides a short excerpt from the current draft (as of September 2020).

What is changing:

- Addition of a logic map.
- Standard chapter 1 discussions: peer threats, large-scale ground combat operations, multi-domain operations, Army strategic roles, and operational framework.
- Emphasis on the close relationship with intelligence analysis.
- Addition of the process step of "support tasking and directing."
- Successive linked graphics and example collection management products.
- Better discussions of targeting (with battle damage assessment) requirements—more explicit and detailed.
- Addition of chapters on collection management during Army strategic roles and large-scale ground combat operations.
- Addition of an appendix of "how to" checklists.

Excerpts from ATP 2-01, *Collection Management*

***Editor's Note: The following text is from Chapter 4 and Appendix E of the Final Draft ATP 2-01,* Collection Management.**

CHAPTER 4: DEVELOP THE COLLECTION MANAGEMENT PLAN

Collection Assets and Information Sources

Before evaluating collection assets, the collection management team must understand what collection assets and information sources are accessible during the information collection effort. Often, there are numerous collection requirements that are critical to a mission's success. Ultimately, this results in a unit covering a vast number of [named areas of interest] NAIs in order to answer those requirements. Therefore, every potential collection asset or information source is important. In addition to the large number of requirements and the desirability of redundant collection, peer threats will create difficulties for Army forces' collection efforts through air defense capabilities, electronic warfare, cyber capabilities, lethal fires, and counterreconnaissance efforts. To develop a creative and effective collection management plan, the collection management team must understand the following collection assets and information sources:

- ✦ Primary information collection assets.
- ✦ Ancillary information collection assets.
- ✦ Nonmilitary information sources.

Despite the complexities and time pressures involved in collection management, the team should think beyond primary information collection assets by including ancillary information collection assets and nonmilitary information sources to the collection management plan. Ancillary information collection assets and nonmilitary information sources are especially important during stability operations, urban operations, and operations in the consolidation area during large-scale ground combat operations. Each of the three categories has different characteristics that must be familiar to the collection management team and the rest of the staff to ensure effective information collection.

Primary Information Collection Assets. Primary information collection assets are those units and systems whose main mission is to perform one of the four primary means of information collection—intelligence operations, reconnaissance, surveillance, and security operations. Formerly, and even now, some documents refer to this group of assets as traditional collection assets. Primary information collection assets include but are not limited to—

Use of the Word *Source*

Do not confuse this common use of the word source with the [human intelligence] HUMINT term source—a person, device, system, or activity from which services or information are obtained (DCHE-M 3301.002).

- ✦ HUMINT collection teams.
- ✦ Prophet teams.
- ✦ Shadow unmanned aircraft systems (UASs).
- ✦ Cavalry units.
- ✦ Infantry units assigned reconnaissance missions.
- ✦ Engineer and chemical reconnaissance units.

The collection management team often evaluates these assets first in order to develop the collection management plan. While some level of collaboration is preferred before recommending that the G-3/S-3 task one of these units, less collaboration and level of detail are required to task primary information collection assets than ancillary information collection assets.

Ancillary Information Collection Assets. Ancillary information collection assets are those units and systems tasked to perform information collection while also performing another mission during the operation. Formerly, and even now, some documents refer to this group of assets as nontraditional assets. Ancillary information collection assets include but are not limited to—

- ✦ Target acquisition radars.
- ✦ Air defense system sites.
- ✦ Logistics convoys.
- ✦ A military police unit performing battlefield circulation.
- ✦ An attack helicopter battalion.

- A sniper team.
- A special operations force team (unless the team is performing strategic reconnaissance).
- Joint terminal attack controller.
- Fire support team.

The collection management team must conduct a high level of collaboration before recommending that the G-3/S-3 task one of these assets; this ensures the tasking is feasible. To ensure the required collection is successful, the tasking should also be detail-oriented since the assets may be unfamiliar with information collection techniques, and their [standard operating procedures] SOPs may not include these types of taskings.

Nonmilitary Information Sources. A nonmilitary information source is any cooperative and regular nonmilitary source that can provide reliable and important information to answer requirements. Nonmilitary information sources include but are not limited to—

- Intergovernmental and nongovernmental organizations.
- Elements of the private sector (any or all nonpublic or commercial individual and business, specified nonprofit organizations, most of academia, and other scholastic institution).
- Local and national foreign authorities.
- Other foreign persons of importance.
- Local hires.

The G-3/S-3 does not task nonmilitary information sources. The collection management team works through the G-9/S-9 to establish these agreements over the course of the operation. During stability operations, nonmilitary information sources are critical to operations because they have greater access to the local population and a better understanding of local sentiments. One technique that facilitates information sharing across these sources and friendly forces is the establishment of fusion centers. (See ADP 2-0 [*Intelligence*] for more information on fusion centers.)

APPENDIX E: ANCILLARY INFORMATION COLLECTION AND NONMILITARY INFORMATION SOURCES

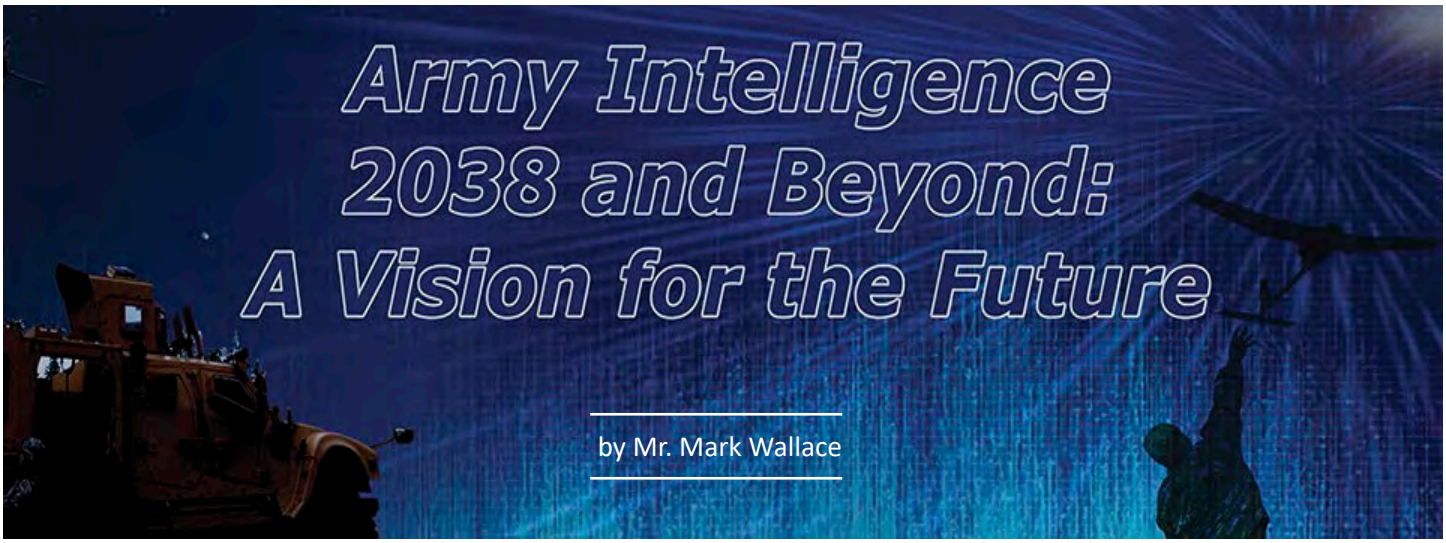
Broadening the Information Collection Effort

Collection management teams must often contend with many complexities, short time windows, and the need for extensive collaboration and coordination across echelons—both within the intelligence warfighting system and among all staff members. It is easy for teams to have a fixed mindset of tasking and requesting information from only primary information collection assets. However, as much as possible, the team should be creative and consider tasking ancillary information collection assets or creating agreements to obtain ancillary nonmilitary information. In some cases, ancillary information collection assets or nonmilitary information sources may be the only assets capable of fulfilling the requirement. Ancillary information collection assets and nonmilitary information sources are especially important during stability operations, urban operations, and operations in the consolidation area during large-scale ground combat operations.

Ancillary Information Collection Assets. Ancillary information collection assets exist across all echelons. Every Soldier must be ready to collect information properly and through the right channels during operations. The collection management team should collaborate with the corresponding staffing element and the G-3/S-3 before staffing an ancillary information collection asset. For example, the team coordinates with the engineer coordinator before tasking an engineer unit to observe an area adjacent to a river crossing site. Additionally, the collection management team and G-3/S-3 should be realistic when tasking the asset, especially when the asset has other tasks to perform.

Nonmilitary Information Sources. Obtaining information from nonmilitary sources is more difficult than tasking information collection assets. However, in some situations, such as stability operations, nonmilitary sources can collect invaluable information that is unavailable through military collection assets. Because the collection management team is dealing with nonmilitary personnel, there is no guarantee the team can obtain the information when needed. Therefore, maximum coordination and leadtime are necessary.

As intelligence professionals, you need to be proficient in the fundamental doctrine. The U.S. Army Intelligence Center of Excellence Doctrine Division also counts on you to provide feedback on doctrinal issues. If you need doctrinal assistance or have important feedback, please contact the Doctrine Division at usarmy.huachuca.icoe.mbx.doctrine@mail.mil.



Army Intelligence 2038 and Beyond: A Vision for the Future

by Mr. Mark Wallace

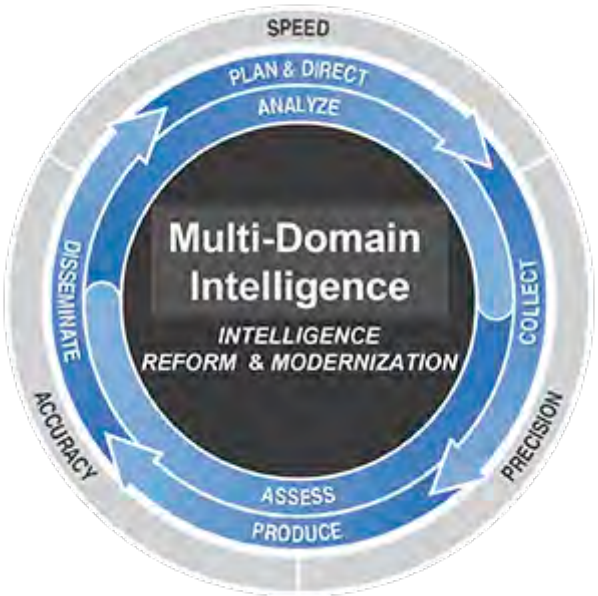
To ensure that the Army will be ready and can win in the future, we must also modernize…But to get to the Army we need in the future requires transformational change, not incremental improvements.

—GEN James C. McConville

This article assumes the successful implementation of the ideas in the Army's operating concept, TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* and anticipates technologically advanced near-peer adversarial countermeasures to those actions.[1] It will imagine the future, provoke thought, and describe how Army intelligence could support warfare beyond 2038. This article describes the current multi-domain operations (MDO) gap and the solutions Army intelligence is pursuing to close the gap. It then focuses on MDO implementation and analyzes potential modernization measures to remain relevant in the face of an evolving threat. Lastly, it describes a potential vision for Army intelligence, providing ideas for the future based on concepts, an assessment of intelligence core competencies, and potential solutions informed through experimentation using research and development and science and technology.

MDO-Capable Army Intelligence, 2020–2028: Near-Term Strategy

The U.S. Army Combined Arms Center completed a 2018–2019 study of large-scale combat operations, which identified the lack of echelons above brigade multi-domain deep sensing; analysis; and processing, exploitation, and dissemination (PED) capabilities to support long-range precision fires as gap 1 of 17 critical gaps. The nature of the emerging threat coupled with emerging technologies capable of delivering lethal and nonlethal fires at much greater ranges drives the requirement for sensors that can see at much greater ranges without latency. Army intelligence force modernization must help to close this critical gap.



Multi-Domain Intelligence[2]

Current organizational changes were designed to ensure military intelligence (MI) forces have the capabilities and capacity required at echelon to support MDO during large-scale combat operations against a near-peer competitor. The multi-domain task force contains a multi-domain MI company to support priority intelligence requirements and targeting with advanced capabilities to identify, locate, and track threat antiaccess and area denial capabilities across all domains at extended ranges. The Army redesigned the MI brigade-theater to increase capacity, doubling the watch section and all-source analysis teams and creating a new open-source intelligence cell. The expeditionary-MI brigade will provide multi-domain deep sensing, analysis, and PED for each division and corps rather than optimize for brigade combat team reinforcement. The Army also restructured the Army National Guard and Army Reserve expeditionary-MI brigades to better support echelons division and above. Finally, the brigade combat team MI company adds an

electronic warfare platoon, divides the multifunction teams into separate human intelligence and signals intelligence collection teams, and removes the company intelligence support teams: the counterinsurgency construct was not suitable for supporting large-scale combat operations.

Modernization priorities for Army intelligence materiel support MDO and long-range precision fires against a near-peer competitor through four major programs:

- **Tactical Intelligence Targeting Access Node (TITAN)** provides a scalable and expeditionary intelligence ground station that supports commanders. TITAN does this by leveraging space and high altitude, aerial, and terrestrial layer sensors to provide targeting data directly to fires information systems as well as multi-discipline intelligence support to targeting and situational understanding in support of command and control.
- **Multi-Domain Sensing System (MDSS)** will provide commanders with an agile, interoperable, and self-healing network of highly relevant and integrated sensors from low altitude to space. The MDSS will offer extended endurance over wide areas and denied airspace providing precision target location using multiple sensors in fluid environments.
- **Terrestrial Layer System** modernizes the terrestrial layer through a globally deployable intelligence, surveillance, and reconnaissance system containing signals intelligence, electronic warfare, and cyberspace operations capabilities.
- **Distributed Common Ground System-Army** will transition to applications on the command post computing environment after it upgrades capabilities from battalion through theater in the near term to improve data analytics.

MDO-Ready Army Intelligence, 2028–2035: Mid-Term Strategy

Operational environment assessments anticipate expanded effects of globalization in addition to competition with near-peer threats. It is a multipolar world, complicated with super-empowered individuals and non-state actors, hybrid capabilities, feral megacities with populations exceeding ten million, and hostilities below the threshold of war. Foreign adversaries conduct cyber espionage and technical operations against U.S. civil and military interests around the globe, and they continue to develop new and more effective capabilities in these areas. Readily available and advanced cyber and technical surveillance tools offer threat actors a relatively low-cost, efficient, deniable, and high-yield means of accomplishing their goals. The development of next-generation technologies, such as fifth-generation cellular communications technology, artificial intelligence, and quantum computing, present new opportunities for foreign entities to collect intelligence and conduct cyberspace operations against the United States and its allies.

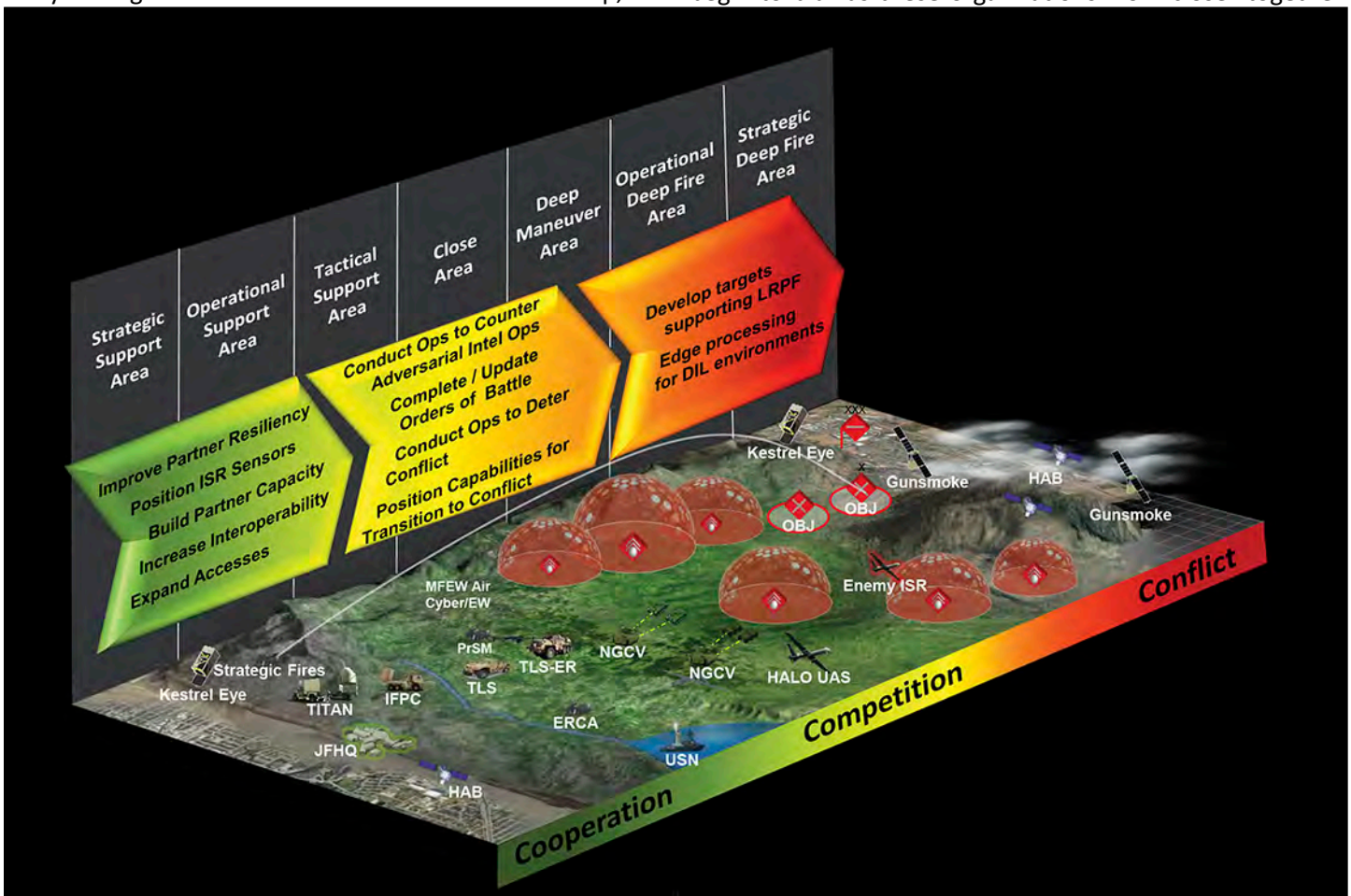
Near-peer military threats will develop and proliferate capabilities to counter the U.S. MDO strategy and to contest sanctuary. They will field a myriad of capabilities and manpower: armed drone swarms, long-range missiles and rockets with advanced munitions, autonomous unmanned vehicles, soldiers powered by exoskeleton technologies, special forces commando teams (possibly posing as refugees from sleeper cells that activate to disrupt domestic harmony), increased air and land mobility, and electronic warfare capabilities to jam satellites and digital and voice communications. Near-peer competitors will be on the verge of militarizing artificial intelligence, machine learning, block-chain, cloud-independent edge computing, and quantum computing capabilities. Combined together and synchronized during large-scale combat operations, these modernized capabilities form a potent counter to the U.S. Army's MDO strategy.

The Army and Department of Defense (DoD) must adjust if they are going to retain the military advantage. Similarly, the U.S. Government cannot sit idly by while DoD does all the heavy lifting. The evolution of MDO involves a comprehensive whole-of-government, allies, and private-sector partner approach. Realizing that foreign governments are threatening key and vital national interests short of war, the U.S. Government must synchronize a whole-of-government approach. The Director of National Intelligence must expand critical infrastructure information exchanges with federal departments and agencies; state, local, tribal, and territorial governments; private-sector partners; and allies. New analytic tools will improve threat warning and enable offensive and defensive operations. The U.S. Government must enhance capabilities to share best practices with partners—in the areas of threat, incident, vulnerability, risk data, and security.

Army intelligence must still provide timely, accurate intelligence support to inform commanders' decision making, leaving intact Army intelligence's core competencies: intelligence operations (collection), intelligence analysis, intelligence PED, and intelligence synchronization. It is certain that the Army MI Branch will not own all the friendly sensors on the battlefield—it does not today. All collection, including cyberspace, will seamlessly integrate into the overall information collection process. Open-source intelligence

and initiatives such as Every Receiver a Sensor and Artillery Delivered Intelligence, Surveillance, and Reconnaissance, using common data standards, will add to the "ocean of data" available to intelligence analysts. MI will continue to provide commanders with predictive intelligence based on modeling and simulation tools to get inside the enemy's decision cycle and make better friendly decisions. Analysis is an art and a science assisted by artificial intelligence and machine learning and driven by automation, robotics, and emergent technologies. PED, distributed and accessible, will evolve from a push construct to one of pulling. By 2028, Army intelligence will field automated tools to develop, integrate, and synchronize the collection plan, track sensor locations and status in real time, visualize available systems and gaps, and tip and cue appropriate sensors. Rapid technology advances will radically change *how* Army intelligence gets inside the enemy's decision-making cycle to provide friendly forces windows of superiority.

How the Army fights will change as the U.S. Government embraces a whole-of-government approach to synchronize capabilities across all domains, the electromagnetic spectrum, and the information environment. The lines between the Services and other branches of government will begin to blur as these organizations work closer together.



Space Layer
- National-to-tactical integrated platforms and sensors
- Small satellites and emerging/commercial technologies
- Army prioritization for targeting and collection

Aerial Layer
- Survivable, penetrating, high-altitude ISR
- Human-machine teaming
- Swarm and expendable ISR

Terrestrial Layer
- Human-AI teaming
- Integrated operations and intelligence
- User interfaces and experiences

Foundation Layer
- Degraded, intermittent, low-bandwidth data transfer
- Edge processing nodes and sensors

AI	artificial intelligence	IFPC	indirect fire protection capability	OBJ	objective
DIL	degraded, intermittent, low-bandwidth	Intel	intelligence	OPS	operations
ERCA	extended range cannon artillery	ISR	intelligence, surveillance, and reconnaissance	PrSM	precision strike missile
EW	electronic warfare	JFHQ	Joint Force Headquarters	TITAN	Tactical Intelligence Targeting Access Node
HAB	high-altitude balloon	LRPF	long-range precision fires	TLS	Terrestrial Layer System
HALO–UAS	high-altitude, long operation unmanned aircraft system	MFEW	multi-function electronic warfare	TLS–ER	Terrestrial Layer System-Extended Range
		NGCV	next-generation combat vehicle	USN	U.S. Navy

Operationalizing Multi-Domain Intelligence to Support Multi-Domain Operations

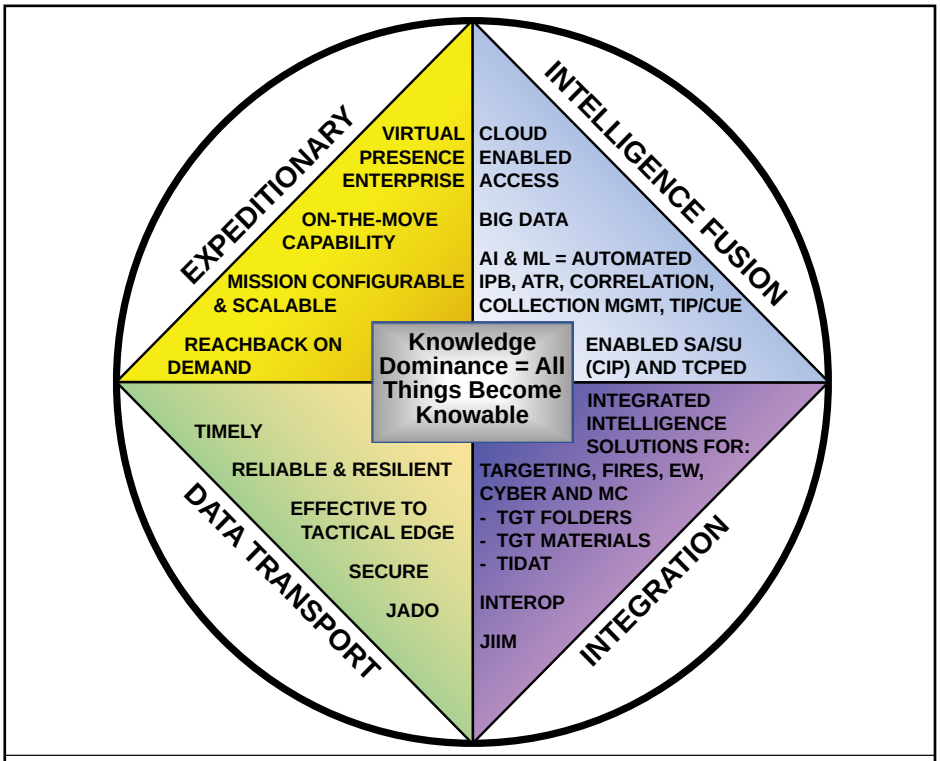
The ubiquitous nature of data, storage capacity, and accessibility will necessitate new rules and regulations governing who can access and share certain types of data and for what purposes. As doctrine evolves, Army intelligence will continue to tailor support to every echelon based on the supported unit's tasks and missions.

Army intelligence will develop materiel solutions that are scalable and tailorable to each echelon. A modular open system architecture will allow rapid technology insertion, especially in sensor design and fielding. Joint common data standards will normalize data and facilitate seamless integrated data sharing between sensors, shooters, and command and control nodes. Miniaturization will enable onboard sensor preprocessing and secure transmission. Artificial intelligence will speed analysis and support the military decision-making process, intelligence preparation of the battlefield, and collection management. Machine learning and natural language processing will enhance predictive analysis, deep data analytics, data sharing, and automated solution development. National functional managers such as the National Security Agency or National Geospatial-Intelligence Agency will have an increased role to improve the materiel development process, creating a next generation of sensors across all observable spectrums and in cyberspace.

Talent management must keep pace with innovation. Through early and often assessment of technical and leadership skills, the Army can implement several initiatives. Separate leadership and technical tracks will align the appropriate Soldier with assigned duties. Training will support new career fields such as data scientists, decision analysts, data managers, and ethical hackers. While initial entry Soldiers will still attend basic and advanced individual training in their respective branch training centers, virtual and online classrooms will provide professional military education after initial assignments. A step-increase program will help recruit and retain highly skilled and trained Soldiers, while regimental assignments will ensure regional continuity and develop cultural expertise. All-source analysts should transition to "decision analysts," mechanical translators will assist linguists, and contractors will add technical know-how. The Army should create a career field for cyberspace counterintelligence to enhance technical security, assess friendly vulnerabilities, defend against hybrid attack methods, and detect insider threats. Human-machine interface and virtual reality will enhance human performance but may bring with them unforeseen mental and physical issues.

Beyond MDO-Ready Army Intelligence, 2038 and Beyond: Far-Term Strategy

The operational environment of 2038 will be significantly different from the early 2030s as adversaries aggressively challenge U.S. overmatch. Nation states will likely form new alliances for survival, super-empowered individuals will threaten stability and international norms, and lines between government and business will become blurred. The threat is not constrained; it lives in a digital world without boundaries. The U.S. Government needs to be mentally and technically prepared to address these threats. Large-scale combat operations against a near-peer competitor remains the worst case scenario for the U.S. military, and nuclear proliferation is still a menace. Highly advanced adversaries will continue to develop methods to transcend U.S. strengths in traditional fire and maneuver capabilities across



AI	artificial intelligence	MC	mission command
ATR	automatic target recognition	MGMT	management
CIP	common intelligence picture	ML	machine learning
EW	electronic warfare	SA/SU	situational awareness/situational understanding
INTEROP	interoperability	TCPED	tasking, collection, processing, exploitation, and dissemination
IPB	intelligence preparation of the battlefield		
JADO	joint all-domain operations	TGT	target
JIIM	joint, interagency, intergovernmental, and multinational	TIDAT	target intelligence data

Knowledge Dominance

domains while disrupting access to space, the electromagnetic spectrum, and most significantly the cyberspace domain, all across a vastly extended area of operations. Adversaries will also use multi-domain economic and information warfare throughout the operational continuum to gain advantage, achieve decisive effects, shape domestic and international sentiment, and influence decision makers.

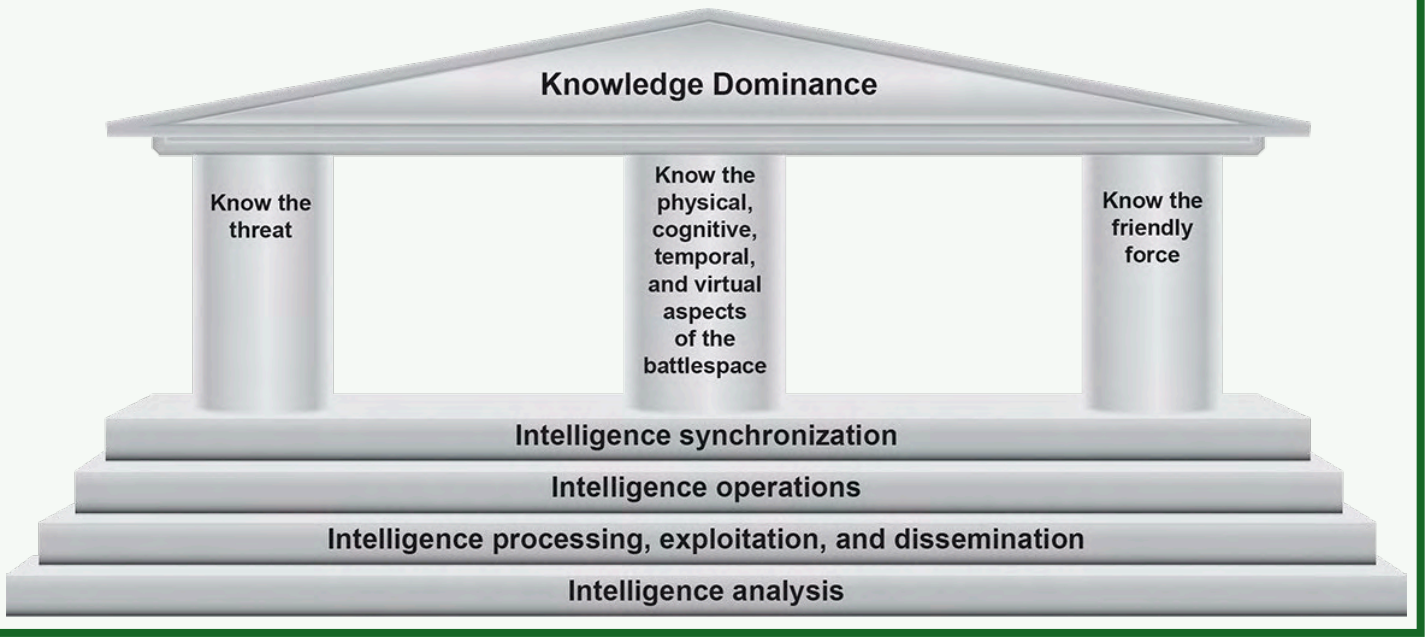
In response, DoD agencies, military services, academia, and the industrial complex must cooperate at an unprecedented level on research and development and science and technology innovation: militarization of new technology must occur faster than ever before. Today's acquisition process will be obsolete to support the demands of increased lethality of weapon systems, sensor proliferation and accuracy, processing speed, ubiquity of data, miniaturization, and other advances. Army intelligence is a high-tech consumer and is not immune to this trend. While efforts made in the 2020-to-2028 timeframe made great strides in closing the deep sensing and data processing gap, the Army must continue to look for ways to achieve overmatch against the threat. Army Futures Command must continue to experiment with concepts designed to address the future operational environment, leverage advanced technology, and inform force structure and materiel development.

How the Army fights beyond 2038 will evolve in every domain and the electromagnetic spectrum and will include economic, knowledge, and temporal considerations while the diplomatic aspect will remain outside of DoD's purview for integration. Information in all its forms becomes a commodity for producing knowledge. The future of the intelligence warfighting function becomes knowledge dominance.

Information operations for an effect remains a separate function from the collection and processing of information to generate knowledge. Knowledge dominance takes situational awareness to the next level as all things potentially become knowable. Priority intelligence requirements are coordinated with stakeholders the same as they were in the past. Knowledge dominance becomes a core competency of Army intelligence. Knowledge dominance is achievable through transforming intelligence organizations and

Alternative Analysis

This article's author and contributors artificially constrained themselves to what Army MI can control. Upon further examination and deliberation with senior leaders, there is likely a more effective way to implement knowledge dominance (KD) in the future. During open dialogue about the potentially revolutionary effects of technology insertion resulting in KD, it became evident that KD has broader implications across the Army and that there are ramifications for stakeholders well beyond MI. KD is potentially much more than simply a core competency for MI. ADP 6-0, *Mission Command: Command and Control of Army Forces,* says, "Knowledge management is supported by four tasks that bring an organization closer to situational and shared understanding. The four knowledge management tasks are creating knowledge, organizing knowledge, applying knowledge, and transferring knowledge."[3] The suggested alternative solution for the Army is to replace the Army Universal Task "Conduct Knowledge Management and Information Management" with "Conduct Knowledge Dominance." By using technology to expand the scope of knowledge and information management, KD could become the qualitative and quantitative mechanism by which the Army provides support to situational understanding for our commanders. We hope this article and alternative analysis will spark the imagination of capability developers across the Army and generate intellectual dialogue that will drive innovation.



structure with Global Information Grid server farms, high-tech data scientists, and skilled ethical hackers working in a federated and distributed enterprise approach, centralized at echelons corps and above and tailored to meet command and control requirements. These high-cost, high-demand, low-density capabilities will downward reinforce division and brigade formations. Army intelligence organizations at divisions and brigades become smaller and are more capable because of technological enhancements. The ability to collect all available information and potentially "know all things" could create the opportunity to use data for illicit purposes, requiring a revision of intelligence oversight regulations. Policy changes may also address additional ethical considerations, including neural implants that enable direct human interaction with machines, and thoughts with other humans, and implications of autonomous machine warfare. In this era, time and knowledge become the critical factors because information and data are widely and openly available. A commander's ability to make the right decision faster than his opponent is the key to success.

U.S. Army photo illustration

The Army's modernization approach requires updating its doctrine, organizational designs, and training to conduct operations as a multi-domain force.

Technology will leap ahead by 2038. Artificial intelligence, machine learning, and quantum computing will greatly accelerate capabilities for research and development and science and technology. DoD and Army acquisition processes will become more streamlined as industry becomes more closely aligned with DoD. A genuine modular open system architecture design will allow rapid technology insertion. Supported by these technologies, the global sensor grid will render range less relevant and crypto less secure. No information will be "off limits," and PED becomes nearly instantaneous. Next-generation technologies will augment analysis and predict indicators of adversarial intent. The tactical cloud will become a virtual Global Information Grid fed by, and accessible from, anywhere in the world using self-healing networks. Nanotechnology will help scale and tailor capabilities to each echelon. Every piece of equipment and every Soldier has an organic, automated, multimodal sensor pod linked to the Global Information Grid and managed by artificial intelligence. Biotechnology, neural implants, and personal avatars improve Soldier capabilities and capacities. Augmented and virtual combined environments with four-dimensional displays enhance visualization. Together these capabilities have the potential to revolutionize commanders' situational understanding by creating an environment where it is possible to collect and know everything.

Soldiers continue to provide the advantage over near-peer adversaries. Future intelligence Soldiers are curious, mentally agile, ethical, adaptive, passionate, and predictive. Well trained and continuously educated, they understand culture, technology, and context and can calmly communicate their contributions to both human and machine. Previous initiatives such as regimental assignments, area specialists, separate leadership and technical tracks, a step-increase program, and linguist management will become routine talent management practices. New training in economics and temporal analysis will supplement increased technical training, all in a virtual environment. Augmented reality, virtual avatar personal assistant, and biotechnology provide opportunities for analysts to collaborate and learn. Infrastructure will reduce as a combination of remote workers/locations, virtual training and interaction, distributed offices, and robotic capabilities. Leaders will adapt to these changes and the increased operational tempo. Contractor experts will augment uniformed personnel at corps and echelon above corps levels.

Conclusion

If technology trends continue to change at an exponential rate, the U.S. military can ill afford complacent thinking

about the future. Army intelligence modernization must not overlook less conspicuous low-tech threats from third-world adversaries. Optimizing to fight future threats requires an adaptive intelligence force capable of supporting competition short of war and maneuver and fires during large-scale combat operations, in all domains with increased speed, accuracy, and lethality throughout the depth of the extended battlefield. As the Army continues adapting to the current and future operational environment, developing a capable intelligence force that exceeds the challenging demands of commanders' expectations is critical. Highly capable Army intelligence organizations are essential to success now and in the future. The Army must not only continue its pursuit of materiel solutions to support MDO and beyond, but it must also recruit and retain highly skilled Soldiers. It must also build the right force structure to collect, process, and disseminate relevant, timely, predictive intelligence in all domains from theater to tactical levels in support of the joint force.

Epigraph

GEN James C. McConville, "2020 Posture Statement House Armed Services Committee," U.S. Army Worldwide News, March 3, 2020, https://www.army.mil/article/233474/2020_posture_statement_house_armed_services_committee.

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).

2. Figure is adapted from Figure 3-1. The intelligence process, Department of the Army, Army Doctrine Publication (ADP) 2-0, *Intelligence* (Washington, DC: Government Publishing Office [GPO], 31 July 2019), 3-2.

3. Department of the Army, ADP 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. GPO, 31 July 2019), 3-8.

Mr. Mark Wallace retired from active U.S. Army service in 2009 as a colonel in the Military Intelligence Corps. Currently, he works as a defense contractor in the Intelligence-Capabilities Development and Integration Directorate (I–CDID), Concepts Division at Fort Huachuca, AZ.

Contributors:

Ms. Mary Ellen D'Amico, a retired U.S. Army military intelligence noncommissioned officer, is the Concepts Team Chief for the I–CDID, Concepts Division.

Mr. James Harper retired from the U.S. Army after 30 years in military intelligence. He is currently a defense contractor writing intelligence concepts in the I–CDID, Concepts Division.

Doctrinal Proficiency and Doctrinal Assistance

PANIC …… 34 publications and over 5,500 pages of doctrine spread across multiple domains and I just want to know the responsibilities of an OMT. What do I do?

- Answer -

Email usarmy.huachuca.icoe.mbx.doctrine@mail.mil for friendly doctrinal assistance. We will not read it for you, but we can point you in the right direction. We will provide you an answer as quickly as possible, but please allow at least two business days.

Want to be in the doctrinal know?

USAICoE doctrine maintains an email notification list to announce —

- Publication of new issues of MIPB.
- Publication of new U.S. Army intelligence doctrine.
- Notification of draft U.S. Army intelligence doctrine staffings.

If you wish to receive these notifications, send a message to the email address listed above and you will be added to the list.

Intellectual Humility and Defining Success

by Chief Warrant Officer 5 Kevin G. Boughton
CCWO, U.S. Army Intelligence & Security Command (INSCOM)

***Editor's Note: This article is reprinted with the permission of* Newsliner, *the professional journal of the U.S. Army Warrant Officers Association, "The Quiet Professionals." It was originally published in the February 2020 issue of* Newsliner.**

In 2018, I submitted an article to the *Military Intelligence Professional Bulletin* that was republished in the *Newsliner* that outlines what I describe as the leadership attributes and characteristics of senior Warrant Officers. This article describes an additional leadership attribute (intellectual humility) and explains my leader philosophy for defining and sustaining success.

To recap the leadership attributes and characteristics of senior Warrant Officers, first and foremost the senior Warrant Officer must be a technical leader, not just a technical expert. The senior Warrant Officer must also be an ethical leader, a professional leader, a disciplined leader, and a steward of his or her profession.

While these five attributes help form a solid leadership foundation (similar to the leadership attributes and competencies in Army Field Manual 6-22), they do not encompass all leadership attributes or competencies required to be successful in the Army as a Warrant Officer.

The additional leadership attribute and leader philosophy are based on my personal lessons learned as the Command Chief Warrant Officer of the Intelligence and Security Command (INSCOM), and on my engagements with hundreds of Warrant Officers across the Army.

The additional leadership attribute of "Intellectual Humility" enhances the five attributes mentioned above. A failure to apply this attribute can result in a loss of trust, career, and in the worst cases loss of life or limb. My leadership philosophy on success is an exemplar model to help shape a Warrant Officer's beliefs and behaviors across a career.

Intellectual Humility (Leadership Attribute)

The concept of humility is not an attribute or leadership characteristic normally associated with the military. However, Field Manual 6-22 "Leader Development" does mention humility as a "desired characteristic of organizational and strategic leaders" (Army Field Manual 6-22, Leader Development, 2015, pp. 1-9).

> ***"Humility is a desired characteristic of organizational and strategic leaders who should recognize that others have specialized expertise indispensable to success. A modest view of one's own importance helps underscore an essential ingredient to foster cooperation across organizational boundaries. Even the most humble person needs to guard against an imperceptible inflation of ego when constantly exposed to high levels of attention and opportunities."***

While I agree humility is important for our strategic leaders, I firmly believe humility applies to ***all*** Warrant Officers, regardless of unit or echelon of assignment. Why is being humble important to the Army's technical leaders? First, a technical leader and expert who is humble understands that the strength of the Army is the collective knowledge, skills, and professional behaviors of its people, and no single Soldier holds all the answers.

I have personally observed the imperceptible – and more often quite observable – inflation of ego in the Warrant Officer cohort, specifically related to the principle of "intellectual humility." Gustavo Razzetti explains, "Intellectual humility means leaving the door open, even when you think you are right. You are receptive to new facts, instead of trying to protect yourself" (Razzetti, 2019).

When a Warrant Officer's ego does not allow him or her to be receptive to new ideas (and to be wrong), it can and does result in a breakdown in other desired attributes, such as disciplined leadership and stewardship of the profession.

When Warrant Officers believe they "know it all," they take liberty with authorities, processes, and critical workflows that often result in devastating consequences to a unit/organization's success, and in some cases even the very careers of those officers. When technical Warrant Officers fail to be intellectually humble, it can result in a loss of trust from commanders, peers, and Soldiers.

Within the Army Aviation Corps, this can lead to devastating, costly, and sometimes deadly results. Many Army aviation accidents are the result of overconfidence and lack of intellectual humility in some of our most senior aviators, especially evident when a pilot might question the need to

use a checklist or forget to use a checklist, even though they have thousands of hours in the cockpit.

Another exemplar of this phenomenon within the aviation and medical profession are described in detail in the National Public Radio Hidden Podcast Hidden Brain episode, "You 2.0: Check Yourself" (Vedantam, 2018).

Bottom line, technical expertise and experience often fail when coupled with overconfidence and a lack of intellectual humility. Army Warrant Officers should carefully guard against this natural tendency in ego as we grow in experience, knowledge, skill, and behavior in our specific technical disciplines. A lack of intellectual humility, tangled with personal ego and overconfidence, can be costly.

Defining Success (Leader Philosophy)

How do we define a successful Army career? Success should never be focused on achieving rank, reward, or accolades. It must be about outcomes, i.e. the effects of your efforts at every assignment and on every mission. My philosophy is to ask myself two basic questions.

- Am I contributing to the mission in a positive manner?
- Am I making a difference for the future of my family, the Army, and the nation?

I have spent my career focused on these two questions, as a basis of my philosophy on success. The decisions I make in regard to my Army career drive me to one foundational concept, and that is to *"execute whatever mission I am given to the very best of my ability in an attempt to answer the two foundational questions."*

However, you cannot just leave success to chance, and just these questions. You must do your best to ***prepare*** for success. Attend Professional Military Education courses with a positive attitude, striving to learn and grow. Look at every day as a new beginning, and new chance to learn and grow your skills and knowledge.

Approach every situation and every interaction with a positive attitude, and view these as opportunities to grow as a Soldier and a person. Treat all Soldiers and civilians with respect and decency. After all, even the most junior Soldier and the janitor have an innate desire to be recognized for the value they bring to the unit/organization.

How do you ***maintain*** success? I believe you maintain success by never forgetting where you came from. Stay humble, be positive, and demonstrate technical leadership – after all, there was a time, not that long ago, when you may have been an inexperienced private or young Sergeant, learning to lead.

Strive to demonstrate value to those around you through continuous focused efforts, maintaining a positive attitude, and never forgetting the two foundational questions. ***"Am I contributing to the mission in a positive manner?" and "Am I making a difference for the future of my family, the Army, and the nation?"***

Works Cited

Army Field Manual 6-22, Leader Development. (2015). Washington D.C.: U.S. Army Publishing Directorate. Retrieved 2019, from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm6_22.pdf.

Razzetti, G. (2019, March 14). What If You're the One Who's Wrong? *Psychology Today*. Retrieved 2019, from https://www.psychologytoday.com/us/blog/the-adaptive-mind/201903/what-if-youre-the-one-who-s-wrong.

Vedantam, S. (2018, August 27). *Hidden Brain You 2.0: Check Yourself.* Retrieved from National Public Radio: https://www.npr.org/transcripts/642310810.

Rapid Transformation

The Distributed Common Ground System-Army (DCGS–A) is a multi-echelon intelligence system that includes hardware and software to support the intelligence warfighting function. The U.S. Army fielded DCGS–A in 2005 and now, 15 years later, the system's technology is rapidly aging. It provides tools for intelligence preparation of the battlefield and access to more than 800 data sources, which enable commanders to execute mission command; synchronize fires; and task intelligence, surveillance, and reconnaissance sensors. DCGS–A is fielded to 1,608 unit headquarters across military intelligence brigades-theater, corps, divisions, brigades, and battalions.

DCGS–A updated its acquisition strategy and restructured in 2017 in response to independent study recommendations and language in the National Defense Authorization Act for Fiscal Year 2017. DCGS–A restructured to a "capability drop" approach to fix and modify certain components to overcome the known limitations of DCGS–A using commercially available solutions.

Capability Drop 1. In July 2017, in an effort to conduct rapid modernization, the Army Requirements Oversight Council approved the Capability Drop 1 (CD1) requirements that focused on a simplified and expeditionary all-source intelligence solution for the battalion echelon. CD1 began fielding and training in May 2019 to all 402 brigade combat team battalions. CD1 is scheduled to complete fielding and to update 15 percent of the total DCGS–A footprint by mid-2020. It will provide the force with a multi-domain capability supporting the tactical "close area" fight.

Capability Drop 2. In a move to modernize the strategic level, the Army approved Capability Drop 2 (CD2) requirements in June 2019. By 2021, CD2 will provide a cloud-enabled and tailored solution to process large volumes of disparate data and assess enemy courses of action via "big data analytics," enabling commanders at all echelons to outpace the threat in a fast-paced joint all-domain environment. CD2 will enable independent maneuver, mission command, cross-domain fires, and cross-domain synergy in tactical, operational, and strategic areas of the battlefield.

DCGS–A is planning to complete fielding of CD1 and CD2 while sustaining only minimum existing capabilities (end of life 2026). It will begin restructuring into two new "next-generation" programs in 2022 to enable the Army's modernization priorities, to support the National Defense Strategy, and to optimize for joint all-domain operations.

Adapting to the Future

The Tactical Intelligence Targeting Access Node (TITAN) and Intel Apps programs will automate and accelerate intelligence processes and will learn and adapt to evolving threats, conditions, and missions through the application of artificial intelligence and machine learning, while delivering critical intelligence to operational commanders from future intelligence sensors.

TITAN. TITAN will bring an expeditionary, mobile, transportable, modular, and scalable intelligence ground station to support deep-sensing gaps and provide intelligence support to targeting for long-range precision fires. TITAN will consolidate capabilities from existing legacy ground stations and leverage space and high altitude, aerial, and terrestrial layer sensors to provide targetable data directly to fires networks, and situational awareness/situational understanding in support of mission command.

Intel Apps. Intel Apps is planned to deliver 10 crosscutting applications to the Command Post Computing Environment from 2022 to 2026. This will occur while updating the geospatial foundation and integrating a new data layer to enable seamless collaboration across warfighting functions (operations/intelligence convergence) and implementation of advanced analytics and artificial intelligence/machine learning. This will enable the Army intelligence community and maneuver commanders to outpace the threat.

Mr. Donald Beattie is a retired Army military intelligence officer who currently serves as the Deputy for Army Capability Manager-Foundation at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. He holds a bachelor of science from Canisius College and a master of arts in education from the University of Colorado.

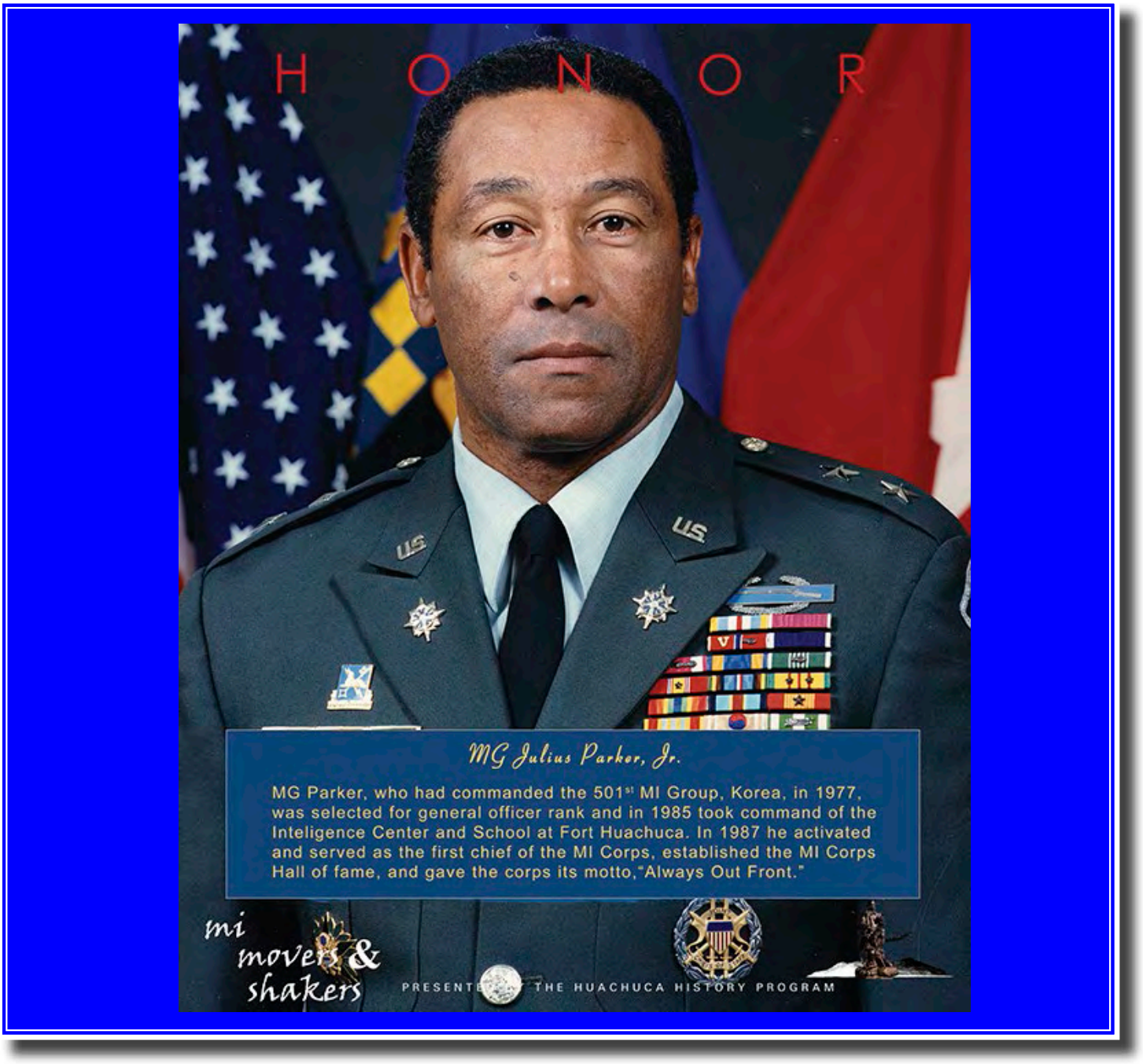


Photo by CPT Scott Kuhn, 3rd Armored Brigade Combat Team, 1st Cavalry Division

Demonstration, Experimentation, and Prototype: Enhancing the Analysis of Alternatives

by Colonel Mark Dotson and Colonel Jennifer McAfee

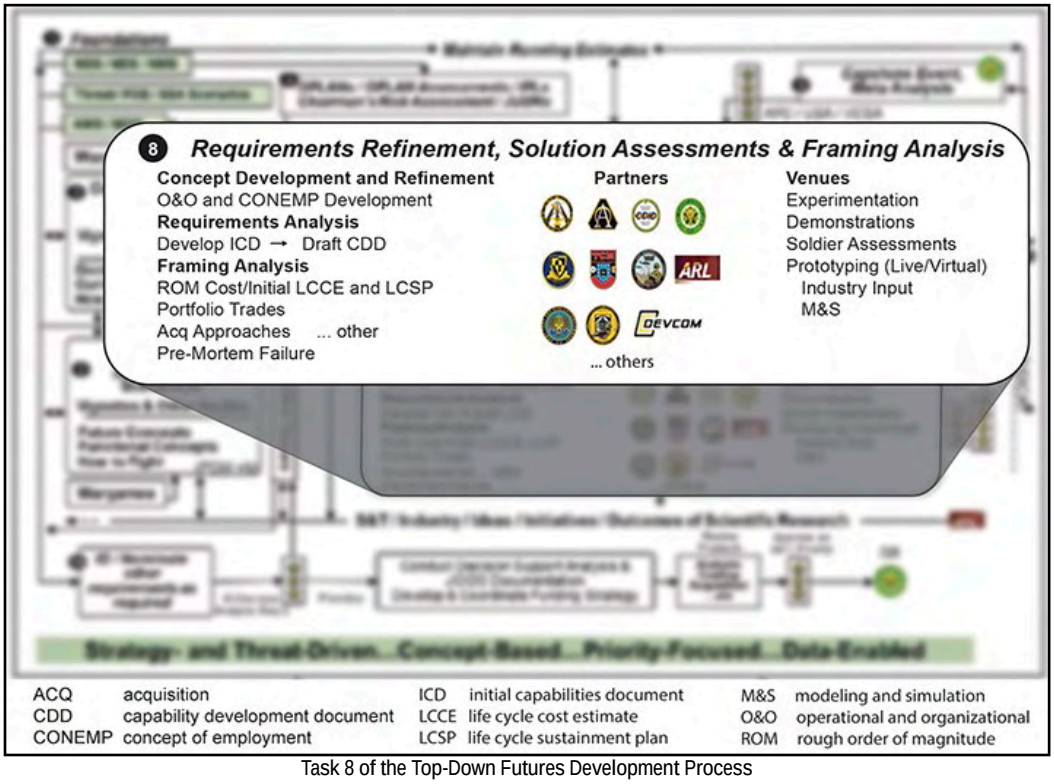
The Army's newest electronic warfare vehicle, the Electronic Warfare Tactical Vehicle (center), was tested in conjunction with other electronic warfare equipment, including the Versatile Radio Observation and Direction (VROD) and the VROD Modular Adaptive Transmit systems (seen mounted on the Humvees) at the National Training Center, Fort Irwin, CA, January 16, 2019.

Introduction

With the global increase in use of the electromagnetic spectrum (EMS) for communications and non-communications activities, the EMS is rapidly becoming more congested and contested. Moreover, peer and near-peer competitors are equipped to further challenge the U.S. Army's ability to operate in the EMS. Maintaining the Army's freedom of maneuver in the spectrum requires new training, leader development, and materiel capabilities. The Terrestrial Layer System (TLS) is intended to meet those materiel requirements. Because the Army needs these and other capabilities in the near future, it has recently re-looked its requirements and acquisition processes with an eye toward acceleration. Several organizations, with the guidance of Army senior leadership, used Demonstration, Experimentation, and Prototype (DE&P) to enhance the analysis of alternatives (AoA) process and speed requirement development, posturing the Army to win in competition and conflict in the EMS. These organizations included the Cyber Center of Excellence (CCoE); Intelligence Center of Excellence (ICoE); and Program Executive Office, Intelligence, Electronic Warfare and Sensors (PEO IEW&S).

In the summer of 2019, the Army continued to document its need for the TLS—the cornerstone of future integrated ground-based signals intelligence (SIGINT), electronic warfare (EW), and cyber operations capabilities. With several approved initial capabilities documents broadly outlining required capabilities, the next step was a study on how to provide those capabilities—this study is an AoA. The purpose of the AoA is to identify and assess a broad spectrum of potential solutions to assist senior leaders in deciding what materiel solution(s) might be able to meet the requirement in the most cost-effective manner.[1]

Since a traditional AoA can take a number of years, Army senior leadership directed an alternative approach to



Task 8 of the Top-Down Futures Development Process

streamline and operationalize TLS requirements development and acquisition. In November 2018, the Army issued an order to blend rigorous theoretical analysis with real-world experimentation in order to learn by doing, and it directed CCoE and ICoE to execute DE&P in lieu of a traditional AoA.[2]

The DE&P Approach

The DE&P approach informs the requirement with actual equipment in use by Soldiers in parallel to the theoretical work normally associated with AoAs. This process is reflected in task 8—Requirements Refinement, Solution Assessments, and Framing Analysis—of the Army's Top-Down Futures Development Process shown in the figure.[3]

As described, the process uses multiple partners and venues to enhance the theoretical work done in a traditional AoA. To meet the requirements of their order, CCoE and ICoE, in coordination with PEO IEW&S, implemented this new process designed to ensure the Army gets state of the art equipment by accurately capturing realistic requirements. CCoE, ICoE, and PEO IEW&S implemented task 8 with a wide range of partners leveraging U.S. Army Forces Command's and U.S. Army Training and Doctrine Command's experimentation venues, while remaining focused on the analytical outcomes:

- Concept Development and Refinement.
- Framing Analysis.
- Requirements Analysis.

Concept Development and Refinement

Three DE&P lines of effort (LOEs) were used in order to nest with the Concept Development and Refinement portion of the Top-Down Futures Development Process: organization, training, and materiel. Each LOE was worked by a team, including leadership, subject matter experts, and data analysts. Starting with the analysis of nearly 200 documents, including a draft military intelligence/EW concept of operations (MIEW CONOP) and a draft architecture document, the LOE teams observed a number of field exercises and simulations. Those events contained more than 3,000 opportunities for Soldiers to use the equipment and provide feedback over 108 days in the field. The events contributed to a greater understanding in three key areas: SIGINT and EW Soldiers working together, SIGINT and EW staff integration, and the data burden on the network.

DE&P observations show a progression of collaboration and an increase in capability for the commander. As the DE&P events started, SIGINT and EW Soldiers operated separately, took direction from different staff elements (S-2, EW officer), and did not complement each other in the field—such as tipping and cueing. During the second observed field exercise, the Soldiers began reorganizing for better communication. By the time they operated at the National Training Center, 4 months later, the military intelligence company commander and Soldiers organized in a tailored manner for each operation—often placing SIGINT and EW Soldiers on the same vehicle. The S-2 increased use of the cryptologic support team, and the cyberspace and electromagnetic activities section actually co-located a portion of its staff with the cryptologic support team in the S-2 section to improve synchronization. Commanders, Soldiers, and staffs improved their understanding of the interdependence of SIGINT and EW with each of the five observed exercises.

These lessons helped refine the MIEW CONOP and define the required information flow. With that knowledge, architecture designers took what had been theoretical, stovepiped concepts and applied real operational data to enhance

how various systems, staffs, and commanders would share information. This in turn enabled realistic simulations to gain a feel for the network communications burden—something that had only been an assumption to this point. The outcome of Concept Development and Refinement was that Soldiers informed the requirement using actual equipment and the processes they developed or improved in the field.

Framing Analysis

During the Framing Analysis, operational execution with surrogates, in addition to historical documents and analysis, provided better resolution on costing, prioritization, and acquisition approaches. This informed Army senior leadership's review and approval of the capability development document.

At the outset, TLS costing was based on the Prophet system with some additional assumptions regarding EW integration. As a result of using DE&P with quick reaction capabilities such as the Tactical Electronic Warfare System (TEWS) and pre-prototypes such as the Tactical Signals Intelligence Vehicle (TSIG), more accurate predictions of cost data and manufacturing times (with the identification of long lead-time items) were completed. Marrying this costing with how TEWS and TSIG actually operated in the field and across the remainder of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF–P) informed Army senior leadership with sound analysis as they prioritized TLS within the Force Development intelligence portfolio.

For PEO IEW&S, understanding costs, associated system requirements, and Army senior leadership prioritization enabled a flexible acquisition approach supporting either a traditional Joint Capabilities Integration and Development System or a Mid-Tier Acquisition (under Section 804 of the National Defense Authorization Act) approach. These options allow the program to continue to evolve as the requirement is refined with "just in time" requirements approval granting Army senior leadership greater decision space and requirement flexibility. As a result of Framing Analysis, requirements and acquisition personnel were able to use historical data and analysis, informed by actual field exercises, to provide more refined information for Army senior leadership decision making.

Requirements Analysis

Concurrent to the activities mentioned, CCoE and ICoE conducted Requirements Analysis and continuously revised the draft capability development document. Revisions focused on the performance parameters and system attributes, added specificity for formations, and ensured all the requirements were realistic and testable. For parameters and attributes, the need for onboard signals of interest libraries, multiple workstations, and the alternate power to operate quietly for long periods of time was added. Document revisions and additional appendices reflect requirement variations by formation type and added the type of vehicle for each type of brigade combat team. Using lessons from exercises and discussions with the greater intelligence community, industry, and EW and testing professionals ensured requirements supported operational commanders' needs. This also ensured requirements were achievable and adequately verifiable through a variety of testing. The balance of operational prototyping and rigorous analytics, as well as organizations, operations, and materiel, helped develop and inform an achievable requirement to deliver TLS capabilities.

U.S. Army photo

As the Army moves forward with integrating SIGINT, EW and cyber, it continues to provide interim EW capabilities to units to pace threats.

A Proven Approach

With a broad spectrum of partners, CCoE, ICoE, and PEO IEW&S found viable solutions for the Army to pursue with respect to developing TLS. These partners included Army research facilities, major Army commands, combatant commands, the U.S. Marine Corps, industry, and others. They did so by analyzing data from previous research and a number of exercise

and simulation venues. The result was the development of a requirement that will greatly contribute to the Army's ability to maneuver in the EMS. This approach was fully nested in task 8 of the Top-Down Futures Development Process and illustrated how this process can help break down stovepipes and maximize functional integration. Most importantly, it concretely demonstrated how a materiel solution's contributions to mission accomplishment in an Army gap area could be rapidly designed, built, and used without an inordinate and premature commitment of resources.

Endnotes

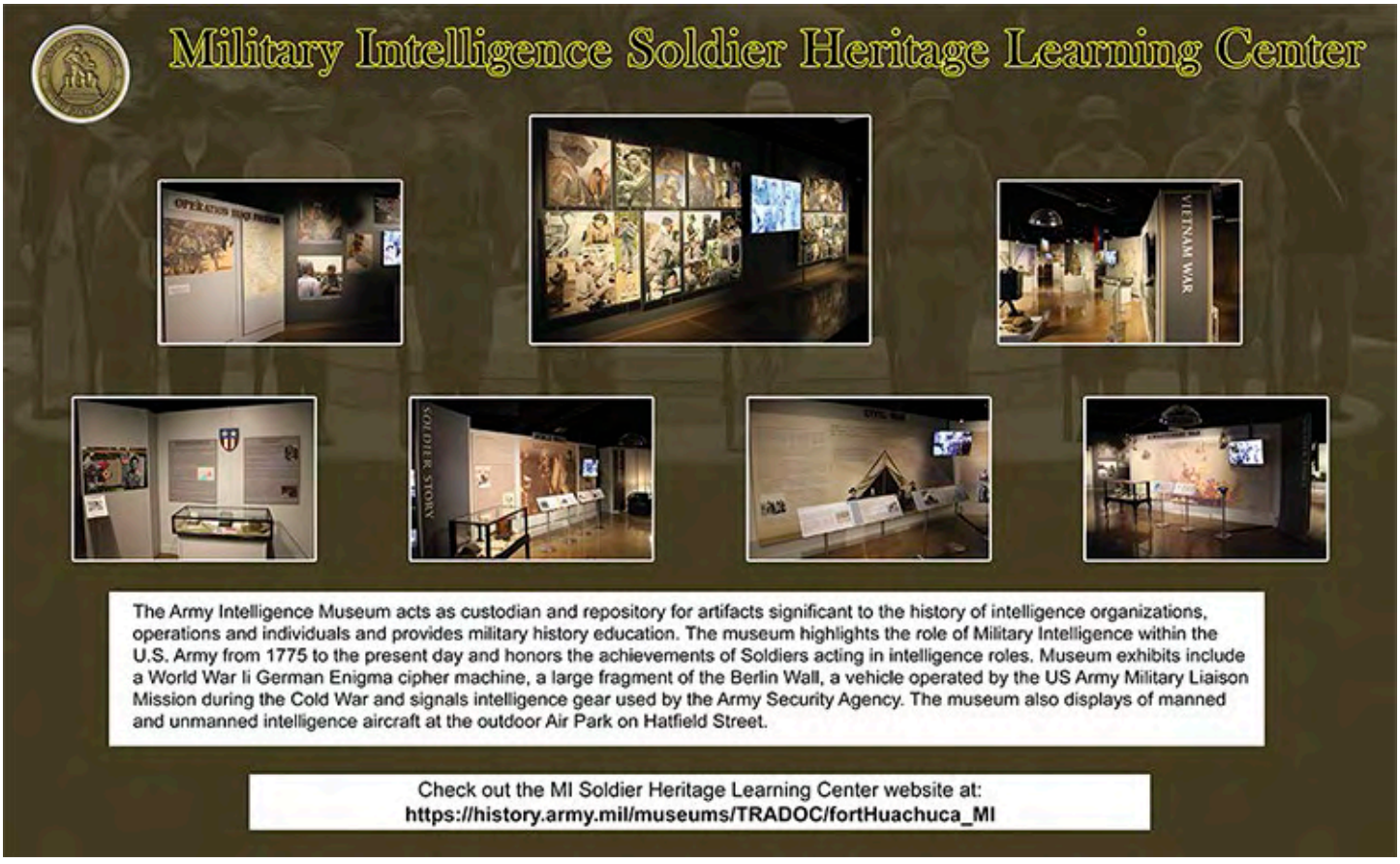
1. Department of Defense (DoD), DoD Instruction 5000.02T, *Operation of the Defense Acquisition System* (Washington, DC: January 7, 2015), 130. Change 1 was issued on April 21, 2020.

2. The order was Headquarters, Department of the Army Execution Order 215-18, *Terrestrial Layer System (TLS) Integrated Signals Intelligence/ Electronic Warfare/Cyberspace Operations (SIGINT/EW/CO) Demonstration, Experimentation, and Prototype*.

3. Department of the Army, Army Futures Command, *Top-Down Futures Development Process* (Version 2.0) (1 October 2019).

COL Mark Dotson is the Army Capability Manager for Electronic Warfare and is assigned to the U.S. Army Cyber Center of Excellence at Fort Gordon, GA.

COL Jennifer McAfee is the Army Capability Manager for Formations-Intelligence and is assigned to the U.S. Army Intelligence Center of Excellence at Fort Huachuca, AZ.



Bridging the Brigade Combat Team Collection Management Manning Challenge

by Chief Warrant Officer 2 Bary McMaster

Introduction

The information collection task of the intelligence warfighting function allows the commander to gain a shared understanding of the operational environment. Doctrinally, the brigade combat team (BCT) collection management element is responsible for the planning and execution of the information collection plan. The current BCT intelligence warfighting function design maximizes support for the BCT in a counterinsurgency environment. While this worked well for most operations over the past decade, the current structure is not organized to meet the requirements of large-scale ground combat. However, there is some good news on the horizon.

Force Design Update

Based on a bottom-up review conducted by the U.S. Army Intelligence Center of Excellence and the Department of the Army G-2, the BCT military intelligence (MI) company internal structure will be realigned to enhance the overall quality, efficiency, and effectiveness of intelligence analysis and production support for multi-domain operations. Changes to the U.S. Army Forces Command (FORSCOM) modified table of organization and equipment (MTOE) will take effect in fiscal year (FY) 2022, and a portion of the changes will increase the BCT's collection management capacity and capability. These changes involve repurposing an all-source intelligence technician and an intelligence analyst noncommissioned officer (NCO) from within the MI company to fill the roles as the BCT's collection manager and the collection noncommissioned officer in charge (NCOIC). This MTOE alignment helps to mitigate the lack of long-term continuity within the collection management section. Pending the approval of a military occupation classification structure action currently with the Department of the Army G-1 (Personnel), both of these positions will carry the Q7 Additional Skill Identifier to ensure the BCT has the appropriate authorizations for formal collection management training.[1] In addition to these approved changes for FY 2022, FORSCOM will likely recommended future modifications to create a collection management section in the BCT S-2. In anticipation of this, in FY 2022 the synchronization and collection management section of the MI company will be renamed the analysis and fusion section. This section still remains a core element of the brigade intelligence support element supporting the BCT S-2.

Army-wide implementation of the new structure will require several years after the initial execution to be fully supported, and there are also doctrine and training considerations as part of the transition. ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*,[2] is undergoing revision to align with updated intelligence and operations doctrine as well as the changes in force design. The revised publication provides a description of the responsibilities belonging to the synchronization and collection management section (which later becomes the analysis and fusion section). This draft publication is on pace for publication in early calendar year 2021. TC 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3*,[3] should also be updated to reflect the MI company structure realignment. However, this change largely does not impact the overall training and certification strategy of the collection management crew because the collection management tasks did not change and are independent of military occupational specialty. The curriculum of the Information Collection Planner Course (ICPC) (ASI Q7) may require some revisions to address the additional complexities associated with large-scale ground combat operations and to keep pace with emerging multi-domain operations requirements. Another consideration for ICPC is to include additional familiarization with the echelon corps and below elements the BCT collection managers are required to coordinate and synchronize with on a regular basis; for example, working with the brigade aviation element and requesting airspace for organic and nonorganic airborne collection platforms. The addition of more FORSCOM Q7 billets will also necessitate an increase to iterations of the ICPC, which is already a highly sought-after course.

During the Transition

During this transition period, it is possible that collection management may not operate at optimal capacity.The BCT MI company force structure realignment is approved, and BCT S-2s can better prepare the BCT by implementing changes now. Manning of an interim collection management section will require flexibility because of ongoing shortages of intelligence officers and enlisted Soldiers at echelon. In line with the BCT commander's intent, the BCT S-2, in coordination with the MI company commander, will need to look internally for solutions to manning for collection management. For example, the MI company's intelligence support team (COIST), which is most effective in counterinsurgency operations, could be an option to staff the collection management section for decisive action operations in the interim.

Roles and Responsibilities. Doctrinally, the collection management element is responsible for assisting the BCT S-3 in developing the information collection plan by creating and updating the information collection matrix, information collection synchronization matrix, and information collection overlay.[4] These planning tools require significant coordination and synchronization with the entire BCT staff, subordinate battalions, and echelons above brigade. BCTs that understaff the collection management element experience challenges at combat training centers effectively managing the collection management responsibilities described in ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*[5]—

- Participates in the BCT's planning.
- Receives requests for collection from subordinate maneuver elements and incorporates those requirements into the BCT information collection plan.
- Receives and coordinates nonorganic requests for collection support, and manages employment of organic information collection assets.
- Develops requests for collection and submits requests to higher headquarters for incorporation into the higher headquarters information collection plan.
- Develops collection-asset [specific information requirements] SIRs based on approved [priority information requirements] PIRs.
- Coordinates with the MI company commander on the employment of MI collection assets.
- Coordinates with the BCT and battalion commanders and staffs on the employment of information collection assets.
- Develops and submits recommendations for information collection tasks to the BCT S-3.
- Coordinates daily with the BCT S-2 plans element.
- Coordinates daily with the BCT S-2 current operations element and obtains information collection asset status reports from the BCT S-2 current operations element and MI company.
- Maintains daily communications with BCT subordinate units to remain current with operations and targeting priorities.
- Coordinates with the brigade aviation element for airspace usage and coordination by aerial collection assets.
- Provides briefings to the commander and staff.

Bridging the Gap. Numerous adjustments can be made to support collection management and bridge the gap until the force design changes are implemented. These adjustments include dedicating a minimum of four personnel to a collection management element and solidifying their roles and responsibilities in the BCT/S-2's tactical standard operating procedures. With regard to assignments, we can assign one of the BCT all-source intelligence officers, the information collection platoon leader, or a senior first lieutenant BCT assistant S-2 as the collection manager. We can also assign an MI company all-source intelligence technician fusion chief (if at 3/3) or the information collection platoon leader as the deputy collection manager.

Leveraging one of the MI company COIST intelligence analyst NCOs as the potential collection management element NCOIC is also a consideration. We should prioritize staffing the collection management element over the COIST if that is in line with the BCT commander's intent because the collection management element has a greater potential to affect operations for the entire BCT. We should consider sending at least one of the MI company's all-source intelligence technicians, BCT intelligence analyst NCOs, or MI company COIST intelligence analyst NCOs to ICPC to acquire "train the trainer"skills for the collection management element and current operations section. The selection criteria for this "train the trainer" role should be based on competency and longevity to ensure the collection management element's efficiency and continuity.

Conclusion

Applying these recommendations will help the BCT collection management element to operate at an improved capacity. This will in turn enable the effective planning and execution of the information collection plan, which will help

the commander to gain a shared understanding of the operational environment.

Endnotes

1. The Q7 Additional Skill Identifier is awarded from the Information Collection Planner Course. The course provides instruction in managing the employment of organic and supporting collection assets, as well as processes for reachback to higher headquarters and intelligence agencies for information, in order to provide the commander with effective intelligence support.

2. Department of the Army, Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. Government Publishing Office [GPO], 10 February 2015) (common access card [CAC] login required).

3. Department of the Army, Training Circular 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3* (Washington, DC: U.S. GPO, 25 February 2020) (CAC login required).

4. Department of the Army, ATP 2-19.4, *Brigade Combat Team Intelligence Techniques,* 2-11.

5. Ibid.

Reference

Department of the Army. *Brigade Combat Team Military Intelligence Company (BCT MICO) Force Design Update Junior.* 14 August 2019.

CW2 Bary McMaster is assigned to Operations Group Brigade Trainers as an observer coach/trainer (OC/T) at the National Training Center. As an OC/T, he is responsible for the coaching and training of brigade combat team intelligence officers, noncommissioned officers, and enlisted Soldiers in conducting intelligence preparation of the battlefield, information collection operations, and reconnaissance planning. He is formally trained in information collection operations through the Q7 Information Collection Planner Course and certified through U.S. Central Command/U.S. Indo-Pacific Command Intelligence, Surveillance, and Reconnaissance Manager courses. As a warrant officer, he has served as a brigade combat team collection manager for 2 years. As a noncommissioned officer, he served as a squadron collection manager during a 12-month deployment to Iraq.

The Future of Collection Management in Multi-Domain Operations

by Captain Michael T. Kossbiel

Introduction

The U.S. Army must expedite and prioritize the integration of collection management and sensor management tasks and capabilities supporting multi-domain operations (MDO) capable forces in joint and coalition environments under joint all-domain command and control (JADC2). The U.S. Army, the Department of Defense (DoD), and coalition partners have several competing projects and efforts relating to the development of MDO-capable collection management. If unaltered, these disparate efforts could potentially create redundant data standards and systems that lack interoperability. The DoD, Army, and intelligence community must fully integrate and synchronize collection management efforts to achieve the desired future state of cross-domain sensor convergence.

TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* implies the need for a joint all-domain sensor computing environment: "The ability to employ cross-domain fires provides options to commanders and builds resilience within the Joint Force to overcome temporary functional separation imposed by enemy anti-access and area denial systems."[1] MDO convergence specifically requires "the 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."[2] The ability for the intelligence warfighting function to support the employment of cross-domain fires is dependent on multi-domain command and control.

Army Efforts

Army efforts in this area include the following technologies, described in detail below:

- Common Operating Environment.
  - Command Post Computing Environment.
  - Mounted Computing Environment.
  - Mobile/Handheld Computing Environment.
  - Sensor Computing Environment (Sensor CE).
- Tactical Intelligence Targeting Access Node (TITAN).
- Machine learning and artificial intelligence.
- Unmanned aircraft systems (UASs).

Common Operating Environment. To address the need for a multi-domain command and control, the Army developed the Common Operating Environment, which is the Army's effort to solve capability integration issues caused by disparate and disconnected Army Battle Command Systems. The Common Operating Environment uses industry-standard open architecture and commercial off-the-shelf technologies to reduce the burden on the warfighter and reduce costs. Conceptually, the Common Operating Environment effort is similar to Apple iOS or Microsoft Windows, which have unified open architecture software that allows the computing environments and warfighting functions to "play in the same sandbox." The Common Operating Environment decouples the bundled acquisition of software and hardware, which reduces cost and simplifies mission command information systems. For example, applications on commercial off-the-shelf laptops will replace Command Post of the Future and Distributed Common Ground System-Army laptops. Once implemented, translation software and hardware such as the Data Distribution System server will not be necessary. The planned future state converges all warfighting functions' Army Battle Command Systems programs of records onto one suite of software and one server.[3]

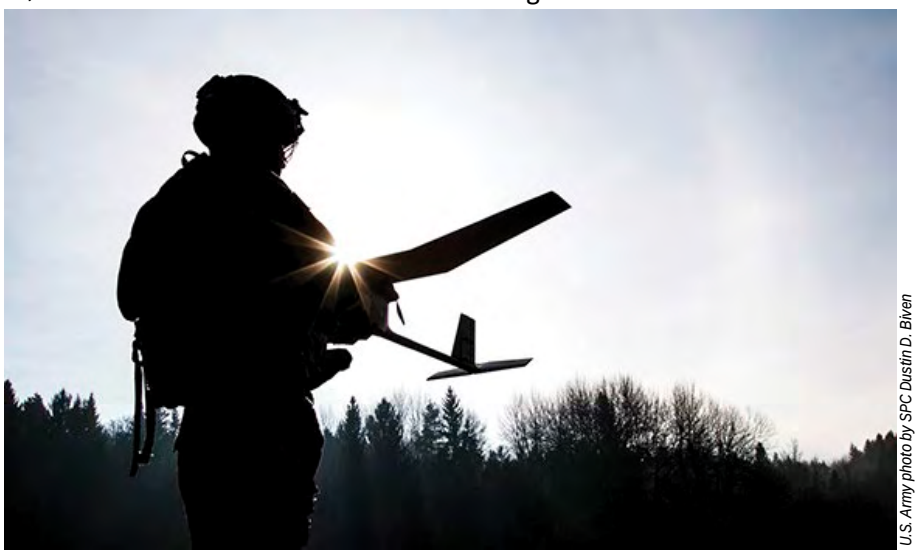
The Common Operating Environment has multiple computing environments, including the Command Post Computing Environment, Mounted Computing Environment, Mobile/

Handheld Computing Environment, and Sensor CE.[4] Sensor CE established a unified (sensor) data model that enables Army-wide sensors to feed (directly or indirectly) the common operational picture (COP). Sensor CE's common data model reduces latency and removes the need for workarounds, thereby shortening the sensor-to-shooter linkage by standardizing data across multiple current and future sensor programs of record. Essentially, Sensor CE allows the network to do the hard work of getting data to the customer. Sensor CE enables the interoperability and integration of sensors and sensor data to the network, other sensors, and consuming applications. Furthermore, Sensor CE requires future sensors and sensor data to be discoverable, visible, accessible, understandable, trusted, and interoperable across the Common Operating Environment. The current solution for Sensor CE is the Integrated Sensor Architecture being developed at the U.S. Army Combat Capabilities Development Command's Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center.[5]

The Integrated Sensor Architecture is a technically mature, government-owned solution that is low cost and has been fielded with several sensors.[6] In 2019, the C5ISR Center and the Program Executive Office for Intelligence, Electronic Warfare and Sensors hosted a demonstration of this capability in Virginia. During the demonstration, a network of Integrated Sensor Architecture-enabled sensors demonstrated a sensor-to-shooter capability by linking several sensors to a Containerized Weapon System. Sensor data was passed seamlessly from sensors to the Containerized Weapon System, enabling the system to rapidly engage targets. Fielding of the first instantiation of Sensor CE capabilities will occur in fiscal year 2023. After that time, the Sensor CE will integrate with additional Common Operating Environment computing environments.

Tactical Intelligence Targeting Access Node. In addition to the Common Operating Environment, the U.S. Army is developing TITAN. TITAN is a scalable and expeditionary intelligence ground station that will support commanders across the entire MDO battlefield framework with capabilities tailored by echelon. TITAN leverages space, high-altitude, aerial, and terrestrial layer sensors to provide targetable data to the fires networks as well as multidiscipline intelligence support to targeting and situational understanding in support of mission command. Overreliance on continental United States-based intelligence production and data hosting limits the Army's ability to effectively engage dynamic and time-sensitive targets. In the future, resilient multidomain ground stations must integrate sensor data in a seamless, dynamic, and continuous manner to generate effects in and from all domains.[7]

Machine Learning and Artificial Intelligence. The Army is investigating machine learning and artificial intelligence capabilities to support collaboration and mission command. The first goal is to reduce the amount of time between target detection and applied effects in the close fight by an order of magnitude through robust sensor data integration at the tactical edge. Key to this project is a synchronized data management strategy that will enable access to the appropriate data and format assisted by artificial intelligence and machine learning to aid in target detection and decision support. The second goal is by 2028 to deliver multi-sensor, multi-platform target correlation; artificial intelligence-aided decision making; automated system behaviors; and manned-unmanned teaming. Beyond 2028, the goal is to deliver tactical/operational artificial intelligence integration, artificial intelligence tasking of autonomous systems, and whole-theater data integration.[8]



U.S. Army photo by SPC Dustin D. Biven

The Army is trying to move away from runway-dependent and cumbersome UAS in favor of UAS that bring advanced teaming capabilities.

Unmanned Aircraft Systems. Program Manager, UAS is spearheading several projects related to collection management. One project, air-launched effects, is a family of systems designed to provide UAS capabilities launched from aircraft to autonomously or semiautonomously deliver effects as a single agent or as a member of a team. [9] "Serving as an [air-launched effects] ALE mothership, the [Gray Eagle-Extended Range] GE-ER will carry multiple ALEs with a variety of capabilities," and that "launching and controlling of ALEs from the GE-ER could potentially increase the survivability

and effectiveness of current and future manned aviation systems with intelligence, targeting, communications, jammers, decoys, and kinetic effects."[10]

Program Manager, UAS is also developing a new UAS platform interface control software suite that will allow authorized users to control selected assets from a mission command information system via a web application programming interface. The new software provides a capability to request several different levels of control, including monitoring of the platform and payloads, control of the sensor payload while monitoring the platform, control of the sensor payload, and limited control of the platform (single waypoints). The new software eliminates the need for ground control stations by providing flexible control through laptops and tablets that can be anywhere on the battlefield.

Joint and International Efforts

Unified sensor data standards not only create interoperability with U.S. Army sensors but will also enable interoperability for joint and coalition partners. For instance, American, British, Canadian, Australian, and New Zealand (ABCANZ) doctrinal and technical interoperability standards would enable sensor-to-shooter linkages across coalition task forces. Future international agreements on sensor data interoperability and security enclave agreements will enable an integrated sensor-to-shooter linkage within a multinational coalition division headquarters with subordinate ABCANZ force elements. In addition to coalition sensor interoperability, the DoD is developing the JADC2 concept. JADC2 requires any sensor to provide data to any shooter, including joint and coalition partners. The JADC2 cross-functional team is led by the U.S. Air Force, which is developing concepts and requirements for a materiel solution to enable joint sensor-to-shooter links.

The Defense Advanced Research Projects Agency's (DARPA) OFFensive Swarm-Enabled Tactics program is developing UAS swarm technology that "envisions future small-unit infantry forces using swarms comprising upwards of 250 unmanned aircraft systems… and/or unmanned ground systems…to accomplish diverse missions in complex urban environments.''[11] In December 2019 at Camp Shelby, Mississippi, DARPA conducted a demonstration of the OFFensive Swarm-Enabled Tactics technology, including the operational management of swarm tactics that Carnegie Mellon University and Soar Technology are developing. The operational management of UAS and unmanned ground system swarms allows users to define and prioritize swarm reconnaissance tasks, and it uses artificial intelligence to automate resource allocation to complete the reconnaissance tasks.[12] During the demonstration, in near real time, the swarm updated a three-dimensional COP on laptops and on augmented reality headsets.

The Seven Fundamentals of Reconnaissance

The seven fundamentals of reconnaissance are—

- Ensure continuous reconnaissance.
- Do not keep reconnaissance assets in reserve.
- Orient on the reconnaissance objective.
- Report information rapidly and accurately.
- Retain freedom of maneuver.
- Gain and maintain enemy contact.
- Develop the situation rapidly.[14]

Future Risks for Collection Management

To achieve "the rapid and continuous integration of capabilities in all domains" necessary for MDO cross-domain convergence, all the collection modernization efforts must standardize data and the command and control of sensors. The standardization of sensor data and command and control technology across the Army and joint force must be integrated and synchronized to achieve the volume and speed of delivery necessary to defeat peer adversaries. In the near future, the number of sensors, volume of data, and collection requirements will overwhelm already undermanned collection management cells. The increase of data and collection requirements with the cognitive overwhelming of collection managers risks a break with the seven fundamentals of reconnaissance.[13] Standardization and automation are necessary to ensure continuous reconnaissance, rapid and accurate reporting of information, and the ability to keep reconnaissance, sensors, and collectors in the fight (and not in reserve). In order to accomplish this, the author recommends that the DoD and the Army establish a collection management cross-cutting capability to fully integrate and synchronize all collection efforts on the MDO battlefield.

The Army must prioritize the creation of a singular conceptual, doctrinal, and materiel developmental strategy to fully integrate a future collection management MDO-ready capability. The Army should pursue the development of a collection management cross-cutting capability that fully integrates Army Capability Manager Foundation's collection management application and Sensor CE's data standards and services. The collection management cross-cutting capability would create a digital solution to bridge the gap between collection requirements management; collection operations management; and processing, exploitation, and dissemination (PED) across the Command Post Computing Environment, Mounted Computing Environment, Mobile/Handheld Computing Environment, JADC2, and coalition partners.

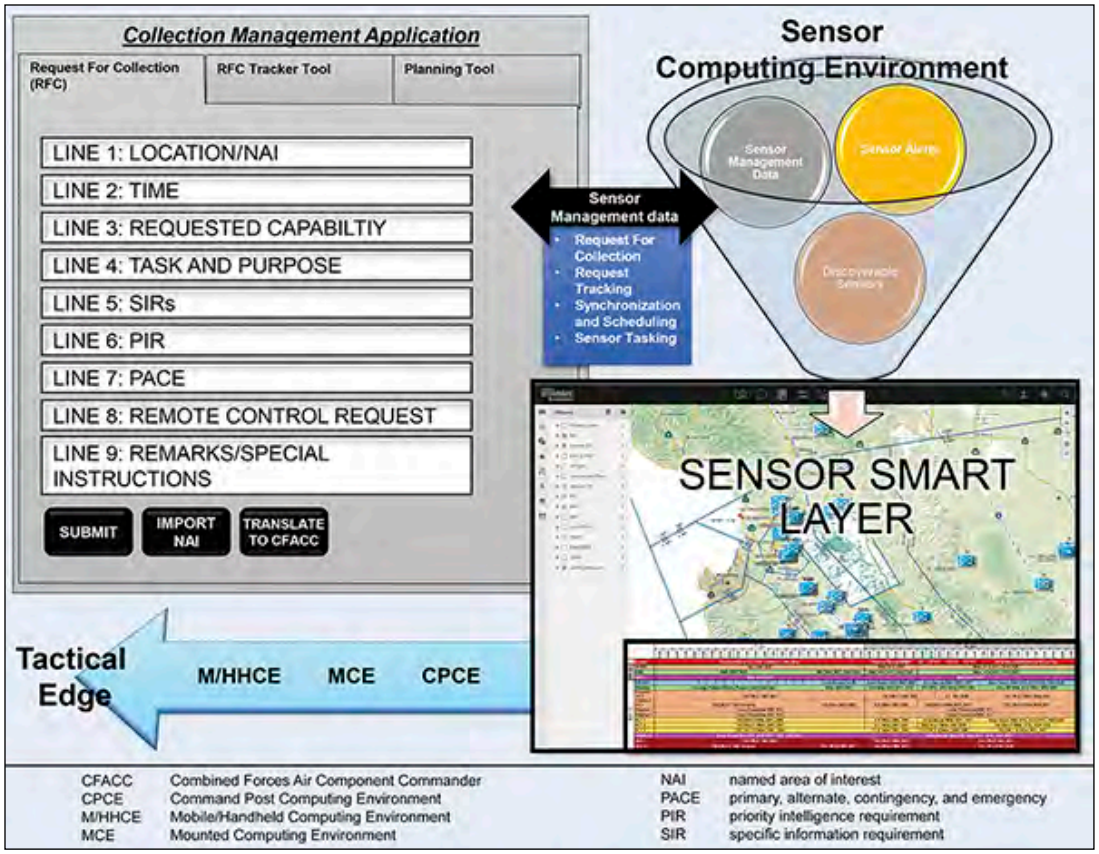


Figure 1. Collection Management Cross-Cutting Capability Conceptual View

The Army should pursue and develop an incremental and holistic strategy for implementing automation and artificial intelligence/machine learning into collection management.

The collection management cross-cutting capability will provide data users (consumers) a direct digital connection with data providers (collectors, sensor managers, and sensors). The collection management cross-cutting capability will reduce the burden on collection managers by standardizing data and digital planning tools and by digitizing a standard request for collection, a sensor COP, and digital collector/sensor tasks through a common collection management application and data standard.

To achieve full operational integration, the collection management cross-cutting capability will fully standardize and link threat data to collection requirements and sensor alerts. Threat data imported from the military intelligence All-Source App must be able to automatically provide enemy order of battle information, including individual object/unit identification. Additionally, technical data must be automatically imported and created into specific information requirements and technical indicators. A common data model must digitally link enemy order of battle, enemy courses of action, event templates, collection plans, and automated collector and sensor tasks. For instance, an analyst creates a named area of interest (NAI) for an enemy tank battalion. The metadata associated with the enemy tank battalion will be digitally linked with specific NAIs and aligned to a priority intelligence requirement. The collection requirement for the enemy tank battalion will then be imported into the Collection Management App for future planning. The Collection Management App will make

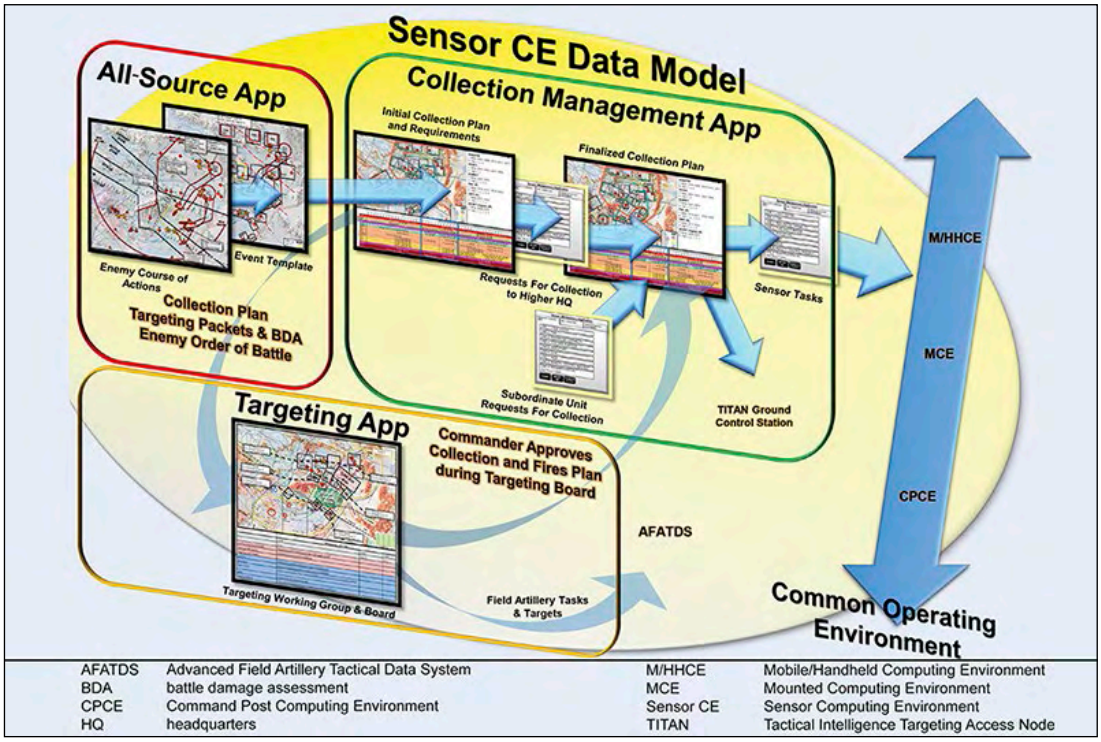


Figure 2. Common Operating Environment Collection Management Conceptual Overview

recommendations on what collection assets and sensors are available to task and what higher assets are available that could collect on the requirement. Once the collection manager assigns an approved collection asset for the tank battalion, sensor tasks, with the associated metadata, are sent to sensor managers via the Sensor CE. An example at a future brigade combat team would be as follows: A terrestrial collection system is tasked with conducting an area reconnaissance of the specific tank battalion's NAI, and the terrestrial sensor operators will have access to all technical metadata related to the associated enemy tank battalion order of battle, course of action, and event template.

The collection management cross-cutting capability will create an end-to-end digital feedback loop for data consumers and collectors to ensure that information is reported rapidly and accurately. This will be achieved by standardizing requests for collection on a single cloud-based application. The Collection Management App will allow requestors, collection managers, and sensor managers to track requests and collection tasks and provide real-time feedback on the status of requests. Additionally, a digital link will be created between data consumers and tasked sensors through Sensor CE's automated sensor alerts and subscriptions. Once a request for collection is approved and a collector or sensor is assigned, the consumer will automatically be subscribed to the sensor's alerts.

The collection management cross-cutting capability will enable the creation of a user-defined COP tailored to the collection mission. Users will have the ability to visually depict sensor and collection management data on a Command Post Computing Environment layer of the COP. The sensor layer of the COP will be visible on the move and at the halt from the Command Post Computing Environment, Mounted Computing Environment, and Mobile/Handheld Computing Environment. The sensor layer of the COP allows leaders and users to understand current collection and sensor operations. In addition, sensor data users will be able to view collection management plans such as a synchronization matrix and NAIs.

The collection management cross-cutting capability will enable the control of sensors via the network rather than "at the sensor source." By digitally linking requests for collection with sensor control software, we will in effect create the "network of things" of intelligence, surveillance, and reconnaissance. The Collection Management App, Sensor CE, emerging sensors or platforms, and future ground control station software will allow consumers such as infantry or armor company commanders to digitally submit requests for collection on their mounted or dismounted end-user devices and receive direct support from higher-level collection assets. The networked control of sensors will allow users to develop the situation rapidly, retain freedom of maneuver, and gain and maintain enemy contact more efficiently.

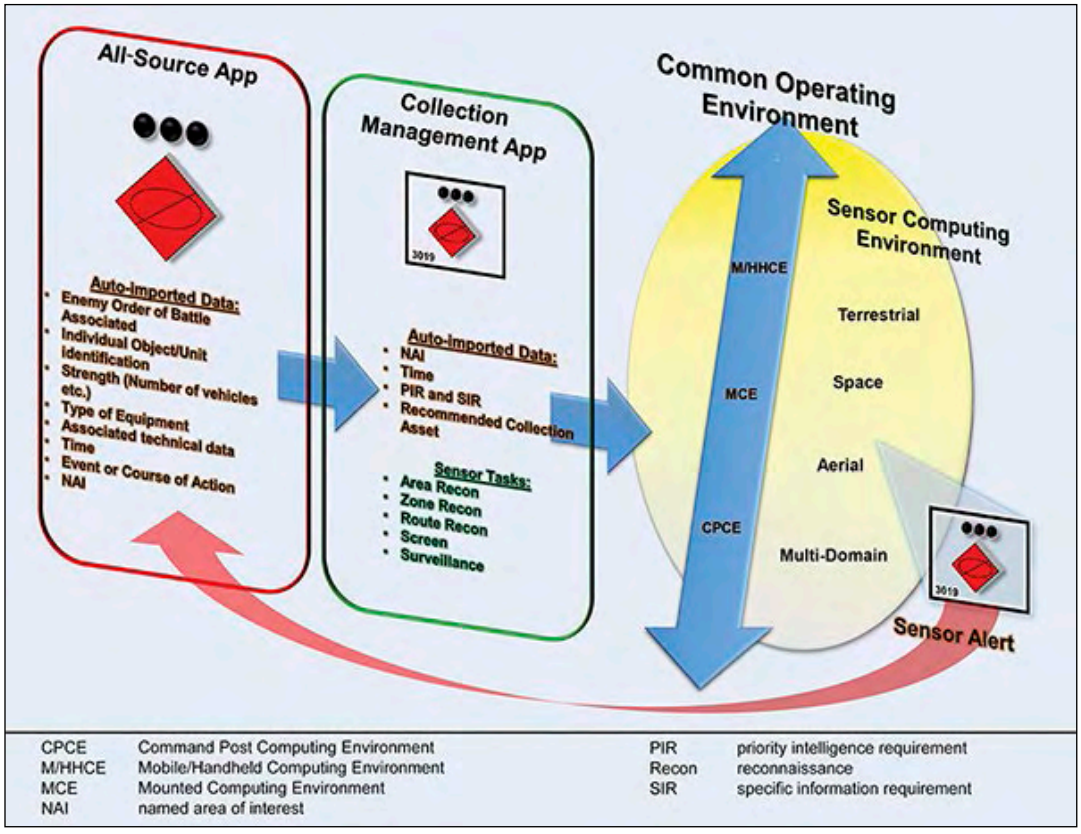


Figure 3. All-Source App to Sensor Data Linkage Concept

The collection management cross-cutting capability will enable sensor-to-sensor automatic cueing. Sensor CE's sensor-to-sensor data exchanges enable sensor-to-sensor automatic cueing. Automatic cueing will allow commanders or authorized users (collection managers and sensor managers) the capability to define sensor-to-sensor cueing relationships. Authorized users will have the ability via the Collection Management App's Planning Tool to plan digital cueing relationships between two or more sensors or collectors. Once collection managers establish a cueing relationship

between sensors, the system will automatically subscribe the cued sensor to the cueing sensor's alerts. Cueing alerts will be sensor-to-sensor automatic and sensor-to-sensor operator/manager for human-controlled sensors.

In the long term, the collection management cross-cutting capability and Sensor CE will provide the underlying data framework and services for automated, autonomous, and artificial intelligence-controlled sensor operations. These will include preprogrammed automated sensors, dynamic autonomous sensors that react to the operational environment, and artificial intelligence-controlled sensors that operate using feedback loop algorithms. Conceptually, users will input information requirements into the Collection Management App where artificial intelligence will resource, task collection, and allocate PED to answer the requirement. The transition to automated, autonomous, and artificial intelligence-controlled collection management will also necessitate the integration of cloud and artificial intelligence-enabled PED. The DoD's and Army's future initiatives, along with private sector innovations, will eventually provide artificial intelligence and machine learning algorithms to identify military targets with a high level of accuracy.[15] For instance, a British company is developing algorithms to apply machine learning to satellites' imagery for the identification of military aircraft with a reported accuracy rate of 98 percent.[16] Additionally, Microsoft has built a sophisticated software capability that allows artificial intelligence/machine learning to detect various patterns that identify snow leopards in snowy terrain using images and data from game cameras (camera traps). Biologists deploy motion-sensing cameras in the snow leopard habitat that capture images of snow leopards, prey, livestock, and anything else that moves. It then sorts through the images to find the ones with snow leopards in order to learn more about their populations, behavior, and range. Over the years, these cameras have produced more than 1 million images. [17] The collection management cross-cutting capability will provide users with edge-to-cloud access and the ability to request/task automated, semiautonomous, and autonomous sensors and to receive automated support with real-time sensor alerts.

The DoD, the Joint Staff, and the Army need to create a joint governing body that develops joint collection management concepts, doctrines, procedures, and technical standards. We can achieve MDO convergence of all sensors and all shooters only through the interoperability of doctrine, data, and network transport standards. Once the DoD establishes doctrinal and technical standard for collection management, it must expand interoperability to coalition partners in support of the mission partner environment. Interoperability with coalition partners, such as ABCANZ, will further enable MDO.

Conclusion

The Army lacks sufficient capability to fully integrate and synchronize all collection assets, sensors, and sensor data in real time to defeat a future peer threat in MDO and large-scale ground combat operations. The increase in the number of sensors, volume of data, and collection requirements will overburden future collection managers and will increase the risk of violating the seven fundamentals of reconnaissance. In order to mitigate this risk and enable collection management, the Army must invest in a collection management cross-cutting capability that standardizes and automates collection management command and control. This will provide the capability to discover, access, and manage interoperable sensor data from all warfighting functions, domains, and joint and coalition partners in support of MDO.

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), 19.

2. Ibid., 20.

3. "Command Post Computing Environment," Program Executive Office Command Control Communications-Tactical website, accessed 24 June 2020, https://peoc3t.army.mil/mc/cpce.php.

4. Nancy Jones-Bonbrest, "Army forges ahead with Common Operating Environment for mission command," U.S. Army Worldwide News, October 25, 2017, https://www.army.mil/article/195864/army_forges_ahead_with_common_operating_environment_for_mission_command; and Department of the Army, *Common Operating Environment* (Washington, DC, October 2015), https://asc.army.mil/web/wp-content/uploads/COE_Flip_Book.pdf.

5. Kevin McCaney, "Next step for tactical nets: Sensors that know how to share," Defense Systems, January 9, 2015. https://defensesystems.com/articles/2015/01/09/army-integrated-sensor-architecture-tactical-network.aspx; and U.S. Army CCDC C5ISR Center, "CERDEC Integrated Sensor Architecture," YouTube video, 3:59, April 6, 2015, https://www.youtube.com/channel/UCuKIFn85_cr0pfHd5pCk84w.

6. Christine L. Moulton, Susan Harkrider, John Harrell, and Jared Hepp, *Integrated Sensor Architecture (ISA) for Live Virtual Constructive (LVC) Environments* (27 March 2014), https://apps.dtic.mil/docs/citations/ADA636887.

7. Sean Kimmons, "TITAN system being developed to tie 'deep sensing' to long-range fires," U.S. Army Worldwide News, October 24, 2019, https://www.army.mil/article/228867/titan_system_being_developed_to_tie_deep_sensing_to_long_range_fires.

8. Ashley Tressel, "Martin: 'Project Convergence' to explore Army's role in JADC2," Inside Defense, March 10, 2020, https://insidedefense.com/insider/martin-project-convergence-explore-armys-role-jadc2; and Patrick Tucker, "The US Army Wants to Reinvent Tank Warfare with AI," Defense One, October 18, 2019, https://www.defenseone.com/technology/2019/10/us-army-wants-reinvent-tank-warfare-ai/160720/.

9. Kerensa Crum, "CCDC Aviation, Missile Center highlights forward-launched UAS technology," U.S. Army Worldwide News, March 30, 2020, https://www.army.mil/article/234100/ccdc_aviation_missile_center_highlights_forward_launched_uas_technology.

10. Jed Judson, "General Atomics demos Gray Eagle's role in multidomain ops," Defense News, January 22, 2020, https://www.defensenews.com/land/2020/01/22/general-atomics-demos-gray-eagles-role-in-multidomain-ops/; and Jed Judson, "US Army to launch drone from helicopter for first time this year," Defense News, May 1, 2018, https://www.defensenews.com/digital-show-dailies/aaaa/2018/05/01/army-to-launch-drone-from-helicopter-for-first-time-this-year/.

11. "OFFensive Swarm-Enabled Tactics (OFFSET)," Defense Advanced Research Projects Agency, accessed 24 June 2020, https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics.

12. Kelsey D. Atherton, "DARPA want commanding robots to work like a video game," C4ISRNet, February 11, 2020, https://www.c4isrnet.com/unmanned/2020/02/11/darpa-wants-commanding-robots-to-work-like-a-video-game/.

13. Paragraphs 1-37 through 1-44 of FM 3-55, *Information Collection*, discuss the seven fundamentals of reconnaissance in relation to information collection activities. Department of the Army, Field Manual 3-55, *Information Collection* (Washington, DC: U.S. Government Publishing Office, 3 May 2013), 1-7, 1-8.

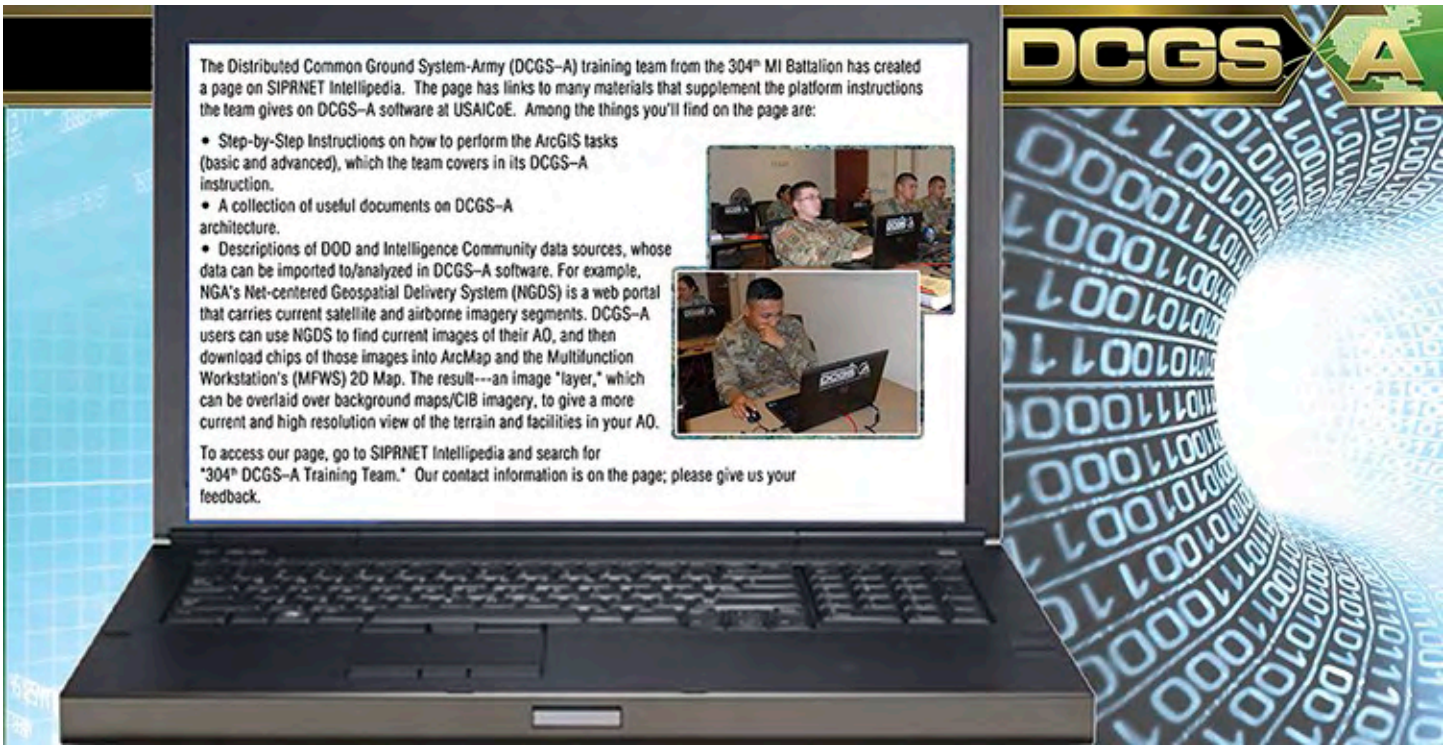
14. Ibid., 1-7.

15. Charlie Kawasaki, "6 Ways AI can make sense of sensor data in 2020," C4ISRNet, February 14, 2020, https://www.c4isrnet.com/thought-leadership/2020/02/14/6-ways-ai-can-make-sense-of-sensor-data-in-2020/.

16. "Battle algorithm: Artificial intelligence is changing every aspect of war," *The Economist,* September 7, 2019, https://www.economist.com/science-and-technology/2019/09/07/artificial-intelligence-is-changing-every-aspect-of-war.

17. Mark Hamilton, Sudarshan Raghunathan, Akshaya Annavajhala, Danil Kirsanov, Eduardo de Leon, Eli Barzilay, Ilya Matiach, Joe Davison, Maureen Busch, Miruna Oprescu, Ratan Sur, Roope Astala, Tong Wen, and ChangYoung Park, "Flexible and Scalable Deep Learning with MMLSpark," *Proceedings of Machine Learning Research* 82 (October 2017): 11–22, http://proceedings.mlr.press/v82/hamilton18a/hamilton18a.pdf; and Databricks, "Microsoft Announces Support for MLflow, Delta Lake and More–Rohan Kumar (Microsoft)," YouTube video, 23:11, April 25, 2019, https://www.youtube.com/watch?v=T_fs4C0aqD0&feature=youtu.be&t=425.

CPT Michael Kossbiel is the commander of Headquarters and Headquarters Company, U.S. Army Intelligence Center of Excellence. His previous assignments include sensor computing environment team lead, Intelligence-Capabilities Development and Integration Directorate, Army Futures Command; assistant S-2 for 3rd Armored Brigade Combat Team, 1st Cavalry Division; battalion S-2 for 215th Brigade Support Battalion; and intelligence advisor to the Royal Saudi Land Forces under Joint Special Operations Task Force-Arabian Peninsula. He is a graduate of Armor Basic Officer Leaders Course, Military Intelligence Officer Transition Course, and Military Intelligence Captains Career Course.



Improving Brigade Combat Team Intelligence Collection Operations for Large-Scale Ground Combat

by Major William Denn, Major Jason Turner, and Captain Adam Wojciechowski

Where and When Will the Enemy Attack?

After detailed mission analysis, the brigade staff was confident they knew where and when the enemy would attack. Over the next 2 days, the engineers dug extensive battle positions, platoons rehearsed their plan, scouts seeded observation posts, and intelligence analysts watched their drone feeds to give advanced warning. When the enemy did arrive, they attacked with such speed and audacity that before the brigade knew it, the enemy had penetrated their defenses and was heading straight for their command post. Every echelon was surprised: the intelligence analysts, the scouts forward, and the platoons in their defensive positions—there was little advance warning. While this is a hypothetical vignette, unfortunately this scenario occurs far too often at the U.S. Army's combat training centers.

Introduction

The U.S. Army is undergoing a dramatic shift in training competencies to fight in large-scale combat operations rather than the counterinsurgency and advisory missions of the past 17 years in Iraq and Afghanistan. Brigades are learning that large-scale ground combat operations require fundamentally different skillsets and competencies than the counterinsurgency fight of the past. Because of how quickly the battlefield moves—at the speed of mechanized forces attacking over large distances—the above vignette is an illustration of how brigades fail to layer their intelligence collection over large areas to give friendly forces enough warning and certainty of enemy intentions to adequately prepare for combat.

In the last year, after having observed multiple brigades encounter similar challenges at the U.S. Army Joint Multinational Readiness Center, we, the authors, have identified several challenges that brigades must address:

- Manning and training an intelligence collection management team at the brigade level that is able to adequately plan and synchronize an effective collection strategy.
- Scoping the brigade's deep fight sufficiently to give the brigade enough advance notification to prepare for contact with the enemy.
- Layering intelligence, surveillance, and reconnaissance (ISR) assets appropriately to increase the chances of detection; planning intelligence handover to coordinate between these ISR assets (and units); and ultimately enabling targeting of the enemy throughout the depth of the battlespace.

Manning and Training Collection Management Cells

The role of the brigade collection manager is essential for planning an effective collection strategy to satisfy the commander's intelligence gaps; for synchronizing the brigade's ISR assets (including the cavalry squadron and radars); and for integrating higher, joint, theater, and national-level ISR assets. However, the struggle for brigades is that no formalized collection manager position exists in the modified table of organization and equipment. Units choose a collection manager from existing personnel, usually a lieutenant or junior captain, in a part-time capacity. This often untrained collection manager then attempts to conduct the difficult task of planning and managing the entire ISR

enterprise for the brigade. Even when collection managers have received training, for example at the U.S. Army Intelligence Center of Excellence (USAICoE) or Defense Intelligence Agency, they are unprepared to effectively synchronize and integrate units such as the cavalry squadron; to participate in brigade battle rhythm events like military decision-making process (MDMP) wargaming and information collection/fires rehearsals; and to contribute to targeting working groups.

U.S. Army photo by PFC Courtney Hubbard

U.S. Soldiers of the 1st Armored Brigade Combat Team, 3rd Infantry Division, provide information to ground units from the tactical operations center while a Latvian soldier, right, observes during exercise Combined Resolve IV at the U.S. Army's Joint Mulitnational Readiness Center in Hohenfels, Germany, May 17, 2015.

Collection management is a complex enough task that it requires a team to manage all collection management requirements. Successful brigades dedicate at least four to six intelligence analysts to aid the collection manager in planning, ISR current operations management, assessments, and targeting—especially in support of 24/7 operations.

Successful brigades will effectively use subordinate liaisons, especially from their cavalry squadron, to integrate into collection management working groups to plan and task assets and units for collection. This allows subordinates to help aid in refinement based on their knowledge of their own capabilities. This input is essential to refine the information collection synchronization matrix that is included in daily fragmentary orders with the specific indicators and source of reporting their assets and teams must answer.

Today's ISR capabilities are also increasingly complex and rapidly changing with technology. There is little expectation that a junior captain can be a subject matter expert in what these ISR assets can or cannot collect. Therefore, it is important to integrate the brigade's warrant officers into collection management planning. The brigade's military occupational specialty (MOS) 352N (Signals Intelligence Analysis Technician), MOS 351M (Human Intelligence Collection Technician), and MOS 131A (Field Artillery Targeting Technician) are especially critical. For example, unused by most brigades is the ability for the Q50/53 counterfire radar to be employed as an ISR asset by reporting lines of bearing whenever enemy counterfire radar transmissions are detected. Without input from these warrant officers, these nonconventional ISR assets will not be included in a brigade's information collection synchronization matrix.

The brigade's ad hoc collection management team must not fight for the first time at a combat training center or in combat. They require practice and training as a team in order to understand what outputs they must produce and how they integrate into a brigade staff within planning (MDMP) and execution (current operations). USAICoE's standardization of military intelligence certification through the Military Intelligence Training Strategy (MITS) framework is an important first step in identifying the need to train and certify collection management crews. Rarely, however, are brigade combat teams (BCTs) arriving at the Joint Multinational Readiness Center with a certified collection management crew that trained together in a previous MITS exercise, nor are they using established collection management standard operating procedures to structure how they operate. BCT commanders and S-2s must place more emphasis on establishing and training their collection management teams before combat training center rotations. Successful BCTs operationalize their collection management cells to operate year-round, even in garrison, rather than on an ad hoc basis during brigade collective training events.

Finally, while school options exist for collection managers, we are not yet observing school-trained collection managers successfully operating at the BCT level. We encourage USAICoE to improve its collection management program of instruction, focusing on—

- Managing and leading a collection team.
- Leveraging joint asset capabilities.
- Integrating collection management into the BCT rehearsals, MDMP (course of action development and wargaming), and targeting process.

Scoping the "Deep Fight"

Within the counterinsurgency era, the BCT often lacked a "deep fight," instead focusing on the needs of platoons and companies in a close tactical fight. Within a large-scale ground combat operations environment, a BCT's deep fight is essential to mission success. FM 3-0, *Operations,* defines the deep area as, "the portion of the commander's area of operations that is not assigned to subordinate units. Operations in the deep area involve efforts to prevent uncommitted or out of contact enemy maneuver forces from being committed in a coherent manner or preventing enabling capabilities […] from creating effects in the close area. […] The purpose of operations in the deep area is to set the condition for success in the close area or to set the conditions for future operations."[1]

Brigades often struggle with where they should define the deep fight. Brigades typically arrive at a combat training center with their maps limited to the geographic training area boundaries or the area of operations boundaries dictated to them by their higher headquarters. Especially for a combat training center like the Joint Multinational Readiness Center, which has a relatively small training area (10 kilometers by 20 kilometers), this decision on the scope of their maps is their first lost opportunity and requires coaching. From an intelligence collection perspective, the brigade's deep fight extends much farther outside the dictated area of operations.

U.S. Army doctrine provides us with assistance to help understand a brigade's deep fight using the concept of area of influence. ATP 2-01.3, *Intelligence Preparation of the Battlefield,* defines an area of influence as "a geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander's command or control. The area of influence includes terrain inside and outside the [area of operations] AO and is determined by both the G-2/S-2 and G-3/S-3."[2]

During mission analysis, brigades typically show their area of operations or area of interest but do not refer to their area of influence. As a concept, the area of influence provides additional space so that the brigade cannot only see the enemy with ISR assets but also has the space to shape the enemy using indirect fires, maneuver, or aviation assets. When the area of influence extends outside the area of operations, coordination with higher headquarters or adjacent units is required. To ignore it shrinks the brigade's focus and increases the likelihood of tactical surprise by the enemy. Moreover, just because the higher headquarters plans for an intelligence handover line does not mean they will focus collection on the near side of it.

Our recommendation is for brigades to consider the full extent of their area of influence and to conduct appropriate mission analysis (terrain, enemy, and friendly capabilities) to maximize the brigade's ability to target and shape within the area of influence before the enemy enters the brigade's area of operations.

Layering ISR to Maximize Detection and Targeting

If a brigade can properly man and train its collection management cell and give the cell enough geographic and temporal space to plan for during mission analysis, then the final key to success is to plan and layer the ISR appropriately to find the enemy.

As part of mission analysis, a BCT S-2 and a collection manager must first consider their overall approach to collection management. JP 2-01*, Joint and National Intelligence Support to Military Operations,* advises, "When developing a collection plan, collection managers should consider whether to maximize efficiency by dispersing collection assets across the widest geographic area in order to maximize collection, or place them in nearby or the same geographic areas to overlap their sensor ranges for synergistic effects, thus providing more opportunities for dynamic tipping and cueing, asset mix, and/or asset redundancy."[3] This concept of asset convergence or dispersion is determined based on whether the enemy course of action is clear versus unknown. For combat training center rotations, the brigade typically understands from where and when the enemy is expected to approach, and we subsequently recommend that the brigade attempt to maximize asset convergence.

Reliance on one type of collection asset severely restricts the level of certainty and dramatically increases the mission risk of not identifying a target. Collection managers must analyze the best assets to answer the commander's intelligence needs and should attempt to layer (or mix) complementary ISR assets to further increase the likelihood of observation. Figure 1 (on the next page), from JP 2-01, illustrates some of these planning factors; however, we recommend collection managers also study ATP 3-55.3, *ISR Optimization—Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization,* published

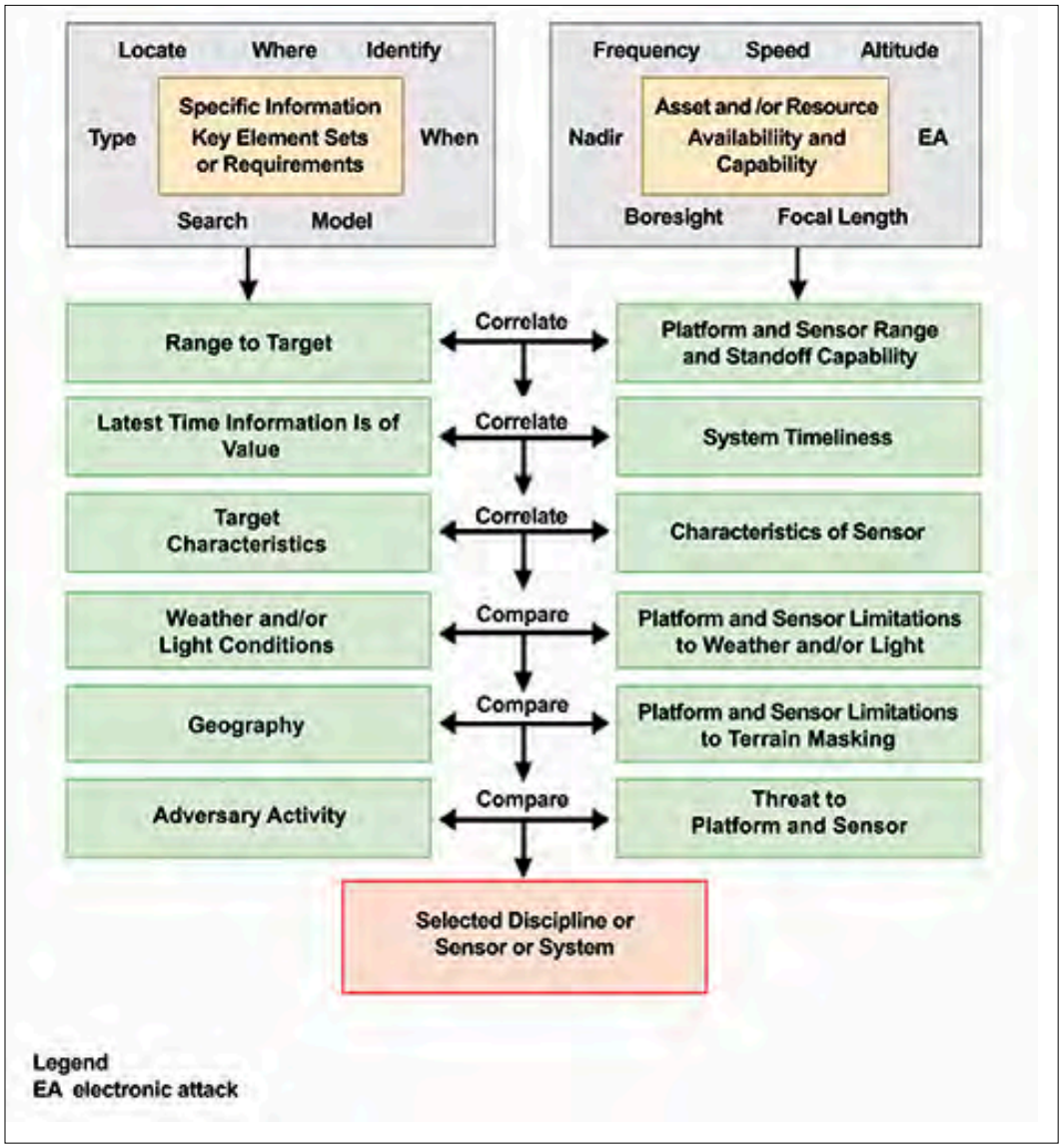


Figure 1. Asset and/or Resource Availability and Capability Factors[4]

in September 2019. ATP 3-55.3 provides more detailed guidance on ISR employment for specific mission requirements based on capabilities.

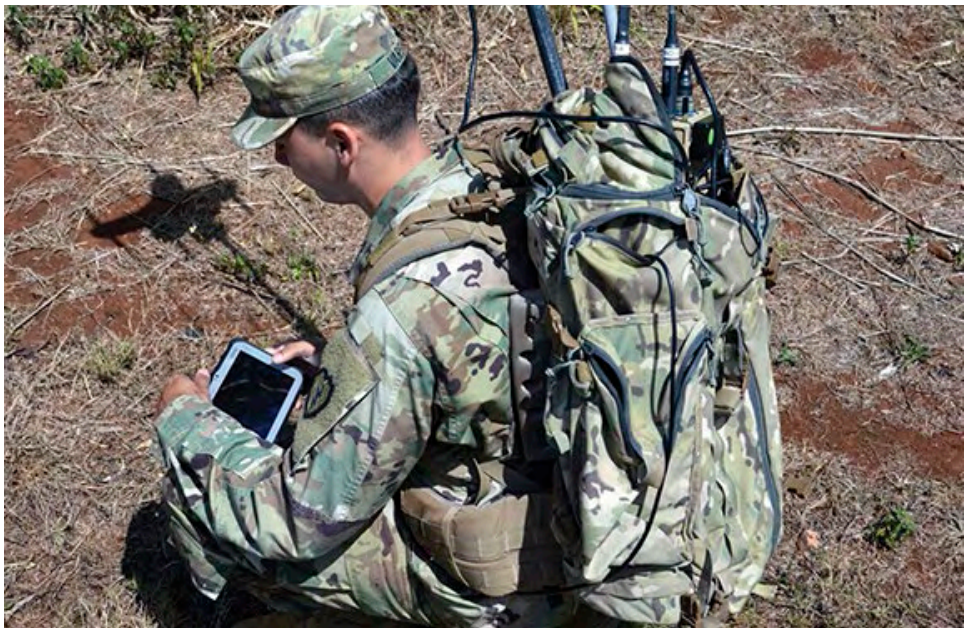
Once assets are determined appropriate or not, brigades typically fail to consider layering ISR assets in order to mass their effects. Layering ISR begins with theater collection, like the Joint Surveillance Target Attack Radar System (JSTARS), which provides important ground moving target indicator intelligence as the enemy moves in the brigades' deep areas. With regard to JSTARS, brigades understand the concept of cueing onto a full-motion video asset, but then they over-rely on their aerial full-motion video ISR (division MQ-1C Gray Eagle or brigade RQ-7B Shadow).

Most brigades fail to task their cavalry formations, infantry/armor battalions, or fire support teams to observe multiple named areas of interest to confirm or deny enemy courses in conjunction with their aerial ISR to enable targeting. Battalions also arrive unprepared to leverage their own organic battalion-level ISR assets, like small unmanned aircraft systems or their own scout platoons. Moreover, brigades struggle to publish a daily information collection synchronization matrix with their fragmentary orders to inform or direct ISR assets, like their cavalry squadron. When weather turns poor, or division assets redirect to higher priority missions, brigades are unprepared because they have not adequately layered all-weather redundant ISR assets, again, like their cavalry squadron.

Brigades do not conduct effective intelligence handover between these assets and units. To avoid surprise, brigades must plan and conduct deliberate intelligence handovers with ISR assets. It starts with an initial notification of enemy movement with theater deep assets in the division area of operations and an assessment by the brigade's current operations floor of what routes and time horizons the enemy is expected to take. Brigade aerial ISR then should acquire the enemy to enable further advance warning and enable brigade indirect fire shaping. The brigade's current operations section should prepare to tip and pass these targets to their reconnaissance squadron in their series of observation posts or scout sections in depth. After the handover of these targets, the brigade should be free to return their aerial ISR to focus back on the brigade's deep areas. Finally, the reconnaissance squadron conducts a deliberate handover of these targets into the infantry/armor battalions' close fight where remnants of the enemy are eventually destroyed.

The intelligence handover of targets is a difficult and deliberate process that requires planning, graphic control measures, and rehearsals. Currently, brigades are not conducting effective information collection technical rehearsals, information collection and fires rehearsals, and

combined arms rehearsals to synchronize the handover of the enemy from the brigade's deep areas into the battalions' close fight. While outside the scope of this article, we recommend brigades spend some effort to understand what is necessary to rehearse in the information collection and fires rehearsal to shape the deep fight and conduct effective intelligence handover.



U.S. Army photo by SSG Armando R. Limon

An electronic warfare specialist with 2nd Brigade Combat Team, 25th Infantry Division, operates a Versatile Radio **Observation and Direction finder at Schofield Barracks, HI.**

Conclusion

The evolution of our fundamental skillsets while linking ISR to targeting across the BCT will continue to use much that the BCT has to offer. We focused on three areas that will allow BCTs to capitalize on the myriad of collection assets and increase their lethality:

- Ensuring a collection management team exists and trains together year-round to plan and synchronize the BCT's collection strategy.
- Conducting analysis of the area of influence to understand and plan for the BCT's deep fight. By doing so, a BCT can conduct a systematic attrition of its enemy instead of simply reacting to contact. To guarantee success in identifying the enemy, the BCT must maximize the utilization and layering of its ISR assets, including its reconnaissance squadron and nonstandard ISR like counterfire radars.
- Conducting an effective information collection and fires rehearsal because it is important for all operators to understand the sensor-to-shooter plan.

As the U.S. Army continues training BCTs for large-scale war, we must relearn many of these fundamentals of large-scale ground combat operations so that we can maximize capabilities to defeat our Nation's emerging threats. Implementing these recommendations will likely reverse several negative trends identified during multinational brigade-level exercises at the combat training centers, specifically in the areas of information collection management and synchronization of information collection and fires.

Endnotes

1. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 1-34. Change 1 was issued on 6 December 2017.

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

3. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 5 July 2017), III-30.

4. Ibid., III-23.

MAJ William Denn is an intelligence observer coach/trainer at the Joint Multinational Readiness Center (JMRC) in Hohenfels, Germany. He holds degrees from the U.S. Military Academy at West Point, Harvard University, and the U.S. Army School of Advanced Military Studies. His is a former brigade combat team S-2 from the 82nd Airborne Division.

MAJ Jason Turner is a fires observer coach/trainer at JMRC in Hohenfels, Germany. He previously served in the 2nd Infantry Division as the division artillery deputy commanding officer and S-3; the 2nd Battalion, 17th Field Artillery Regiment battalion S-3; and the 2nd Stryker Brigade Combat Team, 2nd Infantry Division, fire support officer.

CPT Adam Wojciechowski is an intelligence observer coach/trainer at JMRC in Hohenfels, Germany. He was the opposing force S-2 at the Joint Multinational Readiness Center, an instructor at the Military Intelligence Basic Officer leader course, and the 173rd Brigade Support Battalion S-2.

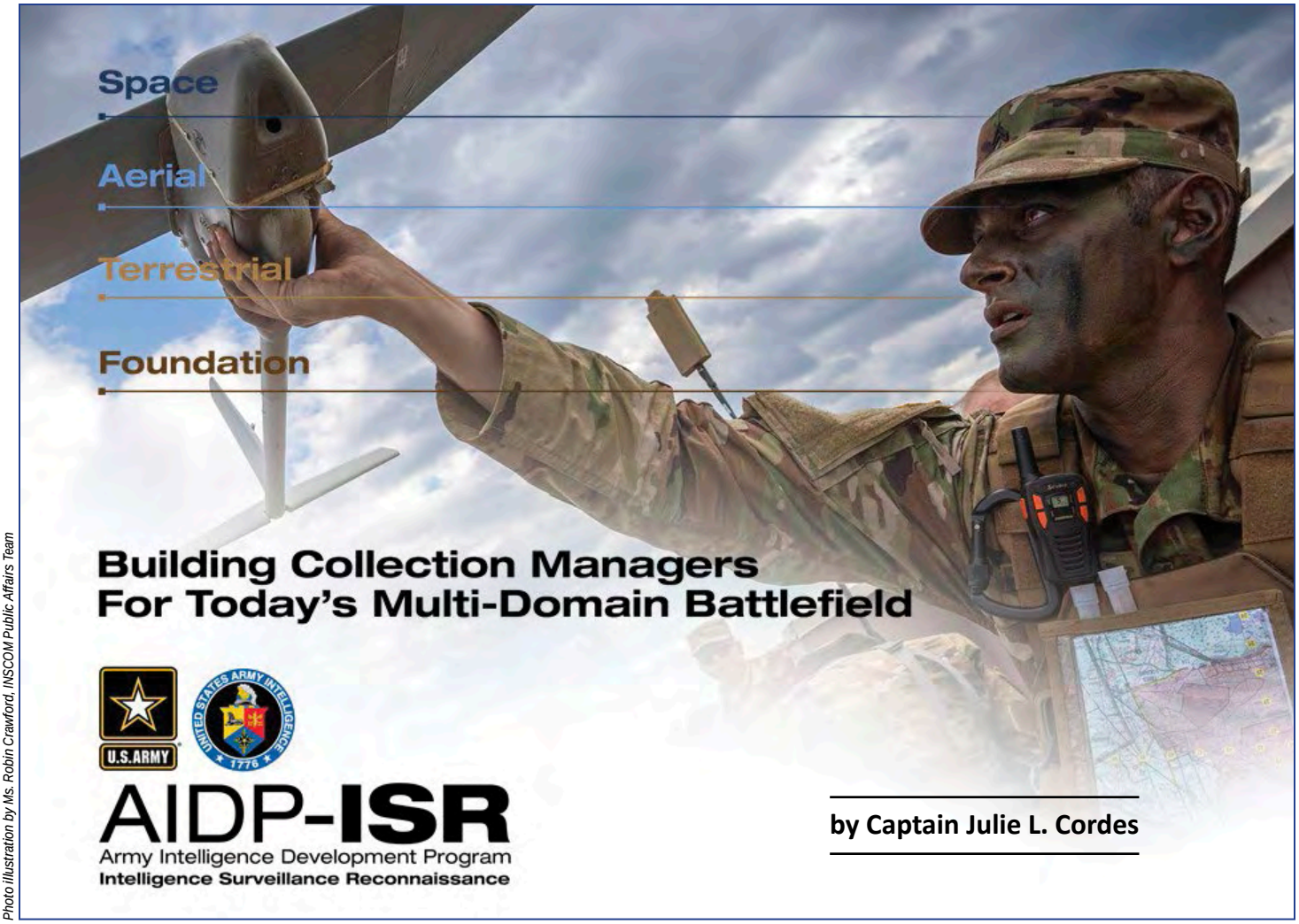


Photo illustration by Ms. Robin Crawford, INSCOM Public Affairs Team

Building Collection Managers For Today's Multi-Domain Battlefield

AIDP-ISR
Army Intelligence Development Program
Intelligence Surveillance Reconnaissance

by Captain Julie L. Cordes

Following the loss of a division Gray Eagle to enemy air defense artillery (ADA) systems, the G-2 collection manager coordinated with division artillery to provide suppression of enemy air defense (SEAD) in support of armed Gray Eagle flights. The SEAD fires forced the enemy to conduct survivability moves to protect ADA assets, allowing the Gray Eagles to fly unopposed to identify and destroy enemy ADA systems with *hellfire missiles*.[1]

Introduction

Thirty years ago, military intelligence forward thinkers envisioned a time when a collection manager—as the pivotal position in our G-2 sections—would orchestrate the intelligence system for an entire command, ensuring the G-2, corps or division commander, and subordinate commanders promptly received the intelligence they needed.[2] In the year 2020, we are there!

The U.S. Army's premier collection management professional development program is being restructured under the guidance of the U.S. Army Intelligence and Security Command (INSCOM) and U.S. Army Forces Command (FORSCOM) G-2 to develop experts in collection management for today's multi-domain operations environment. Under the new construct, the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance (AIDP–ISR) program graduates will be ISR scientists—experts who perform at a higher rate than their peers and go on to carry the mantle of finding and knowing the enemy through operationalizing the collection plan. AIDP–ISR already excels at preparing selected officers and warrant officers for the next phase of their career, not only as collection managers but also as all-source intelligence leaders.

Program History and Evolution

When INSCOM started the National Systems Development Program (NSDP) in 1992, the intent and focus were to develop a cohort of officers who would be proficient in the collection of the next generation of strategic, unconventional space-borne signals intelligence and imagery intelligence systems. Efforts to support warfighters in the early 2000s caused an evolution of the program, including the management of national-level human intelligence collection. INSCOM formally approved the change in 2004, and NSDP

became a training program focused on creating all-source national- and theater-level asset smart collection managers.

During the early to mid-2000s, NSDP cohorts consisted of three board-selected military intelligence officers who were advanced course graduates and had already served in a company command position. The officers completed the designated program of instruction and then received their assignments in the field, sometimes moving directly to a combat zone as a collection manager.[3]

In the years since, the Army's Military Intelligence Programs Office at Human Resources Command (HRC) adopted an intelligence development program focused on collection management as a professional development program chartered to produce qualified junior officers (senior captains or new majors) and warrant officers. Students gain an understanding of how to bring national and theater intelligence systems to the fight—supporting warfighters at the corps levels and below.[4] AIDP–ISR was the first of such programs, and using its successful model, HRC developed two additional specialized tracks—one with a focus on counterintelligence (CI), AIDP–CI, and one with a focus on cyber operations, AIDP-Cyber. The Army considers all AIDP graduates to be operational and planning experts in their respective disciplines.

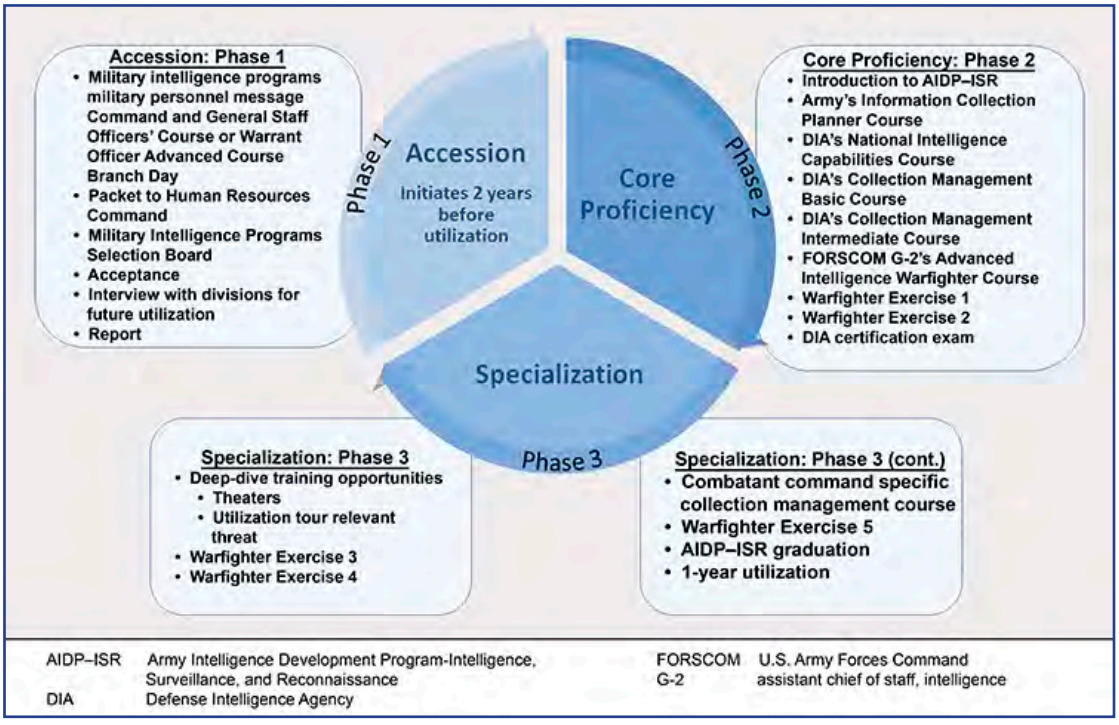
Multi-Domain Operations

The United States is in a state of continuous competition with peer and near-peer adversaries capable of contesting the United States in all domains—land, sea, air, space, cyberspace, and the electromagnetic spectrum. Our adversaries seek to separate U.S. forces and our allies in time, space, and function in order to defeat us. Moving forward, the Army identified the need to leverage available information from collection platforms to enable commanders and staffs at echelon to visualize and operate in all domains.[5] Gaining cross-domain overmatch against a peer or near-peer threat through rapid and continuous integration of capabilities in all domains, a tenet known as *convergence,*[6] can only be accomplished with specially selected and well-trained collection managers operating at every echelon. Building those collection managers for the corps and division levels is the end state we intend to achieve through the newly revamped AIDP–ISR.

Contrasting Past and Future: FY 2021 and Beyond

Previous versions of the program sought to broadly address newly emerging collection capabilities in support of counterinsurgency and counterterrorism operations. Program electives, previously selected based on preference, course seat availability, and funding, did not match graduates to tactical Army requirements. Indeed, some graduates of prior programs have never served as a collection manager—the stated objective of the program since its inception.

AIDP–ISR is gearing up to annually train a collection manager for every validated division- and corps-level position. Future AIDP–ISR cohorts can expect changes intended to bring program requirements in line with the needs of today's division and corps G-2s for large-scale ground combat operations. AIDP–ISR will now be a three-phased program consisting of accession, core proficiency, and specialization, illustrated in the figure below.



Graphic adapted from original provided by CPT Julie Cordes

New AIDP–ISR Continuous and Overlapping 2-Year Phased Cycle Program Design

Accession Phase. This phase begins with the selection of applicants through the Military Intelligence Programs Selection Board. Successful applicants will conduct interviews and discussions with prospective division- and/or corps-level units

before their arrival at Fort George G. Meade, Maryland. The AIDP–ISR Program Management office will work with the FORSCOM G-2, INSCOM staff, Intelligence Center of Excellence, and HRC to develop curriculum requirements specific to each participant's post-program utilization assignment as a collection manager (additional skill identifier [ASI] 3F) in an Army division or corps headquarters. The needs of the Army become the driving force behind each AIDP–ISR student's tailored curriculum.

Core Proficiency Phase. Courses for this phase aim to ensure all AIDP–ISR graduates possess the ability to apply collection planning, tasking, asset synchronization, data mining/research methods, critical thinking/problem solving, and an understanding of the tactical and national/theater intelligence architecture and capabilities necessary to support combat operations across the full spectrum of multi-domain operations. These core courses include the—

- Army's Information Collection Planner Course.
- Defense Intelligence Agency's (DIA) National Intelligence Capabilities Course.
- DIA's Collection Management Basic Course.
- DIA's Collection Management Intermediate Course.
- FORSCOM G-2's Advanced Intelligence Warfighter Course.

The Air Force's Intelligence, Surveillance, and Reconnaissance Operators Course (IROC) provides a joint national, theater, and coalition focus. IROC is now a candidate for future inclusion in the Core Proficiency Phase; until then, students can take it later in the program as part of related specialized development. AIDP–ISR students will conclude this phase's requirements upon successful completion of a DIA certification examination to obtain the Certified Collection Manager Professional-Fundamentals credential.

Specialization Phase. A tailored Specialization Phase will produce collection managers prepared for utilization at a specific division- or corps-level assignment. These deep-dive training opportunities will be prioritized for students based on relevancy to their utilization tours and will include theater- and threat-specific collection management education. Students will also participate in warfighter exercises meant to further prepare them for their utilization and, when possible, align against their utilization assignment's warfighter exercise.

The addition of a mentorship program is also underway via direct and virtual opportunities. The program connects current cohorts of AIDP–ISR students to collection managers through a milSuite page for graduates of the program and those actively working collection requirements management across the enterprise. Collaboration through mentoring can only further enrich the overall impact of collection managers on the Army's multi-domain operations mission set.

Known Challenges

Historically, collection manager billets were not all coded with the 3F ASI[7] and not everyone who served in the capacity of collection manager within their respective corps or division graduated from the AIDP–ISR because assignments within a G-2 are determined locally. The high operational tempo of an Army corps and division headquarters, whether forward deployed or at home station, makes it extremely challenging to train and acclimate an incoming collection manager. With the robust and intense training AIDP–ISR offers to its students, graduates receive the foundational knowledge to advance their section and collection strategy for the G-2 and commander immediately upon assuming the new assignment.[8]

Besides the numerous qualifications and excellent training they receive through AIDP–ISR, officers are postured perfectly for their career as an Army field grade officer. Immediately after completing AIDP–ISR, graduates arrive at their next duty assignment, ready to fill a collection management key developmental billet for 12 to 24 months. AIDP–ISR graduates are then ready to complete 24 months in competitive, top-tier key developmental positions within the first 2 to 3 years of their promotion to major. This is a significant advantage because many officers need time to build credibility in order to earn a key developmental position when arriving at a new unit or new installation.[9] Collection management billets are high-profile positions that offer routine engagement with division and corps senior leaders. These billets also allow the AIDP–ISR graduate to demonstrate the desired competency for other follow-on key developmental positions, for example, brigade combat team S-2, analysis and control element chief, or military intelligence battalion S-3/executive officer.

Conclusion

Even with the advantage of the formal AIDP–ISR education, the synchronization requirements placed on collection management teams in terms of daily operations, assessments, and frequent allocation decisions are significant, giving greater importance to the initial pre-program selection process. The ideal candidate will possess a high level of emotional intelligence and the ability to form positive collaborative relationships outside their respective staff section. The strong fundamentals instilled through AIDP–ISR

are and will continue to be crucial to the success of the individual sitting in the collection manager billet.[10]

The U.S. Army's premier collection management professional development program is on a restructuring track that will reap dividends across the Army enterprise in response to the growing needs of our Nation's multi-domain operations requirements.

Endnotes

1. Department of the Army, *Warfighter 16-5 Final Exercise Report* (Fort Leavenworth, KS: Mission Command Training Program, June 2016), 9–10.

2. John H. Black and Kenneth A. Watras, "Collection Management/TENCAP 2000: The Revised CM/TENCAP Course," *Military Intelligence* 18, no. 2 (April–June 1992): 44–45.

3. Department of the Army, National Systems Development Program, 704th Military Intelligence Brigade program binder, 4 April 2005.

4. Department of the Army, Military Personnel Message 19-162, *Academic Year 2020-2021 Military Intelligence Programs and Advanced Civil Schooling* (Human Resources Command, 21 May 2019).

5. 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), xi.

6. Ibid., 20.

7. This is being remedied through synchronization efforts with the Office of the Chief of Military Intelligence, Military Intelligence Branch representatives at Human Resources Command, and AIDP–ISR.

8. Camero Song, "Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance: Critical to an Army Corps," *Military Intelligence Professional Bulletin* 44, no. 1 (January–March 2018): 52–54.

9. Ibid., 53.

10. Dwight L. DuQuesnay, "Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance (AIDP–ISR): A Senior Leader Perspective," *Military Intelligence Professional Bulletin* 43, no. 3 (July–September 2017): 16–20.

CPT Julie Cordes serves as the 742nd Military Intelligence Battalion current operations officer in charge and Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance (AIDP–ISR) program manager. She has successfully completed three 1-year combat deployments, most recently from 2018 to 2019, serving as the foreign disclosure officer in support of 75th Ranger Regiment operations in Afghanistan. CPT Cordes holds a bachelor of arts degree from the University of Iowa. She possesses the Army's 1D (Imagery Intelligence Officer) and 5P (Airborne) additional skill identifiers (ASIs). She also earned the Department of Defense's (DoD) Geospatial Intelligence (GEOINT) Professional Certification-Fundamentals credential and the Collection Requirements Manager Certification from the National Geospatial-Intelligence College.

Contributors:

MAJ Matthew Wright serves as the 2nd Brigade, 10th Mountain Division (LI) S-2 and previously served as the 10th Mountain Division's collection manager and dissemination chief. MAJ Wright holds a bachelor of arts degree in history from Virginia Tech and a master's degree in business administration from Webster University. He is a graduate of AIDP–ISR and possesses multiple ASIs: 1D (Imagery Intelligence Officer), 3F (AIDP–ISR Collection Manager), 3Y (Army Space Cadre), 5K (Instructor), 5U (Air Operations Officer), and Q7 (Information Collection Planner). MAJ Wright also earned the Defense Intelligence Agency's (DIA) Certified Collection Manager Professional-Fundamentals credential and the DoD's GEOINT Professional Certification-Fundamentals credential.

MAJ Graham Shelly serves as the 3rd Infantry Division Artillery S-2 and will serve his next assignment as the 3rd Infantry Division collection manager. MAJ Shelly holds a bachelor of arts degree in government and international politics from George Mason University and a master's degree in military arts and sciences from the Army Command and General Staff College. He is a graduate of AIDP–ISR and possesses multiple ASIs: 1D (Imagery Intelligence Officer), 3F (AIDP–ISR Collection Manager), 3Y (Army Space Cadre), 5U (Air Operations Officer), and Q7 (Information Collection Planner). He also earned DIA's Certified Collection Manager Professional-Fundamentals credential, the DoD's GEOINT Professional Certification-Fundamentals credential, and the Collection Requirements Manager Certification from the National Geospatial-Intelligence College.

The New Normal: Information Collection Planning in Large-Scale Combat Operations

by Major Christopher D. Thornton

Introduction

Information collection planning, like course of action development, is a visualization exercise. This is stating the obvious for anyone who has had to build a synchronization matrix. It is the collection manager's job to build a plan that employs units and sensors in time and space. The collection manager bases the plan on an expected sequence of actions and decisions by friendly and enemy forces, starting with an event template and refining the plan during the wargame.

One of the first visualization challenges that collection managers face, however, may involve expectation management, in particular, for those leaders who have cut their teeth in a theater with a high density of collection assets. At the theater level, friendly forces often have the benefit of a persistent stare for significant portions of the area of operations, and the threat may not have artillery or surface-to-air missiles to pose a deterrent.

Expect a Shift in Coverage Capabilities

The warfighter has been spoiled for years by the U.S. Central Command's area of responsibility, which has a robust mix of government- and contract-operated intelligence, surveillance, and reconnaissance (ISR) capabilities. This includes a fleet of dozens of manned and unmanned aircraft, ground sensors, and theater information collection assets operating from sanctuary to provide layered capabilities and multiple lines of 24-hour full-motion video coverage. This is understandable, given a mature theater where there is no credible challenge to the aerial and space domains, nor is there a peer to threaten networks and the electromagnetic spectrum.

Training audiences at warfighter exercises typically enjoy 24-hour coverage from fixed-wing aerial assets such as the Joint Surveillance Target Attack Radar System, Rivet Joint, and the Enhanced Medium Altitude Reconnaissance and Surveillance System. However, it is unlikely that Army force providers and Air Force providers will have the capability to deliver this amount of coverage to the warfighter during large-scale combat operations against a peer. National capabilities can help fill some of these gaps to a degree, but make no mistake, both space and cyberspace can and will be contested domains in a large-scale conflict.

Photo courtesy of NATO

Soldiers from the U.S. Army's 1st **Cavalry Division maneuver across a linear danger area during a live-fire exercise at Pabradė Training Grounds in Lithuania, February 12, 2020.**

Answering priority intelligence requirements in large-scale ground combat operations will be even more challenging, particularly in the early phases when the air, space, and cyberspace domains are at their most contested. Component commanders will be forced to prioritize because of the timelines to deploy capabilities to the theater of operations and a lack of a sufficient number of platforms to provide 24-hour coverage with theater-level wide area surveillance. The inevitable loss of sensors, both ground and aerial, will exacerbate the issue. As such, in large-scale ground combat operations, a brigade combat team or division is not likely to benefit from unmanned aircraft system (UAS), fixed-wing ISR, or fighter aircraft. Whenever these capabilities do show, they are more of an opportunity to be seized than an expectation.

Mississippi National Guard photo illustration by SSG Tim Morgan, 102nd Public Affairs Detachment

Army aviation systems, like these AH-64 Apache helicopters from the North Carolina Army National Guard's 1st Battalion, 130th Aviation Regiment, positioned in the Mojave Desert at the National Training Center, Fort Irwin, CA, will need to operate in an antiaccess and area denial contested airspace against adversaries that have advanced capabilities that constrain freedom of maneuver.

Information Collection during Transitions

The rapid movement and large distances that a ground force must cover (for the European problem set, at least) mean that information collection products, which were sometimes ignored in counterinsurgency, like the event template with its time-distance analysis and the synchronization matrix, are of critical importance. Formations must plan deliberately through transitions, such as jumping a main command post or collapsing a rear boundary.

These transitions involve significant impacts for information collection, with implications far beyond the information collection synchronization matrix. During headquarters transitions, perhaps the most important of these is the positioning of the Tactical Intelligence Ground Stations, which provide a headquarters with more than just full-motion video. How will the tactical command post get imagery and intelligence feeds while the main command jumps? Should a brigade combat team have a specified task to push information of particular import that they receive on the Tactical Intelligence Ground Station to the tactical command post via chat, or voice? Another example of an important transition is the displacement of combat aviation brigades, because of the impact to attack aviation and Gray Eagle collection. Should equipment move in multiple serials so that the unit maintains a degraded capability (probably)? If the combat aviation brigade will jump in phases, what equipment will be required to maintain that degraded capability? The answer depends upon the number of lines required through the jump and the need to operate these systems in a beyond line-of-sight configuration. The answer also depends upon the line of sight from the expected Universal Ground Data Terminal location, the location of the coordinated fire line and fire support coordination line, and the threat to convoys in the area. A division probably cannot afford to lose a low-density pacing item like a satellite ground data terminal.

For years, brigade combat teams at combat training centers have lived through the pains of planning through transitions like these. The ability to conduct transitions deliberately and understanding the trade-offs can be the difference between a successful and an unsuccessful rotation. Divisions and corps must also plan through such transitions, and rehearse the subtasks in their train-up as well, because they entail key capabilities and a command post is more than just a tent.

Keep `Em Flying

Due to threats from air defense, effective Shadow and Gray Eagle unmanned aerial vehicle (UAV) employment in large-scale combat operations requires deliberate planning and risk mitigation beyond the normal considerations of weather, maintenance, and airspace deconfliction if you want the asset to be around after the first few days. Routes to and from search areas should be varied to increase platform survivability as the enemy repositions air defense artillery systems in response to friendly information collection.

A best practice to consider is employing UAVs at maximum altitudes, even at the expense of full-motion video feed quality. Generally, air vehicles should be flown at as high an altitude as is practicable to decrease the probability of detection. Even the Shadow should be able to stay above man-portable air defense system's maximum altitude unless it flies directly over a team of SA-18 or SA-24 operators. The Gray Eagle is able to stay above the SA-15's maximum engagement altitude under most weather conditions (do not try it in Afghanistan in the winter). Even if you are operating the platform at the maximum altitude, you will still see the tank battalion. Promise.

Aside from survivability considerations, UAVs should fly offset from the named area of interest—farther is generally better, but even a few kilometers is better than nothing—whenever possible to make it less obvious where the asset is looking, to facilitate airspace management, and to increase the system's survivability. This is particularly true at the division and higher levels, where platforms such as Gray Eagle and Reaper typically have more than one sensor. While it won't help your warfighter exercise, it is invaluable to be able to cover two named areas of interest (one with a ground moving target indicator radar and one with the full-motion video common sensor payload) when you do not have a large number of combined force air component commander assets in support.

The incorporation of UAVs into attack aviation employment and in air assault operations in a screening capacity ahead of the aviation, whether through manned-unmanned teaming or otherwise, enables early identification of threats. If a surface-to-air system engages, the UAV successfully identifies the threat without the loss of an Apache and allows for rapid decision making as to whether to proceed. Key enablers such as UAS should be considered carefully in the "min force" criteria for an operation.

Finally, security of key links in the system chain, such as Gray Eagle data terminals and Ground Control Stations, is a must. These systems are low density, distinguishable, and vulnerable.

Task Organizing for Large-Scale Ground Combat Operations: The Division Cavalry Rides Again

After the shift to the modular brigade combat team model, divisions lost their battlefield surveillance brigades and division cavalry squadrons in favor of organic brigade-level cavalry to conduct reconnaissance and guard/screening tasks. The key limitation to this modularity in division and higher operations is that a maneuver commander must commit a maneuver formation to conduct reconnaissance and security tasks.[1]

Commanders have found the limits of even unrealistically persistent aerial and national sensors that facilitate gaining and maintaining contact with an enemy force in an exercise environment; therefore, through the manipulation of task organization and command and support relationships, they have resurrected the division cavalry or corps reconnaissance and surveillance "from hide." The foundation for this cavalry task force has varied. For a division, it has been a cavalry squadron detached from a brigade combat team with attack aviation in direct support, air defense artillery, and indirect fires.[2] Other enablers, such as engineers, cyber-electromagnetic activities, and unmanned aerial surveillance, are added when they are required by the terrain and mission.[3]

Over the course of its command post exercise series in preparation for warfighter exercise 20-04, Joint Warfighting Assessment 20, and Defender 2020, the 1st Cavalry Division experimented with a few variations on the composition and capabilities appropriate to a division cavalry squadron. A few key principles were consistent:

1) Division cavalry or the corps reconnaissance and surveillance are a "delivery system" for enablers such as fires. By pushing back against the enemy's disruption zone, a division cavalry can "pull" fires and sensors forward, but maneuver forces have to catch up, and quickly. These sensors can and should include air defense and counterfire radars because this will increase the survivability of the division cavalry and enable more effective lethal targeting, which is the whole point.

2) The division cavalry must retain freedom of maneuver by avoiding decisive engagement. This involves correlating forces and means, giving an appropriate mission to the formation, and having a reasonably accurate event template. A different formation or echelon (light or heavy, squadron, or brigade) may be required depending upon the frontage, distance, and task. Is the division cavalry an advanced guard? Screening? Both?

3) There is no "one-size fits all" division cavalry or corps reconnaissance and surveillance task organization; it is mission-dependent and will probably change by phase. What is the air defense threat in the enemy disruption zone? What is the desired form of contact—indirect fire, aircraft, visual, or something else?[4] The exact capabilities must be tailored to the terrain, the threat, and the mission for the formation to fight successfully for information and enable maneuver and fires in subsequent phases.

4) Deliberate primary, alternate, contingency, and emergency communications planning is a must to enable the formation to develop the situation rapidly and feed its

U.S. Army photo by SGT Dommnique Washington, 7th Mobile Public Affairs Detachment

The scout platoon of Headquarters and Headquarters Company, 1st Battalion, 5th Cavalry Regiment, 2nd Armored Brigade Combat Team, 1st Cavalry Division, conduct a scout validation exercise January 21-22, 2020, at the Novo Selo Training Area in Bulgaria. They are evaluated on their ability to navigate terrain while accurately gathering, assessing, and reporting information, along with providing security and engaging targets when necessary.

information to the supported headquarters. While the simulation environment cannot replicate this realistically, a division cavalry or corps reconnaissance and surveillance will not be successful without its ability to communicate.

A couple of key considerations 1st Cavalry Division had for warfighter exercise 20-04 were how much unmanned aerial surveillance to provide (two or four RQ-4B Shadow UAS), and whether to support zone and area reconnaissance with Gray Eagle UAS as the division pushed into the enemy's disruption zone. A key addition after command post exercise 3 was the program of record-B Prophet or the Saber Fury electronic warfare/signals intelligence (SIGINT) systems.

Based on the expected dispersal of enemy air defense artillery to protect the integrated fires command assets, the G-2 staff recommended maintaining the ability to identify and destroy enemy radars by ground-based SIGINT collection. This enabled a limited capability to engage these systems immediately, even in the event aerial SIGINT/electronic intelligence became unavailable because of theater- and national-level air defense or enemy fixed-wing air threats to joint ISR.

A tailored reconnaissance and surveillance formation of some kind is particularly important in offensive operations at the division and above. Proper task organization and utilization of this formation will probably feature in large-scale ground combat operations at brigade and above echelons. However, do not assume that each echelon requires a reconnaissance and surveillance formation. Frontage, terrain, synchronization of operations at echelon, and the nature of the mission will dictate where (and how) a formation will fight for information.

Conclusion

Ultimately, the return of the division cavalry squadron is an example of what has not changed with the "new normal" of large-scale ground combat operations, and this includes the fundamentals. The fundamentals of reconnaissance and of security—as well as the importance of information collection synchronization, fires and effects, and maneuver—remain as applicable as they were to 1st Squadron, 4th Cavalry Regiment, when it served as the division cavalry for 1st Infantry Division during the Gulf War.[5] To seniors in the Army, the return to the "new normal" is less like an adaptation to something radically different and more like putting on an old pair of boots—it is a return to the "old normal."

Endnotes

1. Nathan A Jennings, *Reconsidering Division Cavalry Squadrons* (Fort Leavenworth, KS: School for Advanced Military Studies, U.S. Army Command and General Staff, 2017), 1-2.

2. Ibid., 35-36. This is what the author describes as a "low augmentation" task force.

3. Ibid., 37-39. The author provides additional options and recommended frontages, ending with an augmented armor brigade combat team screening a frontage of 120 to 150 kilometers.

4. Department of the Army, Army Doctrine Publication 3-90, *Offense and Defense* (Washington, DC: U.S. Government Publishing Office, 31 July 2019). However, it is probably not visual contact that is desired. This will tell out in the task organization, with a Q-53 counterfire radar-equipped artillery battalion in direct support, an unmanned aerial vehicle platoon attached, or similar.

5. Jennings, *Reconsidering Division Cavalry Squadrons*, 24.

MAJ Chris Thornton is the collection manager for the 1st Cavalry Division. Prior to his current position, he served as the task force executive officer for Task Force Observe, Detect, Identify, and Neutralize, providing aerial intelligence, surveillance, and reconnaissance in support of Operations Resolute Support and Freedom's Sentinel. He has served as a Joint Surveillance Target Attack Radar System exercise planner and instructor in the continental United States and as an operator over three deployments to the U.S. Central Command area of responsibility supporting Operations Enduring Freedom, Inherent Resolve, and Freedom's Sentinel.

U.S. Army photo by SPC Michael Schwenk

Army Soldiers with the New Jersey National Guard sit inside a ground control station for an RQ-7B Shadow unmanned aircraft system at Joint Base McGuire-Dix-Lakehurst, NJ, February 10, 2020.

Information Collection Synchronization

by Chief Warrant Officer 3 John E. Burris

Introduction

Information collection management during large-scale ground combat operations is a new concept for modern collection managers, and the synchronization of the information collection plan is proving difficult. Trends and observations regarding information collection include reach limitations; communication disruptions; processing, exploitation, and dissemination (PED) issues; and limited availability of assets. Additional challenges are associated with the lack of experience in large-scale ground combat operations and knowledge of traditional and nontraditional collection capabilities, along with the rapid advances in technology. Through integrated information collection efforts, commanders and staffs can continuously plan, task, and employ appropriate collection assets and forces to gather timely and accurate information to facilitate satisfying commander's critical information requirements (CCIRs) and other information requirements.[1] Information is the driving factor behind the operations process, including the military decision-making process, staff estimates, and commander's decision points. As such, collection managers must ensure their efforts are synchronized and nested to accomplish the needs of their customers (commander, staff, and subordinate units).

FY 2019 Key Observations and Trends

Annually, the Center for Army Lessons Learned (CALL) assists the combat training centers and mission command training program with publishing key observations and trends. These documents are located on the CALL website,[2] accessible to common access card-enabled users through CALL's Request for Publication portal. In fiscal year (FY) 2019, several recurring trends emerged from various rotations at the combat training centers and mission command training program. These trends indicate that—

- Divisions, corps, and Special Operations Forces (SOF) units do not effectively synchronize information collection with operations and targeting.[3]
- CCIRs and priority intelligence requirements (PIRs) were not synchronized with the intelligence collection plan.[4]
- Collection management requires multi-echelon synchronization and incorporation of all possible collection assets to maximize support to targeting and decision making.[5]
- Rehearsals do not synchronize operations or enhance developing a shared understanding and generally revert to wargaming.[6]

Pathways to Success

These trends are not the only intelligence warfighting function observations described in the FY 2019 documents; however, they have a single commonality—the synchronization of all parties involved in the information collection management process. FM 2-0, *Intelligence,* states:

> ***Rehearsals assist units in preparing for operations by either verifying that provisions and procedures are in place and functioning, or by identifying inadequacies that leaders and the staff must remedy. They allow operation participants to become familiar with and translate the plan into specific actions that orient them to their environment and other units when executing the mission. Rehearsals allow the [military intelligence] MI element to integrate with and become familiar to the supported unit. It also allows the MI element to understand its role and scheme of maneuver within the larger mission objectives.***[7]

FM 2-0 further states, "MI leaders conduct information collection rehearsals to ensure the right information is collected…information collection rehearsals may be combined with the combined-arms rehearsal or fires rehearsal."[8] When executed properly, rehearsals will orient all parties to their exact roles and responsibilities in upcoming collection operations. As the operational tempo in large-scale ground combat operations generally does not allow for full dress rehearsals, the best rehearsal option is a digital rehearsal. These rehearsals should be built into an information collection working group. The information collection working group table (pictured below), which is from ATP 6-0.5, *Command Post Organization and Operations,* identifies the participants and agenda of the working group.

General Information	*Participants*
Title: information collection working group **Purpose**: coordinate for, integrate, and synchronize information collection in support of the concept of operations **Frequency**: daily **Duration**: one hour **Location**: G-2 work area **Medium**: face-to-face, defense collaboration service	**Staff proponent**: G-2 **Chair**: chief of staff **Members**: G-3 (current operations), G-3 (future operations), G-9, fires, air liaison, information operations, space, cyberspace electromagnetic activities, staff judge advocate representative, liaison officers
Inputs and Outputs	*Agenda*
Inputs: • Commander's guidance • Commander's critical information requirements • Future operations requirements • Subordinate unit requirements • Targeting requirements • Air tasking order nomination **Outputs**: • Priorities and recommendations for latest updated information collection plan • Recommended changes to commander's critical information requirements • Fragmentary order input	• Roll call (G-2) • Past information collection plan review (G-2) • Weather update (staff weather officer) • Intelligence update (G-2) • Operations update (G-3) • Future operations requirements (G-3) • Subordinate unit requirements (G-3) • Targeting requirements (targeting officer) • Allocation of collection resources and assets availability (collection manager) • Summary (G-2) • Guidance (chief of staff)
G-2 assistant chief of staff, intelligence G-3 assistant chief of staff, operations	G-9 assistant chief of staff, civil affairs

Information Collection Working Group Table[9]

The information collection working group is built into the operations process as part of the critical path leading to the commander's decision points and is programmed into the headquarters' battle rhythm. During every warfighter exercise in FY 2019, an information collection working group was included on the battle rhythm. However, the timing and variations in execution of the working group were evident in each unit. The working group was also not optimized to synchronize the staff and participants in the collection planning. The agenda (shown in the lower right quadrant of the table) sets the conditions to accomplish the coordination, integration, and synchronization of information collection in support of the concept of operations. The agenda steps are as follows:

Roll call: The roll call, which the collection manager typically conducts, should include the participants listed in the upper right quadrant of the table. The information collection working group should be expanded to include—

- **Collection asset(s) team members.** Examples would be a Gray Eagle (unmanned aircraft system) pilot, reconnaissance platoon leader/noncommissioned officer in charge (NCOIC), or SOF liaison officer. This enables a shared understanding of what the asset needs to collect and from where.
- **PED asset team member.** The asset tasked to exploit in near real time any ongoing collections. The PED member will back brief what they are looking for and where they need to report time-sensitive information.
- **Supported unit representative.** This will help to ensure the supported unit is being supported in the desired manner.
- **Electronic warfare representative.** This ensures the deconfliction of collection assets and electronic attacks. The electronic fratricide vignette, on the next page, provides an example.
- **Air liaison officer or joint tactical air controller.** This individual will identify any potential ad hoc collection opportunities as aircraft transition above a unit's battlespace.
- **Army aviation unit representatives.** Army aviation elements operating within the battlespace are capable of conducting traditional and nontraditional collection during multiple types of operations.
- **Field artillery intelligence officer.**
- **Targeting officer.** This enables a walkthrough of both deliberate and dynamic targets for

the next 24 hours. This includes understanding what assets are tasked to conduct first- and second-level battle damage assessments. JP 3-60, *Joint Targeting*, provides information about the levels of battle damage assessment, and CJCSI 3370.01, *Target Development Standards*, describes the phases of battle damage assessments.

- **Analysis and control element (ACE) chief or NCOIC.** This allows them to garner an understanding of what reporting should be forthcoming in an effort to update battle damage assessments and running estimates. This individual could also lead the G-2 update portion of the information collection working group.

Electronic Fratricide

Following document exploitation from material found on an enemy scout, which revealed the frequencies of enemy reconnaissance command net and reporting timeframes, the G-2 signals intelligence section requests collection and exploitation of identified frequencies. The mission was tasked to both ground and aerial assets to build in redundancy. Collection from both tasked assets yielded zero results after attempted collection during two enemy reporting timeframes. It was later identified that nonlethal effects in the form of electronic attack were jamming the same identified frequencies to prevent enemy call for fire missions.

Past information collection plan review: Units should back brief the collection manager on whether the collection met the required intent, if additional collections are needed, and if anything hindered the collection.

Weather update: The weather officer should identify any potential weather effects on planned collection missions. This includes ground and air missions.

Intelligence update: The ACE chief or NCOIC should outline enemy potential courses of action 24 to 96 hours out (dependent upon echelon) in order to enable named area of interest (NAI) refinement. If there have been adjustments to NAIs, collection schemes must match the new NAIs in order to maximize the collection.

Operations update: The designated operations officer will discuss the friendly forces scheme of maneuver for the next 24 to 96 hours outlining key targets and objectives. The operations officer also ensures that collection assets are properly tasked in the operation order or fragmentary order. Finally, the operations officer should ensure that collection assets and PED entities are working to answer CCIRs and PIRs and support the commander's decision points.

Targeting requirements: During this portion of the information collection working group or, as an alternative, during the targeting working group, the field artillery intelligence officer, collection manager, and PED should cover deliberate and dynamic targets programmed in an "if-this-then-that" format.

Collection Example

The field artillery intelligence officer calls out target 001 and describes the target. The collection manager identifies the asset(s) to collect against the target and the timeframe in which the asset is collecting and in which NAI(s). The PED analyst(s) identifies the information requirement(s) and indicator(s) followed by how the analyst will relay critical target information. The field artillery intelligence officer then indicates what assets execute the mission's desired effects. Then the collection manager identifies assets designated to conduct phases 1 and 2 battle damage assessment. The PED analyst should then call out how they will assess effects and how they will report to the ACE and field artillery intelligence officer the assessed battle damage assessment. Re-attack guidance is called out, circling this process back to the initial target call out. This is finalized with the ACE representative, indicating the updated battle damage assessment's tracking and running estimate.

Allocation of collection resources and assets availability: The collection manager ensures a shared understanding of the intelligence collection plan 24 to 96 hours out and allows the SOF and air liaison officers to provide additional input to collection opportunities. An example of this is in the tipping and cueing vignette.

Tipping and Cueing

While attempting command and control of a division wet-gap crossing, Task Force-Gap (TF–G) was heavily engaged by enemy long-range fires. Efforts to suppress the continuous attacks were less than fruitful by the friendly counterfire batteries due to rapid displacement by the enemy. The G-2 initiated ground moving target indicator (GMTI) collection based upon radar-acquired points of origin and providing the end location of the GMTI track for immediate targeting. After requesting immediate engagement, the division legal advisor informed the targeting team that engagement based upon GMTI alone was counter to the rules of engagement. With the available information, the G-2 requests SOF reconnaissance assistance to provide eyes on target. After the next iteration of enemy fire, the G-2 followed the GMTI from the point of origin and provided the end of the track to the SOF team, which then moved into position, verified the enemy artillery location, and initiated a call for fire. After several hours, this tactic reduced enemy fires on TF–G by 80 percent, allowing friendly forces to complete the wet-gap crossing.

Summary: The collection manager should summarize collection efforts, communication plans, and re-tasking criteria of collection assets during this portion of the information collection working group.

Guidance (from the chief of staff/executive officer or designated representative): Like other working groups, the information collection working group is designed to synchronize staff efforts. In any working group, guidance can change or one staff section's priorities may not align with another staff section's priorities. It is imperative that the chief of staff/executive officer or designated representative have a complete understanding of the commander's intent and priorities. These key personnel must be present at the information collection working group and other working groups. Their attendance ensures the staff is working as a cohesive team toward the commander's most recent and relevant guidance. During this portion, the chief of staff/executive officer will confirm that the information collection working group's inputs and outputs are on track and, if not, will make the necessary adjustments.

Completing a full rehearsal during the information collection working group allows synchronization of the staff and alleviates the need to conduct another battle rhythm event in an already saturated timeline during large-scale ground combat operations. This recommended approach is not an attempt to dictate how S-2s and/or G-2s should conduct an information collection rehearsal; rather, it is an attempt to reinforce the need for rehearsals and the level of detail the rehearsal requires in order to mitigate recurring observations and trends at the combat training centers and mission command training program.

U.S. Army photo by SPC Joseph E.D. Knoch

First Corps staff directorates compare notes before a targeting briefing during Warfighter Exercise 20-3 on Joint Base Lewis-McChord, WA, February 11, 2020.

Understanding and Tasking of All Available Assets

An additional identified trend focuses on the collection manager's and information collection operations' lack of understanding of all available assets for the collection and tasking of those assets to provide information to customers. An example of this is the counterfire radar's acquisitions or resupply missions by Army aviation and sustainment units. All friendly forces operating within an area are capable of providing potentially valuable information and enhancing situational awareness. (FM 3-0, *Operations,* provides additional information on situational awareness.) Continuing to review the FY 2019 mission command training program key observations, we find additional inefficiencies that led to less than optimized collection plans that were not synchronized:

- Collection managers from brigade to Army Service component commands have universally been hesitant to leverage collection requirements on subordinate units.[10]
- The collection plan is generally not approved by the G-3 nor promulgated through operation orders or fragmentary orders.[11]

During FY 2019 warfighting exercises, the collection manager developed daily information collection matrixes to share at various battle rhythm events; however, few were included in fragmentary orders and even fewer assets were tasked to conduct collection. When the higher headquarters' information collection matrixes include all subordinate assets and units, a clearer picture is developed, enabling the collection manager to gain efficiencies in the collection plan and optimize redundancies and tipping/cueing efforts in the plan. The synchronization of the information collection plan as described could alleviate the collection manager's need to recommend a direct tasking on subordinate units, even though the collection manager has no tasking authority. FM 3-55, *Information Collection,* indicates "the G-3 (S-3) is the

primary information collection tasking and directing staff officer in the unit, tasking the organic and assigned assets for execution. The G-3 (S-3) collaboratively develops the information collection plan and ensures it synchronizes with the operation plan."[12]

Conclusion

As identified through FY 2019 observations from the combat training centers and mission command training program, the collection manager's synchronization of the information collection plan is critical to the success of the entire staff and operations process. Using the information collection working group as a rehearsal and synchronization mechanism, and effectively tasking collection assets in all order types, will allow the intelligence community to begin reversing these trends.

Endnotes

1. Department of the Army, Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 3-5.

2. The Center for Army Lessons Learned website is at https://call.army.mil/.

3. Department of the Army, *Mission Command Training in Large-Scale Combat Operations: Mission Command Training Program Fiscal Year 2019 Key Observations* (Fort Leavenworth, KS: Center for Army Lessons Learned, n.d.), 5.

4. Ibid., 9.

5. Ibid., 22.

6. Ibid., 54.

7. Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Washington, DC: U.S. GPO, 6 July 2018), 3-14 (common access card login required).

8. Ibid.

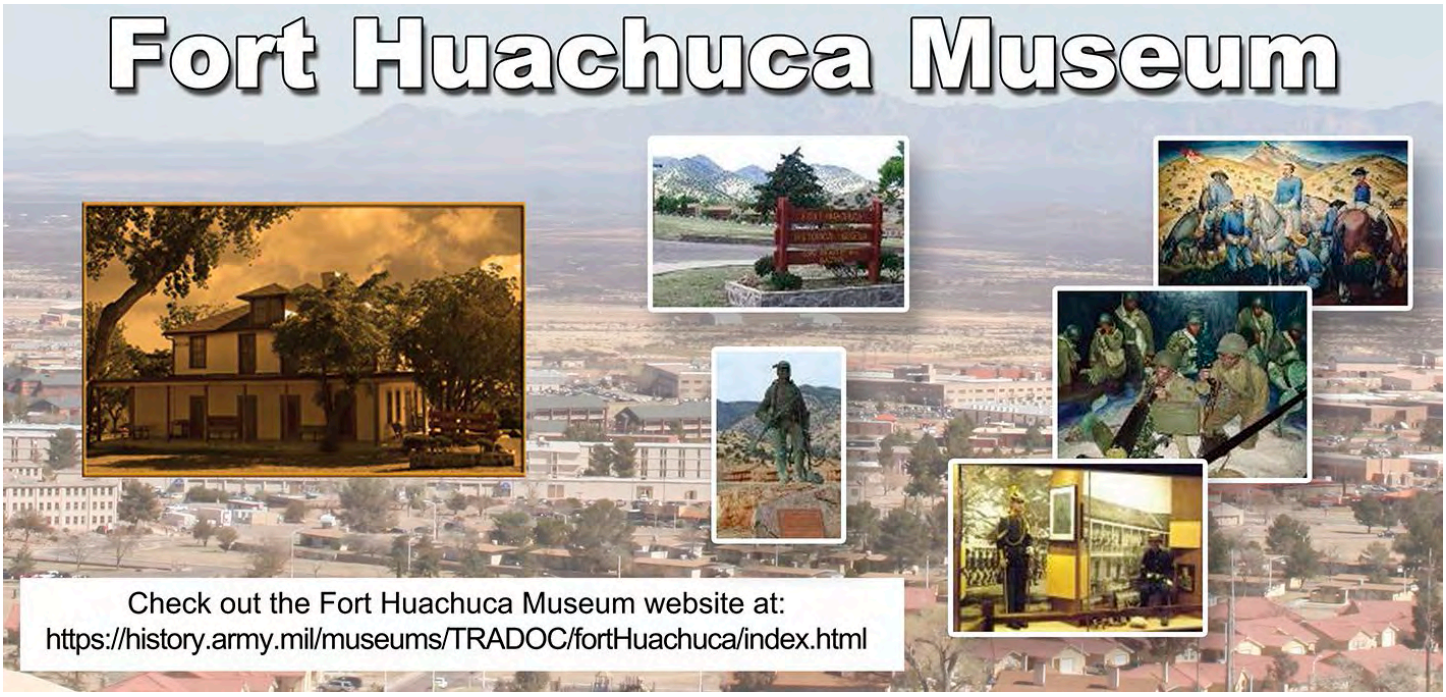
9. Department of the Army, Army Techniques Publication 6-0.5, *Command Post Organization and Operations* (Washington, DC: U.S. GPO, 1 March 2017), A-20.

10. Department of the Army, *Mission Command Training,* 22.

11. Ibid., 5.

12. Department of the Army, FM 3-55, *Information Collection* (Washington, DC: U.S. GPO, May 2013), 2-4.

CW3 John Burris is a military occupational specialty 350F (All-Source Intelligence Technician) who serves as a military analyst at the Center for Army Lessons Learned. Other notable assignments in which he worked information collection include the National Ground Intelligence Center, 8th Army G-2, and a deployment with 3rd Stryker Brigade Combat Team, 2nd Infantry Division, in Operation Enduring Freedom. He is pursuing a master of science degree in data analytics and holds a bachelor of arts degree in American history.



Army Reserve photo by MSG Michel Sauret

Soldiers conduct reconnaissance the night before a morning mission at Fort Hunter Liggett, CA, July 22, 2017, as part of a combat support training exercise.

Resolving Challenges for Brigade Combat Team Collection Management

by Major Richard L. Sharp, Chief Warrant Officer 4 Ray C. Joyce II, and Chief Warrant Officer 3 Roy S. Swearengin

Information is a source of learning. But unless it is organized, processed, and available to the right people in a format for decision making, it is a burden, not a benefit.

—William Pollard

Introduction

Brigade combat team (BCT) collection management elements face many challenges during Joint Readiness Training Center (JRTC) rotations, the majority of which can be overcome through the study and application of the best practices and lessons learned of other rotational units. Over the past several years of JRTC rotations, the brigade command and control intelligence observer coach/trainer (OC/T) teams identified that collection management elements have encountered three primary obstacles:

- Uncodified collection management officer-in-charge position.
- Lack of collection management team-focused training.
- Unplanned and ill-defined information collection products.

While the BCT collection manager has not been a captain position since the modified table of organization and equipment (MTOE) change in fiscal year 2014, the majority of BCTs have realized the significant advantage of placing experienced leaders in this critical function area.

Nine of the last ten rotational training units have filled the BCT collection manager position with a captain of varying experience; however, the officer generally serves in this position for only a year or less because it is not a key developmental position. U.S. Army Forces Command has taken this particular lesson learned and is working in conjunction with the U.S. Army Training and Doctrine Command and

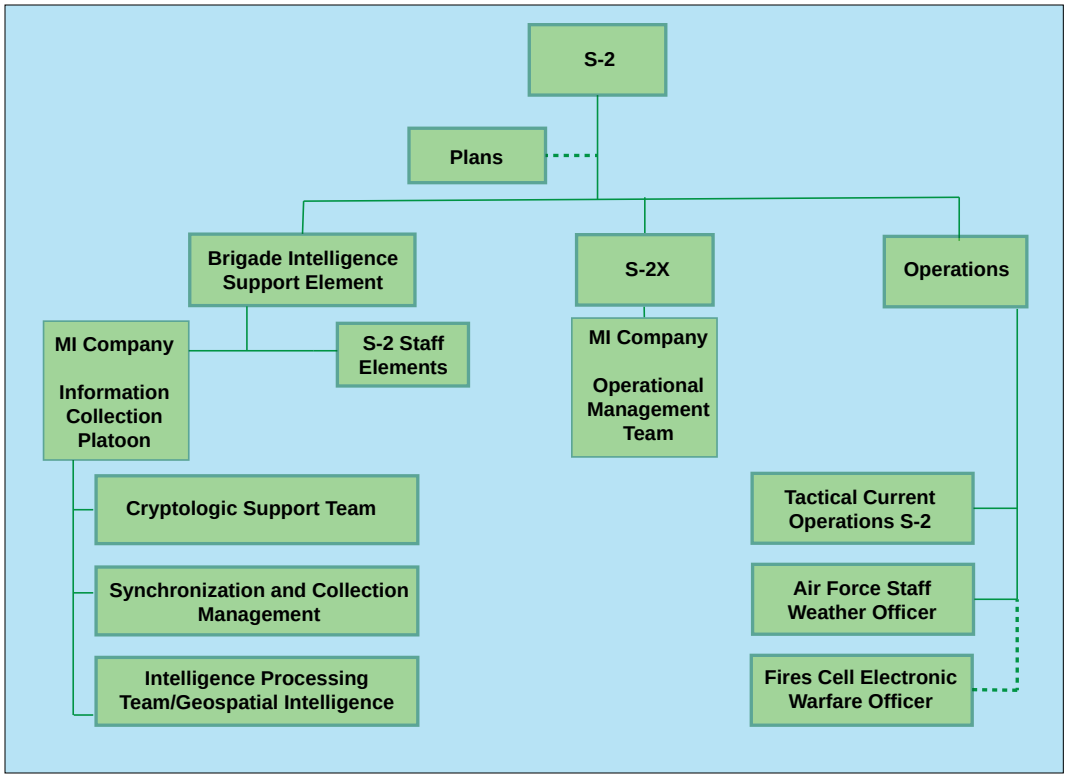


Figure 1. Brigade Combat Team Intelligence Cell Structure[1]

Headquarters, Department of the Army to adjust the future BCT MTOE to allocate and align collection management positions within the collection management element. Figure 1 (above) illustrates the current BCT S-2 intelligence cell structure formed from both BCT intelligence staff and military intelligence company Soldiers.

Despite the growing realization that emphasis is needed for collection management, collection management teams continue to struggle at home station with having sufficient information collection training, synchronizing collection management tasks across all warfighting functions during the military decision-making process (MDMP), and validating information collection products that are both detailed and functional. Although these challenges can be tackled individually, BCT S-2s and collection managers can study the lessons learned from rotational units at JRTC over the past year on how to incorporate the BCT collection manager and the collection management element into both the MDMP and the rapid decision-making and synchronization process.

Gathering the Tools

Success at JRTC for collection management elements starts well before the rotation begins and involves the collection management section's training and integration with the brigade intelligence support element (BISE) and the BCT staff. The most successful BCT S-2s at JRTC prioritize the collection management element and the collective training of the collection management element with the all-source synchronization and collection (ASSC) element of the BISE during intelligence preparation of the battlefield and step 2 of MDMP. TC 2-19.401, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 1,* describes culminating collection management element certification and provides tables to validate the BCT S-2 and intelligence warfighting function teams; however, only small sections of the TC 2-19.400 series, which addresses tiers 1 through 4 of the Military Intelligence Training Strategy (MITS), are dedicated to explaining how BCT collection management elements can train individually and as teams. Multiple training resources exist for collection management elements besides what is within MITS, but not all are easily accessible. The majority of BCT collection management elements rely on the U.S. Army Intelligence and Security Command Foundry Program to obtain training; however, other resources can provide successful training, product validation, and integration with the rest of the BISE.

Successful units identify the collection management team well ahead of their JRTC rotation and develop a multi-echeloned training plan. One of the best resources to achieve this approach is the division collection management element. The division collection management element has not only a key developmental major assigned but also a senior all-source technician, a geospatial technician, senior noncommissioned officers, and multiple Soldiers. The division collection management element takes advantage of other available resources to develop training plans, and the BCT collection management element can coordinate their training plan development to link into the available training. Some of these training opportunities include the Foundry Intelligence, Surveillance, and Reconnaissance (ISR) 301–303 classes, the Information Collection Planner Course offered at the U.S. Army Intelligence Center of Excellence, and other online classes offered through the Defense Intelligence Agency's AGILE portal available on the SECRET Internet Protocol Router Network and Joint Worldwide Intelligence Communications System. Finally, collection management elements can coordinate with local Air Force ISR liaison

officers to conduct training on echelon above brigade assets, not just for their section but also for the entire BCT staff.

Successful collection management teams develop and gain approval of their "fighting products" from their BCT commander early in the training cycle. These products can be an information collection synchronization matrix (ICSM), an information collection matrix combination, or best practices of a combined ICSM with added fires assets (Figure 2) describing the correlation of sensor-to-shooter linkage in a quick glance product. Gaining approval from the BCT commander will alleviate information collection plan miscommunication and give time back to planners and supported units executing "the plan." While the ICSM example provided includes both information collection and fires assets to show the linkage between sensor and shooter, the ICSM uniquely identifies windows of specific enemy activity (improvised explosive device cells and indirect fire cells) based on historical pattern analysis. This addition to the ICSM enabled the rotational training unit's current operations cell to look for dynamic targeting windows of when enemy elements were the most active instead of remaining focused solely on deliberate targeting. More importantly, the BCT commander requested the ICSM each morning before attending any other meeting.

The final best practice observed during step 2 of MDMP has been the integration of the collection management element and the ASSC element of the BISE. The ASSC element

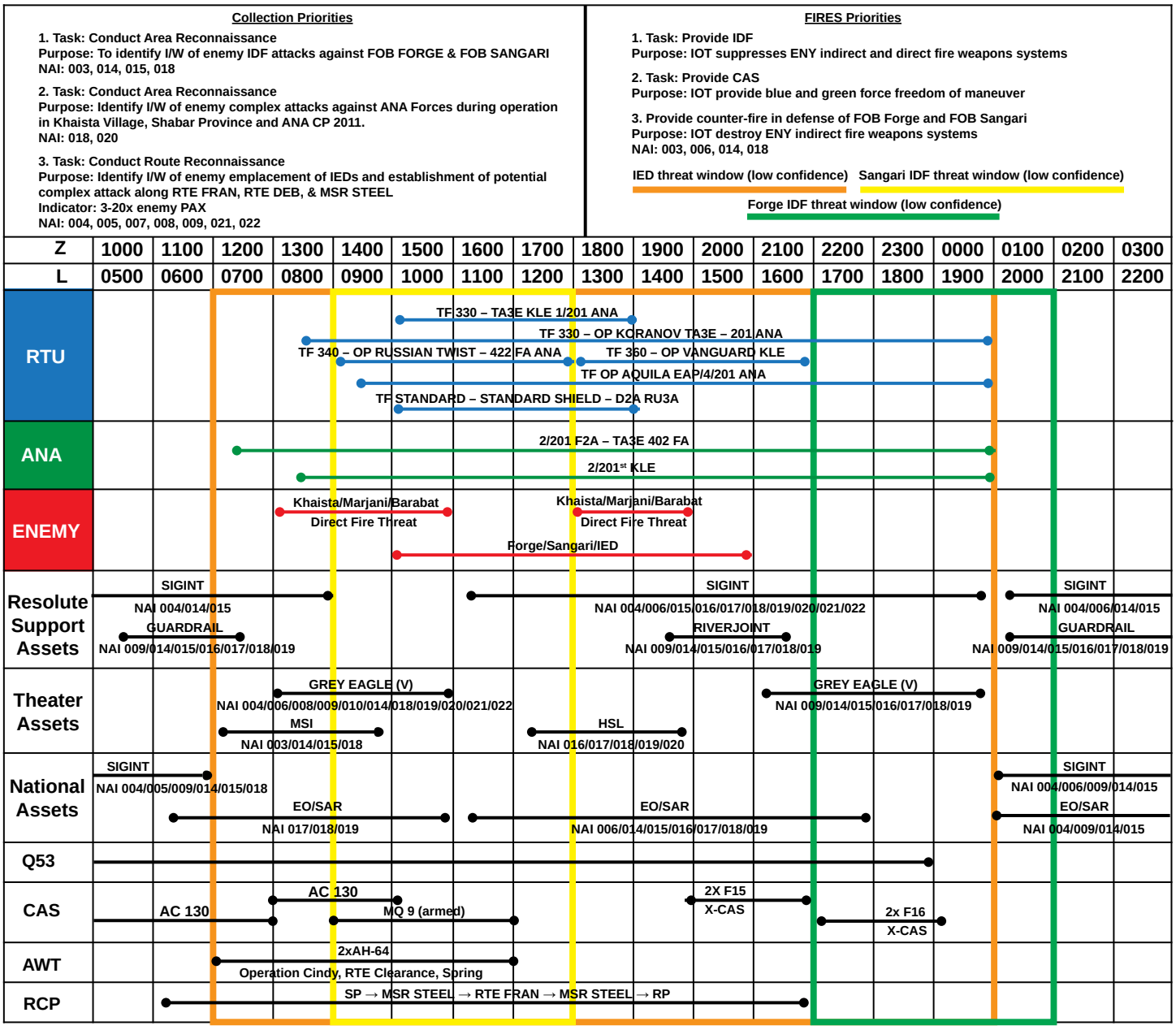


Figure 2. ICSM Synchronizing Intelligence and Fires

is responsible for developing the enemy event template and event matrix. The most successful units have the ASSC element identify and provide the gap analysis and information requirements to the collection management element. The collection management element then develops the scheme of information collection. The units that struggle have relied solely on the collection management element to develop the priority intelligence requirements and generate all information requirements. Additionally, they expect the collection management element to define the essential elements of information to build the information collection matrix and ICSM as the intelligence warfighting function generates the necessary outputs to support step 3 of MDMP. The BCT collection management element has neither the manpower nor the situational understanding of the enemy required to identify and produce all intelligence gaps, requirements, and information needs for the BCT. In doing so, the collection management element is overwhelmed, which is almost always seen as the collection management element being behind instead of in front of the BCT's mission execution. After action reviews with collection management teams and OC/Ts revealed that collection management elements struggled with the roles and responsibilities of intelligence and operations requirements both within the BISE and with the rest of the staff. This resulted in fewer preplanned information collection missions requiring more ad hoc/8-line requests for collection to the division collection management element.

We've Gathered the Tools. It's Time to Gather the Experts

Step 2 of MDMP for the intelligence warfighting function focuses primarily on the enemy and the development of running estimates. Step 3 focuses on developing the course of action (COA) for the rotational units' options, refining the scheme of information collection into a working ICSM, and building the information collection matrix to support COA development and wargaming. COA development focuses on generating options for the BCT commander. OC/Ts historically observe units struggle through this process because they bring only the BCT S-2, assistant S-2, and collection manager to COA development rather than the single-source technical experts who would best be suited to attend.

It is a continuing best practice at JRTC for the military intelligence (MI) company commander, warrant officers, and senior noncommissioned officers of the various intelligence and aviation disciplines for the organic BCT assets to attend and provide necessary inputs during COA development. From the human intelligence operational management team to the unmanned aircraft system aviation warrant officers, these experts bring a multitude of collection options and expertise to the process. They are also present to understand the guidance from the BCT commander and operations officer and can provide input to collection asset placement and task organization considerations. These experts can relay the requirements and intent to their collectors. Separately the MI company commander can add the tasks within the MI company base order if the verbiage is not present in the BCT base order.

While the BCT S-2, collection management element, and technical experts are conducting COA development, ASSC elements conduct continuous intelligence preparation of the battlefield refinement. One of the best practices of the past year is the development of an enemy synchronization matrix that provides more detail to enemy actions throughout the planning timeline. Instead of relying solely on an event template and event matrix developed during step 2 of MDMP, the ASSC element developed the enemy synchronization matrix. The ASSC element did this by using this common format as the rotational units' synchronization matrix over separate 24-hour periods for both easy comparison and support to collection efforts and options during COA analysis/wargaming (Figure 3, on the next page). The enemy synchronization matrix turned into a necessary fighting product that not only supported detailed wargaming but also served as a fighting product that the BCT commander requested daily.

Collection Management Element Actions during Wargaming and Beyond

Tools from the previous steps of MDMP include the event template, event matrix, enemy synchronization matrix, priority intelligence requirements with essential elements of information and information requirements, information collection matrix, and ICSM. With these tools, the intelligence warfighting function and collection management section are prepared to tackle one of the most important, but often not well executed, steps of MDMP—the wargame. Too often at JRTC, OC/Ts observe units that fail to analyze the relative combat power analysis and turn-based effects on enemy and friendly units. For both the collection management element and the fires warfighting function to accurately account for battle damage assessment collection, the BCT staff needs to determine the adjudication criteria for turn-based wargaming. Successful units used the correlation of forces matrix (COFM) or calculator to determine the effects on both friendly and enemy forces, to adjust and refine friendly COAs, and to emphasize collection during the counteraction turn. The COFM tool provides an unbiased look at the effects of various engagement types from a

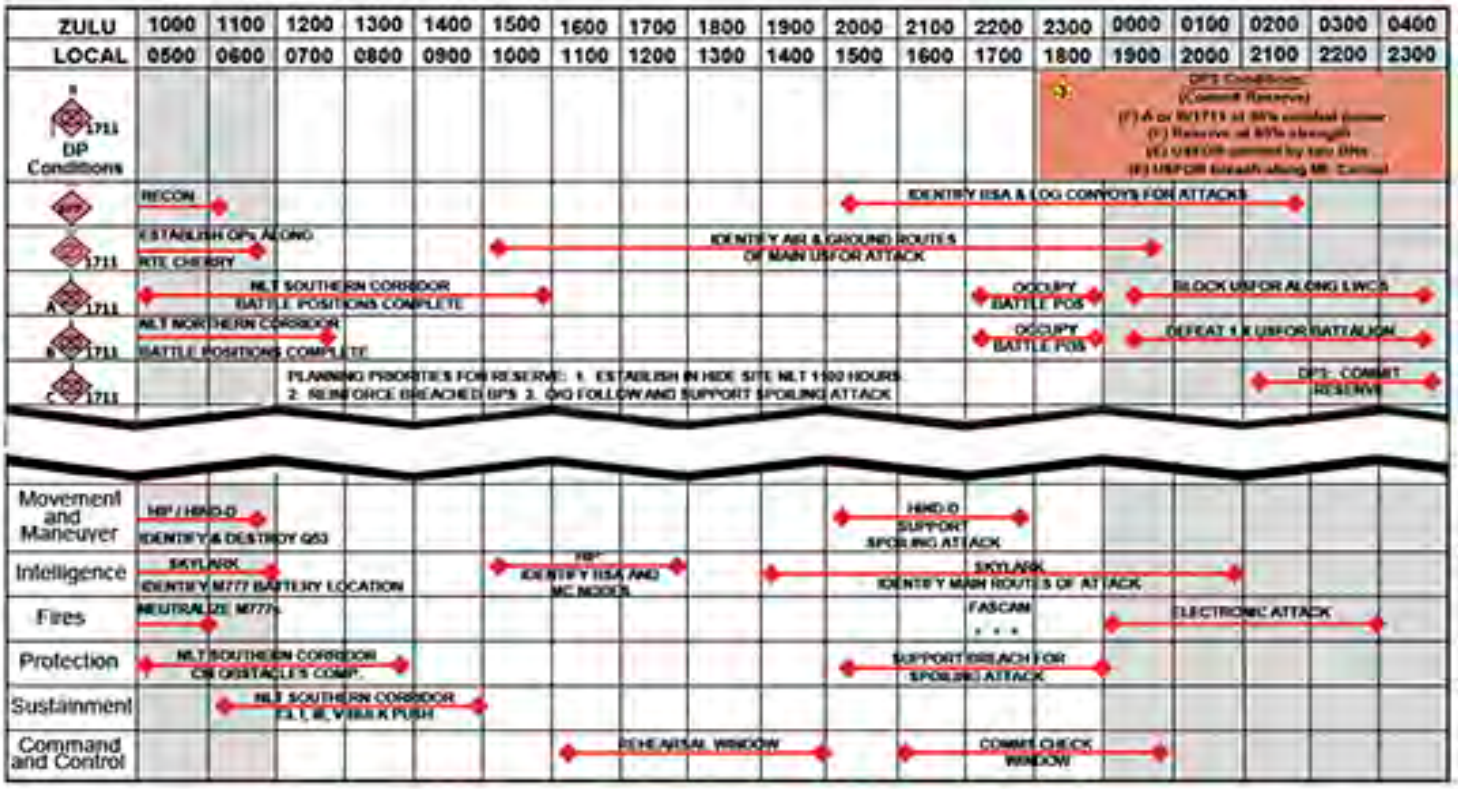


Figure 3. Enemy Synchronization Matrix

friendly and enemy perspective. The use of COFMs by divisions during warfighter exercises is a best practice adopted by multiple units. Dale Spurlin and Matthew Green describe COFM in detail in their 2017 *Infantry Magazine* article.[2]

During wargaming, the collection manager, MI company commander, and collection asset leads also refine the verbiage for the BCT's operations order and MI company operations order to provide exact tasks to subordinate units and collectors by phase, to enable sensor-to-shooter linkage from both a physical and logical topology. This discussion of topology and architecture during the wargame enables the staff as a whole to understand what physical assets and communication systems are required to provide both structured and unstructured messages to flow using the SPOT method (sensor, processor, output, and transport mechanism). Understanding the SPOT method and applying it during wargaming enables the collection management element and the rest of the staff to understand the flow of intelligence information and indicators. This feeds not only the common operational picture but also the other mission command systems.

Once the BCT commander approves the COA, successful collection management elements, intelligence warfighting function leads, and other staff sections build the necessary scripts, address books, and protocols in their digital systems to support deliberate targeting of the enemy rather than rely solely on analog means. All 10 of the past year's rotational units conducted a version of an information collection/fires rehearsal and fires technical rehearsal (such as the best practice GTA 30-04-001, *Information Collection Rehearsal (IC RX)).*[3] However, only 1 of 10 units conducted a deliberate information collection and fires technical rehearsal validating the point-to-point transfer of U.S. message text format messaging or a combination of peer-to-peer transfer and dissemination through the defense dissemination service to other mission command systems. If more rotational units deliberately plan, prepare, and validate the sharing of data within the objectives of the Army Data Strategy in AR 25-1, *Army Information Technology* (visible, accessible, understandable, trustable, and interoperable), OC/Ts anticipate greater success not only for collection management sections and the intelligence warfighting function during JRTC rotations but also for future large-scale ground combat operations.[4]

Final Tips for Future Rotational Collection Management Elements

Every rotational training unit struggles in some areas of the intelligence core competencies (synchronization; intelligence operations; processing, exploitation, and dissemination; and analysis). Fortunately, each rotational unit has at least one or more best practices or lessons learned to assist the MI Corps and BCTs at both JRTC and in future operations. Collection managers and collection management elements are making progress based on numerous best practices that

OC/Ts have observed. Those units that conduct collective training as a collection management element in accordance with MITS and other "outside the box" training strategies refine and validate their standard operating procedures over multiple exercises. They integrate the collection management element and technical single-source collectors into their MDMP process and conduct multiple iterations as a BCT staff. These units will continue to have the greater levels of success at the combat training centers.

Epigraph

"William Pollard Quotes," BrainyQuote.com, accessed 29 May 2020, https://www.brainyquote.com/quotes/william_pollard_125776.

Endnotes

1. Figure 1 is adapted from figures in Department of the Army, Training Circular 2-19.401, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 1* (Washington, DC: U.S. Government Publishing Office [GPO], 14 May 2019) (common access card [CAC] login required) and Department of the Army, Army Techniques Publication 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. GPO, 10 February 2015) (CAC login required).

2. Dale Spurlin and Matthew Green, "Demystifying the Correlation of Forces Calculator," *Infantry Magazine* 106, no. 1 (January–March 2017): 14–17, https://www.benning.army.mil/infantry/magazine/issues/2017/JAN-MAR/index.html.

3. Department of the Army, Graphic Training Aid 30-04-001, *Information Collection Rehearsal (IC RX)* (Washington, DC, 10 April 2019).

4. Department of the Army, Army Regulation 25-1, *Army Information Technology* (Washington, DC: U.S. GPO, 15 July 2019), 2, 39.

Reference

Department of the Army. Field Manual 6-0, *Commander and Staff Organization and Operations*. Washington, DC: U.S. GPO, 5 May 2014. Change 1 was issued on 11 May 2015. Change 2 was issued on 22 April 2016.

MAJ Richard Sharp is the brigade S-2 observer coach/trainer (OC/T) assigned to the Joint Readiness Training Center (JRTC) Operations Group. Before serving at Fort Polk, LA, he served as the brigade S-2, 1st Brigade Combat Team, and as the division collection manager, both for the 101st Airborne Division (Air Assault). He is a graduate of the Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance, and holds professional certifications in collection management, intelligence planning, and security fundamentals.

CW4 Ray Joyce II serves as the senior all-source intelligence OC/T assigned to the JRTC Operations Group. Before serving at Fort Polk, LA, he worked as the Joint Force Land Component Commander intelligence operations requirement manager for U.S. Army South. He has served as the chief advisor to the Commandant, Saudi Arabian Armed Forces Joint Intelligence School, brigade senior intelligence technician, information collection management team officer in charge (OIC), Levant ballistic missile defense analysis OIC, and Russian/former Soviet Union analysis OIC. He holds a bachelor's degree in psychology and is a graduate of Warrant Officer Intermediate Level Education course.

CW3 Roy Swearengin is the senior human intelligence (HUMINT) OC/T assigned to the JRTC Operations Group. Before serving at Fort Polk, LA, he served at the Combined Joint Special Operations Task Force–South J-2X with 5th Special Forces Group (Airborne). He has served as the operational management team OIC, brigade 2X, and advisor with 2nd Brigade Combat Team, 101st Airborne Division (Air Assault). He is a graduate of the Defense Advanced Tradecraft Course, Source Operations Course, and U.S. Army Forces Command's Advanced Operations Course–HUMINT.

U.S. Army photo by MAJ Sonie Munson, 2nd SBCT, 2nd ID Public Affairs

Soldiers of 2nd Battalion, 1st Infantry Regiment, plan for a mission at the Yakima Training Center, WA.

A Team Approach to Collection Management

by Lieutenant Colonel James King

Introduction

Collection manager is one if the hardest jobs in a brigade combat team. Unfortunately, it's a job often assigned to one of the least experienced people on the staff. This lack of experience and understanding of intelligence systems and operations often results in a less then optimal collection plan, one with holes big enough to drive a T-80 tank through it. However, the Army is a team sport, one that leverages its individual strengths at the appropriate time to achieve the desired effect. We can tackle the collection management problem in the same fashion. Building a team that can leverage the expertise of reconnaissance, organic collection assets, and echelons above brigade (EAB) assets will result in a collection plan that plugs its holes like a tank ditch in the Central Corridor.

Finding a Collection Manager

As the S-2 for a Stryker brigade, I found myself in the same dilemma as many brigade S-2s. We were training for a rotation at the National Training Center, and I had to appoint someone as our collection manager. My team at the brigade level was short several military intelligence (MI) officers, so the brigade commander graciously augmented us with some first lieutenants whose branch details were expiring soon. Doing so allowed these lieutenants to gain experience in an intelligence section before attending the Military Intelligence Captains Career Course. It was from this group that I had to find a collection manager.

I chose an officer whose branch detail was to field artillery. I believed his experience on the receiving end of collection

would help him make good decisions about the employment of sensors. Before our unit's validation exercise, I used the U.S. Army Intelligence and Security Command's Foundry Program to send him to a couple of collection management classes, one hosted in Hawaii and another at Fort Huachuca, Arizona, to familiarize him with the task. After he returned, I assumed he was ready for the role going into the validation exercise. I was wrong.

He didn't fail completely. He had a few successes but stumbled through most of it. The enemy problem set and the complexity of having to manage EAB assets at the National Training Center would be exponentially harder, and we had to up our game. I couldn't swap him out even if I wanted to because we had invested too much training in him. We had to find a way to make him better—or as they say in baseball, "raise the floor of our talent level." We discovered that very little academic focus is placed on the art and science of collection management. We had exhausted our Foundry options and were resigned to the fact that we were going to the batter's box with the staff section we had, rather than with the staff section we wanted.

Filling Two Additional Roles

At the same time that we in the S-2 were working through this problem, the brigade commander was working through how to incorporate a "chief of recon" for the brigade and who would fill that role. We were also kicking around ideas on how best to use the MI company commander. At the time, these were separate problems needing different solutions. We went to the National Training Center determined to try a few ideas to see what would fit.

Love it or hate it, doctrine or not, our commander wanted to have a "chief of recon." The process went through some fits and starts. We knew what we wanted the chief of recon to do—provide the brigade commander, S-3, and S-2 with recommendations on employment of the cavalry squadron—but we didn't know who should fill the role. After some trial and error, we settled on the cavalry squadron headquarters and headquarters troop (HHT) commander. We knew we didn't want to use the squadron commander, but we needed someone who could hold their own with the brigade staff. Before settling on the HHT commander, we tried the squadron executive officer and the squadron liaison officer. The executive officer had the necessary experience but his time was already split too many ways, and the liaison officer was generally a post platoon leader lieutenant who didn't have the requisite experience.

The MI company commander question was much easier to answer. It was determined early on that during operations the MI company would be task organized from the brigade engineer battalion to work for the brigade and take direction from the S-2. The question now was what role the commander would have in support of the S-2. I didn't want to take away the fact that he was a commander and make him an assistant S-2, but I also couldn't afford to waste his experience as an intelligence officer on just managing the day-to-day administration of his company, which his first sergeant and executive officer handled most of anyway. I needed to get him in the fight.

The Collection Management Team

Our solution to these problems came early in the National Training Center rotation. To effectively incorporate all the collection assets available to the brigade, we decided to build a collection management team. This team would exploit the unique subject matter expertise of each of its members in order to build a collection plan that maximized the strengths of the reconnaissance capabilities of the cavalry squadron, the brigade's organic intelligence sensors, and EAB assets. Let's take a look at each member of the team and what they bring to the fight.

U.S. Army photo by SGT Dommnique Washington, 7th Mobile Public Affairs Detachment

The scout platoon of Headquarters and Headquarters Company, 1st Battalion, 5th Cavalry Regiment, 2nd Armored Brigade Combat Team, 1st Cavalry Division, conduct a scout validation exercise January 21-22, 2020, at the Novo Selo Training Area in Bulgaria. They are evaluated on their abilities to navigate terrain while gathering, assessing, and reporting information, along with providing security and engaging targets when necessary.

Chief of Recon

Not every unit has a "chief of recon." It is a non-doctrinal position intended to provide the brigade staff with a subject matter expert on cavalry operations. Within those units that maintain a chief of recon, there is no consensus on who should fill the role. One thing we did know was our organization did not want to use the squadron commander as some units have done. As discussed earlier, we chose the HHT commander.

The HHT commander's role in the collection management team was to provide insight into how to best use the cavalry squadron to collect and what they could collect. As the only organic, all-weather collectors in the brigade, their effective utilization is vital to the success of the overall plan. An intelligence officer who has no experience with employing cavalry units often assigns tasks that turn out to be impossible to accomplish when attempted on the ground. This happens because intelligence collection managers make mistakes when they don't understand reconnaissance operations, such as the terrain doesn't support movement, the named area of interest is unobservable from where the reconnaissance team can get to, or the squadron is given too many named areas of interest to cover. Correct employment of the cavalry is the first layer of the team approach to collection management.

The Military Intelligence Company Commander

A brigade combat team's MI company commander has historically been one of the most misused and often underutilized leaders in the organization. As with the chief of recon, very few units use their MI company commander the same way. Some use them as "just a commander," leaving them to the day-to-day administration of the company. Others attempt to tap into the seniority of the individual within the intelligence branch and use them as another assistant S-2. In the collection management team concept, you get the best of both sides of the coin.

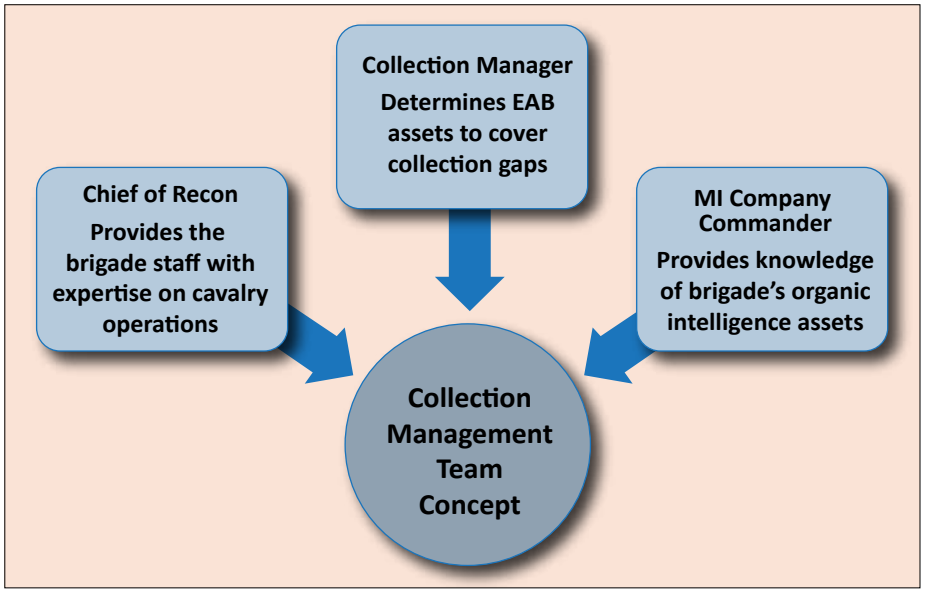
The MI company commander provides the knowledge on how to use the brigade's organic intelligence assets. Employed properly, a brigade combat team brings to the fight a fairly robust set of signals intelligence, human intelligence, imagery intelligence, and unmanned aircraft systems. Aligned with what the cavalry can do, you have an all-encompassing overlay of all the collection that a brigade combat team can do on its own without asking its higher headquarters for help.

Bringing the MI company commander into the planning process has the benefit of instilling a sense of ownership for the operations that their command is undertaking. Too often, MI company commanders watch as the brigade combat team S-2 farms out their assets without understanding the intent or requirements. This newfound understanding of the operation can energize the MI company commander to ensure that collection is happening and is happening effectively. When problems arise, as they inevitably will, the MI company commander can exercise mission command to solve problems and ensure limited to no interruption in collection.

The Collection Manager

In the team construct, the collection manager is responsible for determining the necessary EAB assets to cover the brigade's collection gaps. They do this by overlaying what the cavalry squadron can cover with what the MI company is able to cover. It is the collection manager's responsibility to request EAB assets to provide coverage for any gaps.

As the only full-time member of the team, the collection manager is also responsible for all the traditional tasks of collection management, including building the collection plan, the information synchronization matrix, Annex L to the operation order (OPORD), the collection overlay, and any briefings as a part of the planning process. The collection manager is further responsible for working with the next higher headquarters to secure EAB assets and to fight for dynamic re-tasking if needed. Ultimately, the collection manager is responsible for all aspects of the final collection plan.



The team concept exploits the distinctive subject matter expertise of each of its members.

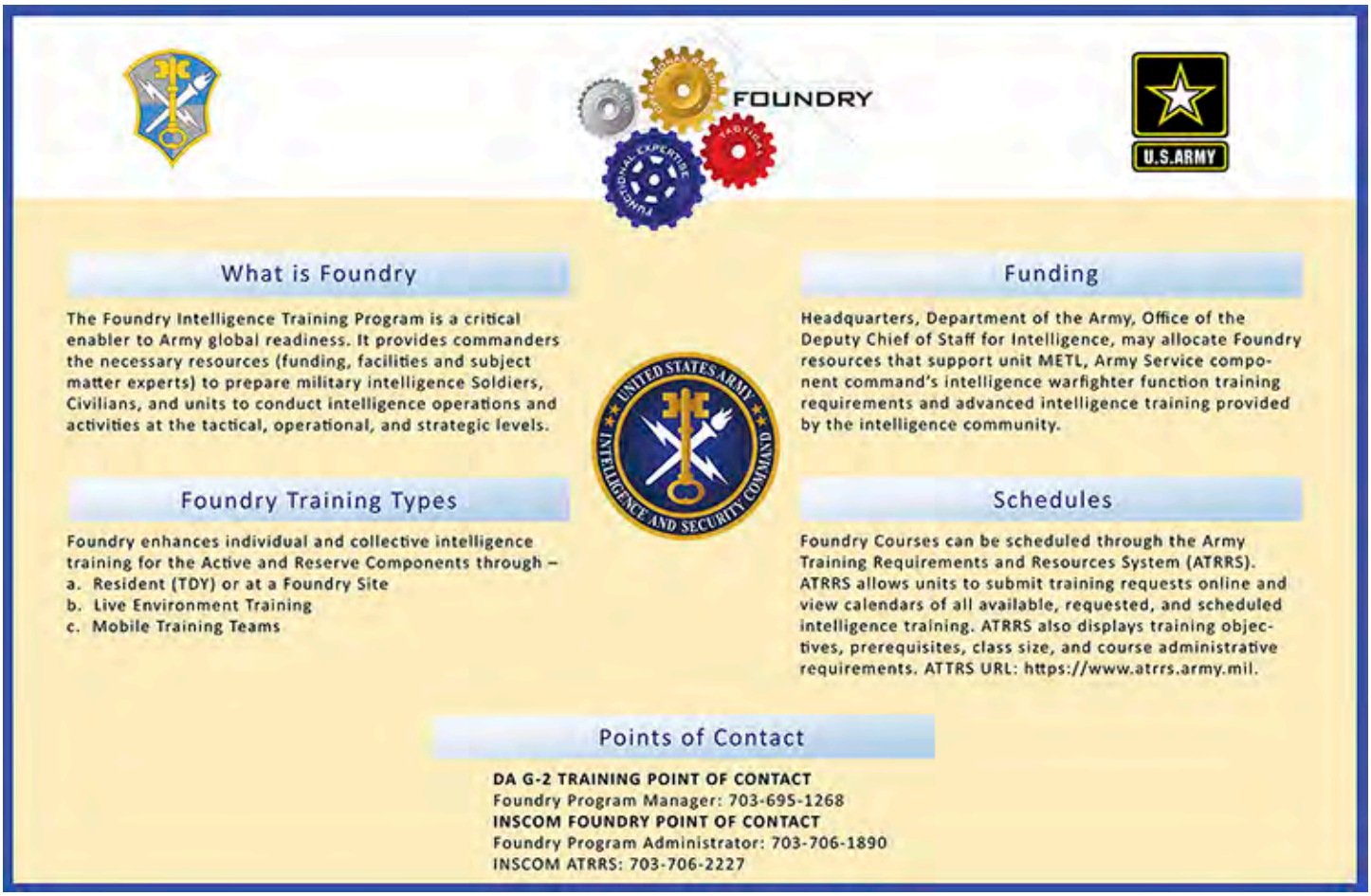
How It Works

In practice, the collection team is most effective during the military decision-making process, when building the collection plan for specific operations. During this process, the collection manager will assemble the other members of the team and lay out the requirements for the upcoming operation. They must do this early enough to get the cavalry squadron their assignments with enough time to allow for movement to cover those locations. The collection manager gathers the inputs of the other members of the team, drafts requests for EAB assets, and builds the overall collection plan. While the other two members of the team return to their primary duties, the collection manager participates in the wargame, socializes required changes with the other team members, writes Annex L of the OPORD, and briefs the collection plan as a part of the OPORD brief to subordinates. The other members of the team come together one more time before execution of the operation to participate in the intelligence collection rehearsal and combined arms rehearsals.

Final Thoughts

The preceding method is a "way" to achieve success in the realm of collection management, particularly when your organization's expertise level is not where you would like it to be. This approach is effective only if members of the team take ownership of their respective element. However, this approach will fail if the "chief of recon" is not a trusted member of the cavalry squadron. All interested parties must accept that individual's recommendations. Any second-guessing by those who think they know better will derail the entire plan. In some cases, this may require brigade commander emphasis to ensure the team isn't overridden. Effective implementation of this approach will result in a holistic collection plan that will provide the S-2 and commander as complete a picture of the battlefield as possible.

LTC James King serves as the G-2X for an Army Service component command. He previously served as a theater analysis and control element chief, a military intelligence battalion executive officer, and a brigade combat team S-2 for two different Stryker brigade combat teams. LTC King holds a bachelor of arts in sociology from the University of Washington and a master's degree in strategic intelligence from American Military University.



Assessing Collection

Image courtesy of PEO IEWS

by Mr. Scott A. Pettigrew

An artist's rendering of the Enhanced Medium Altitude Reconnaissance and Surveillance System.

Intelligence at the Front

In 1943, an American Soldier manning an observation post in Tunisia reported a column of Panzer tanks moving toward Allied lines. The division intelligence officer (G-2) jumped quickly into action to confirm the report, verifying the location of the observer and the coordinates of the reported tanks. The G-2 plotted the reported location on a topographic map, revealing very steep terrain, what some would call a cliff, and thus impossible for an armored vehicle to navigate. The G-2 relayed the information back to the observer to confirm the report, leading to the discovery that the well-meaning scout was looking in the wrong direction. The dust he saw was never adequately explained, but the G-2 concluded that enemy tanks were not the cause.[1] The rapid collection assessment that the G-2 had performed prevented an entire American corps from reacting to an enemy attack that never was. Although the available technology has improved, the importance of assessing collection remains as vital today as it was in World War II.

Overview

Assessing collection, what Army doctrine in 1943 referred to as "evaluation," seeks to measure the performance of collection assets and the relevance of their reports in supporting a unit's intelligence requirements. Assessments help determine if an activity contributes to accomplishing a task or achieving a desired objective.[2] The staff performs operational assessments to inform commanders of the progress of operations, identify risks, and establish resource requirements that will lead to more effective operations.[3] To optimize information collection, the staff continuously assesses the information collection plan; the performance of Army and joint force intelligence, surveillance, and reconnaissance (ISR) assets; and the processing, exploitation, and dissemination (PED) of the resulting intelligence.[4] Collection managers have the primary responsibility to assess the results from reconnaissance missions, surveillance tasks, intelligence operations, and security operations. These assessments help to improve situational understanding and the acquisition of targets and to support commander decision making.[5] Based on the assessment, information collection plans are modified, and tasks to collection assets are changed to better support the unit and commander's intelligence requirements.

Assessing collection happens both during and after each collection mission. Tactical headquarters and ISR asset controllers and analysts have some capacity to evaluate the performance of collection missions as they occur. It is preferable for the staff to identify poor mission performance while it can still be corrected than after the operation has ended. Some ISR missions are not conducive to adjustments during execution, such as the use of special operations forces that may schedule infrequent communication windows to relay reports. Evaluating and adjusting an

ongoing mission requires that the element doing the evaluation have access to the data in near real time and that they can communicate with the collection asset or those who control it.

It is useful to assess collection from two different perspectives. Measures of performance help determine the proper execution of collection missions.[6] However, a perfectly executed collection operation may not answer the underlying question, which is why we also want to measure effectiveness. Measures of effectiveness seek to discover if we are doing the right things. In other words, are we collecting appropriately? This means being sure we are collecting when and where we need to, and with the correct sensor type and suitable indicators and specific information requirements (SIRs) to answer the supported intelligence requirement. Perfectly executed ISR that does not solve the intelligence requirement supporting the underlying objective is ineffective. An intelligence requirement designed to facilitate targeting must produce information that enables the accurate and timely delivery of fires. Merely answering the intelligence requirement is not sufficient if the targeting team still lacks the necessary data to engage.

Assessing the measure of performance and measure of effectiveness should happen simultaneously, but considering the pace of operations and limited time available, determining effectiveness is more important than evaluating performance. Supplying the commander with the intelligence needed to make more informed decisions is of the utmost priority. Repairing performance issues may be necessary to improve effectiveness, but we do not want to spend time addressing performance aspects and lose focus of the most critical reason we conduct ISR. The collection manager, assisted by the staff, should start by evaluating ISR's effectiveness in support of the commander's priority intelligence requirements (PIRs).

Before conducting any type of assessment, we must first identify what it is we are assessing. One method is to develop indicators of both good performance and effectiveness.[7] The information collection plan and other staff planning documents possess the indicators needed to assess both performance and effectiveness. In addition to the indicators, we must know why we are collecting. Every collection mission has a purpose. The purpose is the decision, action, analysis, or planning process that the intelligence requirement supports.

Priority Intelligence Requirements

PIRs are the commander and staff's most important intelligence needs to understand the threat and other aspects of the operational environment.[8] However, the assessment should not gauge effectiveness based only on answering PIRs. The staff must look more in depth as to the reason intelligence questions have been given priority and determine if the objectives were met.

Effectiveness is measured based on the purpose of the collection mission. We can assess collection effectiveness by ascertaining if the collection met the objective. The PIR list alone does not identify the purpose. Documents such as the decision support matrix, target synchronization matrix, and event matrix provide the intent behind each PIR. Collection assessments that only gauge whether the PIR was answered may fail to meet the underlying objective.

Although the PIR's purpose is to focus the intelligence effort, answering the PIR does not necessarily satisfy the intent of the requirement. As Figure 1 shows, satisfying commander decision points and targeting objectives determine effectiveness. If effectiveness is not achieved, the collection mission elements (indicators, SIRs, named areas of interest, and collection times) are an excellent place to start to review performance.

MOP

MOE

Priority Intelligence Requirement	Indicators	Specific Information Requirement	NAI	Start	Stop	Assets: Brigade: 1st BN	2d BN	3d BN	3/67 CAV REG	Shadow	Prophet/LLVI	HCT	Assets: EAB: COMINT	ELINT	HUMINT	GEOINT	CI	MASINT	Decision Point	Target Area of Interest
1. Where along AA1 will the 375th BTG initiate shaping operations for an area defense?	1. Special purpose forces in hasty battle positions in vicinity EA1 and EA2	1.1.1 Report communications coordinating enemy movement	1,2	H-48	H+2	C	C	C	C	NT	TA	NT	R	R					1	1
		1.1.2 Report movement of fighters into defensive positions	1,2	H-48	H+2	C	C	C	TP	TA	TA	NT	R			R		R	1	1
		1.1.3 Report communications of reconnaissance assets	1,2	H-48	H+2	C	TA	C	TP	TA	TP	NT	R	R					1	1

Figure 1. Sample Information Collection Matrix Showing Indicators of Performance and Effectiveness[9]

Decision Points

A PIR is customarily written to support specific commander decision points but may also support other requirements such as targeting objectives. Whether ISR has adequately supported the commander's decision point is not always apparent. Open communication between the collection manager and operations officer (G-3/S-3) will help clarify if the collection is sufficient or needs more work. The collection task, indicators, and SIRs may need adjustment to support the decision point adequately.

To assess performance, collection managers can use the information collection matrix to determine what right looks like by deciding if the ISR asset collected in the designated place and at the right time, using relevant indicators and reporting the assigned SIRs. Combat training center observations have identified weak indicators and SIR development as a common trend that negatively affects collection performance.

Indicators inform the collector or sensor analyst of the relevant observables or signatures. Do not underestimate the importance of well-thought-out, insightful indicators. Although collectors and single-source analysts may be well trained, many lack sufficient experience to know all the signs that a particular activity has happened or is about to happen. Irregular warfare creates unique challenges with indicator development because everyday life events and patterns of movement can be mistaken for, or hide, insurgent actions. Foreign cultures also present challenges—"the American way" can be quite different from how things are done in distant lands.

ATP 2-01.3, *Intelligence Preparation of the Battlefield,* contains sample indicators for spotting enemy offensive and defensive actions.[10] The staff should develop additional indicators over time as the unit's understanding of the threat and their tactics increases and by leveraging all the expertise and experience across all staff elements and outside intelligence agencies. The staff element that creates the intelligence requirement owns the primary responsibility to develop the indicators and SIRs. Do not rely on the collection manager to perform this function. The collection manager does not have the time or personnel to complete the analysis on every intelligence gap and gain an understanding to the level of detail required.

High-Payoff Targets

The targeting team reviews and evaluates the entire decide, detect, deliver, and assess targeting process after the completion of each 24-hour targeting cycle. Participation by the entire targeting team will provide a more accurate reading than if the collection manager attempts to evaluate only the "detect" function in isolation. Collection effectiveness in support of targeting during the "detect" phase is typically easier to ascertain. However, incomplete intelligence reporting may result in delivering fires with incomplete data to achieve the best effect. Simply locating a target is not always sufficient to realize the best result. Targeting officers may also require details such as the posture of the target to select the best delivery asset or munition.

A Lesson on Assessments

From 24 March to 9 June 1999, a United States-led North Atlantic Treaty Organization (NATO) force bombed Yugoslavia from the air in an attempt to influence the Yugoslav President to end his country's human rights abuses against the people of Kosovo. The coalition reported great success (based primarily on strike aircraft observation reports) in destroying 120 tanks, 220 armored personnel carriers, and 450 artillery pieces.[11] After the conflict ended, U.S. Air Force investigators on the ground could only confirm 8 percent of the targets reported destroyed. Many of the military hardware targeted turned out to be decoys, or the munition had simply missed the mark.[12] The air campaign produced minimal effectiveness. Airborne ISR assets performing a battle damage assessment were forced to fly less than optimal orbits to avoid the surface-to-air missile threat, hampering battle damage assessment efforts.[13] The lack of an accurate battle damage assessment left the coalition military and political leaders with a false perception of mission success and influenced decisions based on inaccurate information. The inability to precisely measure the level of collection effectiveness also prevented commanders from adjusting operational mission parameters to increase performance.

The targeting team assesses information collection in support of targeting based not only on whether the target was located but also on meeting the target selection standards. Target selection standards address accuracy and other criteria that must be met before targets can be engaged.[14] The target selection standards will affect determining which ISR sensors are best suited for each target and will also feed SIR development. The SIRs inform the PED analyst on what to report and at what level of detail. Collection managers must ensure an ISR platform can meet both the target selection standards and SIRs before designating it to locate or track a target. Figure 2 (on the next page) shows sample target selection standards. These standards consist of four categories:

- **Target location accuracy or target location error.** The grid coordinate that the sensor report provides must be less than the maximum error allowed. Most targets will have multiple accuracy requirements depending on the type of delivery asset used. A 105-mm howitzer, depending on whether the means to adjust fire is present,

may necessitate higher location accuracy than engaging the target with air interdiction assets that have the ability to refine the target location.

- **Size of the enemy activity (point or area target).** The size of the formation may influence delivery asset and munition selection. Targeting officers may also bypass targets that fail to meet the minimum size to preserve delivery capacity for targets with a more significant payoff.
- **Status or posture of the activity (stationary, moving, hull defilade, etc.).** The target's posture is required for most entities because it affects timeliness requirements and will influence delivery asset or munition selection. Collection managers should understand ISR asset capabilities and recognize that some assets are poorly equipped to determine posture.
- **Timeliness of the information.** Tactical assets can move. Some assets, such as a tank formation, can quickly shift from a defense to a march formation, while a massive headquarters takes more time to tear down and pack up before displacing. Therefore, a 1-hour-old report may be sufficient to employ fires against some targets while others will require a more recent confirmation.

High-Payoff Target	Timeliness	Accuracy	Posture	Min. Size
Artillery	10 min	500 M	Stationary	Section
Command Post	1 hr	1 KM	Stationary	Battalion
Armor	15 min	750 M	Stat/Moving	Company
SA Missile	30 min	300 M	Stationary	Section

Figure 2. Sample Target Selection Standards[15]

Other Intelligence Requirements

All intelligence requirements are important to answer; otherwise, they would remain intelligence gaps and no resources would be allocated to satisfy the requirement. The reality of large-scale combat operations is that time available for the staff to conduct assessments is in short supply. PIRs are questions that must be answered, while other intelligence requirements are less urgent and should receive collection resources only if possible.[16] If pressed for time, assess collection in support of PIRs first, and only evaluate ISR leveraged against other intelligence requirements as time permits. Another time-saving tool is to conduct an initial assessment for all requirements, such as the number of collection missions and the number of reports per requirement while saving a detailed evaluation for the commander's PIRs.

Assessing the "Why"

Determining why performance or effectiveness did not meet expectations is vital and frequently misidentified. Failure to accurately identify the underlying cause of performance or effectiveness issues could lead to applying the wrong solution to the problem. We have already discussed many of the reasons why collection may be ineffective or perform poorly based on not meeting the specific collection requirements or target selection standards, but a myriad of issues can cause information collection challenges, some of which are specific to the type of collection asset or the operating environment.

An excellent first step in determining where the collection misfired is to ask the collection asset operators or single-source analysts. ISR asset operators possess an intimate understanding of the capabilities and limitations of their systems. They can provide performance insights and assessments that collection managers may find challenging to reach based on less training or experience. A time-saving approach would be to merely ask the collector why the mission did not produce the desired results. Organic single-source intelligence sections should provide the collection manager with an assessment of their intelligence discipline's performance and effectiveness, along with recommendations for improvement.

A fundamental and standard method to assess human intelligence (HUMINT) collection team performance is to count the number of reports generated over a designated period. While this technique is not a bad starting point, leaders must look deep to determine why team production levels vary and not reach rash conclusions related to Soldier proficiency or effort. HUMINT collection teams are frequently attached to maneuver battalions. How the force employs the asset, population density, cultural norms, civilian support for the enemy (either passive or active), and interpreter proficiency or access can all affect team production or report effectiveness in answering the requirements.

Signals intelligence (SIGINT) and geospatial intelligence (GEOINT) collection assets may experience performance issues due to terrestrial or space weather, terrain, line of sight, or range limitations. Weather can present challenges beyond merely how the elements affect the sensor. Human activity, whether trained military personnel, insurgents, or civilians, changes with the weather. Do not discount the weather as a potential reason why activity and reporting have either increased or decreased.

Collection managers should also consider operational environment characteristics as possible reasons affecting ISR effectiveness. National, religious, and cultural holidays and celebrations, including sporting events, can influence ISR

ATO AB						
Echelon	ISR Asset	NAIs	DPs	HPTs	Effectiveness	Performance
EAD	E-8 JSTARS	1002, 1003	1	5,7,9	Located 12xG6	Outside time requirement
	EC-130 Compass Call	1105 - 1110	3	3	Located 3xCrotale	No issues
	SOF	1250	5	NA	ID possible insurgent cell	No reports
Division	Gray Eagle 1 (FMV)	1105, 1106	1	5,7,9	Located tank column	SIR inadequate
	Gray Eagle 2 (FMV)	1107, 1108	3	3	Possible C2 node vic WG	No issues
	Gray Eagle 3 (FMV)	1109, 1110	5	2	NA	NMC - Maintenance
	Gray Eagle 4 (GMTI)	1105 - 1110	2	NA	100+ vehicles vic AA1	No issues
1 BCT	RQ-7B Shadow	1007, 1008	4	1	NA	Grounded - High winds
	HUMINT	1001, 1002, 1003	5	NA	No reports	No interviews
	PROPHET	1001, 1002, 1003	NA	6,8	ID possible SPF net	DF did not meet TLE
	Cavalry Squadron	1009	1	2	No pertinent observation	Late to objective

Figure 3. ICSM Modified to Track Effectiveness and Performance

asset observations and reports. Activity may inexplicably increase or decrease depending on the culture and nature of the event or season.

Collection Assessment Working Tools

The information collection synchronization matrix (ICSM) is a useful ISR planning and execution tool.[17] The collection manager builds the ICSM for each daily tasking cycle, depicting ISR asset support and how each sensor's mission times and collection locations support friendly operations. The current operations staff uses the ICSM to ensure collection remains focused on the commander's priorities. The product helps understand the overall goals of the ISR plan when making adjustments through dynamic retasking.

The ICSM is also well suited to be a working tool to assess collection. It is easy to modify the document to track the effectiveness and performance of each mission (Figure 3). As previously mentioned, once either an effectiveness or a performance issue is identified, more research must be done to fully understand the problem and ascertain why effectiveness or performance suffered and what actions are required to prevent future challenges.

To maximize the time available and leverage resident expertise, the senior intelligence officer should spread the assessment duties throughout the intelligence section based on functions and responsibilities, with the collection manager retaining overall responsibility for collection assessments:

- **G-2/S-2 current operations:** Assess active ISR missions and provide timely feedback to collectors and PED analysts to improve the performance and effectiveness of ongoing tasks.
- **Fusion section:** Assess ISR effectiveness support to PIRs and work with the intelligence and operations planners to assess intelligence support to decision making.
- **Intelligence targeting section:** Collaborate with the field artillery intelligence officer and the targeting team to evaluate collection support to targeting.
- **GEOINT/SIGINT/G-2X:** Assess both the measure of effectiveness and the measure of performance of each collection mission within each single-source section's respective discipline.

Collection Assessment Presentation Tips

How a unit presents information to the commander is based on the individual commander's preference and the staff's creativity. In general, graphics are preferable to high volumes of text, and the charts should be easily understandable and require minimum explanation. Figures 4 (below) and 5 (on the next page) are examples of how to demonstrate collection effectiveness in supporting commander decision making and targeting priorities. Some leaders desire to see more data related to the number of missions conducted compared to how many were planned,

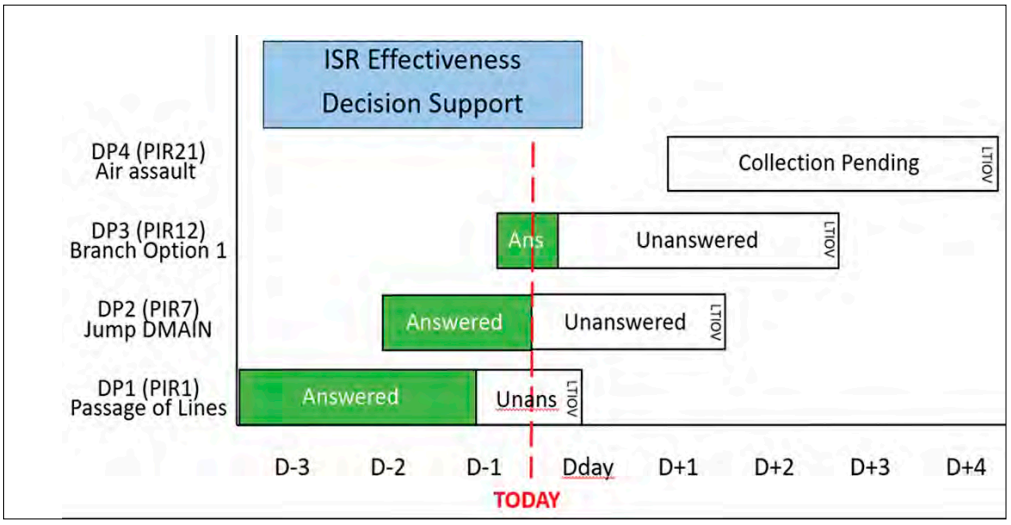


Figure 4. ISR Effectiveness Decision Support

or production numbers tied to the number of reports received. Presenting this type of data can give a false impression of either performance or effectiveness. Be prepared to provide analysis-based reasoning, digging deep to flesh out the "why" for any data presented.

In Figure 4, the left side of each bar represents the approximate time when the requirement becomes active and collection begins. The graphic provides a visual representation to the commander of progress toward the identified intelligence requirements in support of anticipated decision points prior to the latest time information is of value (LTIOV).

Figure 5 counts the number of enemy systems located and the measures of effectiveness based on meeting daily and overall targeting goals. The graphic provides a visual representation to the commander of progress toward locating high-payoff targets.

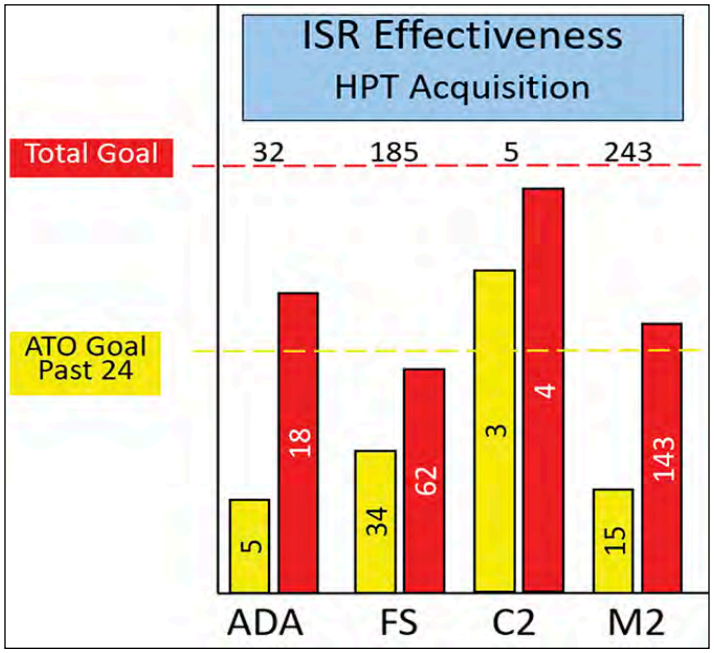


Figure 5. ISR Effectiveness High-Payoff Target Acquisition

Conclusion

The staff continuously assesses the operation to know where they stand in accomplishing the specified tasks and reaching the desired end state, and to identify where they need to make adjustments to get back on track. Within the overall assessment function, the collection manager leads the critical role of coordinating and conducting the evaluation of ISR activities. Failure to thoroughly assess information collection could contribute to missed targeting opportunities and the commander not obtaining the knowledge necessary to make the most informed decisions. Assessments are important and should not be regarded as optional. Proper planning will create a framework in which the entire intelligence, operations, and fires team plays a role in assessing collection, thus maximizing ISR asset resources and meeting the commander's objectives.

Endnotes

1. Stedman Chandler and Robert W. Robb, *Front-Line Intelligence* (Washington, DC: Infantry Journal Press, 1946), 93.

2. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: The Joint Staff, 17 January 2017). Change 1 was issued on 22 October 2018.

3. Department of the Army, Army Techniques Publication (ATP) 5-0.3, *Multi-Service Tactics, Techniques, and Procedures for Operation Assessment* (Washington, DC: U.S. Government Publishing Office [GPO], 7 February 2020).

4. Department of the Army, ATP 3-55.3, *Multi-Service Tactics, Techniques, and Procedures for Intelligence, Surveillance, and Reconnaissance Optimization* (Washington, DC: U.S. GPO, 3 September 2019) (common access card login required).

5. Department of the Army, ATP 2-01, *Plan Requirements and Assess Collection* (Washington, DC: U.S. GPO, 19 August 2014).

6. Office of the Chairman of the Joint Chiefs of Staff, JP 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 16 June 2017).

7. Department of the Army, ATP 5-0.3, *Multi-Service Tactics, Techniques, and Procedures*.

8. Department of the Army, Army Doctrine Publication (ADP) 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 31 July 2019).

9. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. GPO, 1 March 2019), 6-24. The article figure is adapted from ATP 2-01.3, Figure 6-15, Information collection matrix example.

10. Ibid.

11. John Barry, "The Kosovo Cover-Up," *Newsweek,* 14 May 2000, https://www.newsweek.com/kosovo-cover-160273.

12. Ibid.

13. Benjamin S. Lambeth, *NATO's Air War for Kosovo: A Strategic and Operational Assessment* (Santa Monica, CA: RAND Corporation, 2001), 111.

14. Department of the Army, ATP 3-60, *Targeting* (Washington, DC: U.S. GPO, 7 May 2015).

15. Ibid. The article figure is adapted from the example table shown on page D-2 of ATP 3-60.

16. Department of the Army, ADP 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019).

17. Department of the Army, ATP 2-01, *Plan Requirements and Assess Collection*.

Mr. Scott Pettigrew is a defense contractor who currently works at the U.S. Army Training and Doctrine Command G-2, Operational Environment Center, Intelligence, Surveillance, and Reconnaissance Integration.

by First Lieutenant Moriamo O. Sulaiman-Ifelodun and Colonel Robert M. Wilkinson (Retired)

Introduction

How can S-2s and collection managers more effectively integrate open-source intelligence (OSINT) into planning and requirements to improve intelligence for a changing and challenging world? This article provides a proposal to meet this objective by better integrating OSINT collection requirements into information collection planning as part of multi-domain operations.

Why Now?

The digital information environment continues to evolve, bringing far-reaching and dynamic challenges for the operational environment. To address the challenges, commanders must understand all relevant aspects of the digital information environment, including identifying and responding to our adversaries' influence operations. OSINT can address many of the commander's intelligence requirements related to the operational environment, if G-2/S-2s and collection managers devote sufficient time and effort to developing and designing collection requirements up front and continue refining them throughout multi-domain operations. G-2/S-2s and collection managers can leverage OSINT as part of a fully coordinated planning effort so that requirements are developed appropriately using OSINT tools and capabilities joined with regional, cultural, and language expertise.

Our suggestion to G-2/S-2s and collection managers, especially those who have not considered OSINT recently, is to revisit OSINT doctrine. ATP 2-22.9, *Open-Source Intelligence* (and its classified companion *Volume II*), issued in 2019, improves understanding of OSINT as a collection discipline. Intelligence staffs should already be familiar with ATP 2-01, *Plan Requirements and Assess Collection*, issued in 2014. Unfortunately, ATP 2-01 does not discuss the specifics of information collection planning for each intelligence discipline. Therefore, we suggest ATP 2-22.9, chapter 3, as a starting point to increase understanding of collection management for OSINT.[1] To address any remaining questions, we offer this article to help Army intelligence professionals and organizations achieve increased understanding in breadth and depth of intelligence operations through OSINT.

OSINT 101

For those unfamiliar with OSINT, here is a quick overview. Congress defined OSINT as "intelligence that is produced from publicly available information [PAI] and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[2] OSINT results from collecting and analyzing information obtained from the publicly accessible portion of the global information pool.[3] Therefore, the term *OSINT* refers to the specialized intelligence discipline, single-source products created, and the collection activity itself.

OSINT is often referred to as open-source information, which is a misnomer. PAI is raw material that can be processed, exploited, and disseminated as an OSINT product or as inputs to all-source production. OSINT is an integral part of the intelligence warfighting function through the collection of PAI to answer intelligence requirements. Ignoring PAI as a source of intelligence reduces collection effectiveness. PAI collection for other purposes, such as information collection for operations, is not an OSINT activity. However, commanders should consider how much operations

security (OPSEC) risk their operations create when collecting PAI without using the G-2/S-2's trained and equipped OSINT practitioners to answer requirements.

OSINT traces its roots to foreign broadcast monitoring services during World War II. Understandably, 21st century OSINT is far more complex. The ever-growing multitude of modes generating data and content are changing the ways PAI is published and consumed, creating perpetual challenges for OSINT as a discipline. Therefore, the OSINT discipline evolves in real time as the proliferation of new media platforms and "Internet of Things" devices generating PAI continues to mature. Unfortunately, policy generally lags behind technology. OSINT is an evolving discipline; its tactics, techniques, and procedures frequently change as technologies stack, creating exponential change in the cyberspace domain.

In 2016, OSINT was revitalized through new Department of Defense (DoD) and Army policies designed to address explosive growth in traditional and social media digital content as well as the advent of new, rich PAI data sources that new technologies were generating. To address a growing demand signal from commanders, the Army OSINT Office (AOO), at the U.S. Army Intelligence and Security Command, was established and became the man-train-equip proponent for OSINT. An acknowledged leader in the DoD for its ability to field OSINT capabilities, AOO raised the DoD standard through training courses, requirements and capabilities management, and auditing/compliance functions. For the Army, AOO is the primary linkage for developing an OSINT capability. G-2/S-2s and collection managers can become familiar with AOO offerings by visiting their web portals and attending the monthly community of interest video teleconferences.

So Why Do Military Intelligence Organizations Need to Improve Their OSINT Capability?

Upon receipt of a new mission, we instinctively turn to the internet and smart devices to develop foundational information and knowledge for mission analysis and intelligence preparation of the battlefield. OSINT can be the starting point to tip and cue intelligence disciplines when generating intelligence knowledge, developing awareness, and tracking events and atmospherics as they develop. It helps further refine situational awareness and enrich understanding of the operational environment to better inform the commander and staff. OSINT also provides indicators for warning to direct deeper research. OSINT can be agile when configured to support situational development and warning missions.

Photo by Joseph Eddins

Publicly available information is becoming increasingly important in the fields of intelligence analysis, cybersecurity, and criminal investigations, among others.

OSINT is comparatively cost-effective. It is quite often the only persistent information collection capability available when exquisite systems and capabilities are unavailable or deployed elsewhere. With training, tradecraft, and tools, a multitude of PAI data points can be collected, processed, and exploited as a single-source production effort or can support vitally important all-source production. OSINT enhances the intelligence process, particularly by tipping and cueing other intelligence disciplines for tasking and collection—making more effective use of a system of systems. Moreover, OSINT can support targeting with insights that enrich the target picture and inform assessments of nonlethal effects or post-strike battle damage. Finally, when it comes to shaping strategic engagements with our partners and allies, we often look to OSINT as the entry-level sharing opportunity to build or strengthen trust with these partners.

A solid understanding of intelligence oversight and Army OSINT guidance is essential to the proper planning and conduct of OSINT activities. DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities,* directs us to start collection with the least intrusive collection methods first. Specifically, procedure 2, "Collection of [U.S. person information] USPI," specifies PAI as the least intrusive.[4] Army Directive 2016-37 (U.S. Army Open-Source Intelligence Activities) states that when an intelligence professional "copies, stores or otherwise preserves" something into an intelligence component database, they have conducted an OSINT collection activity.[5] For most all-source analysts, suddenly becoming a collector is a radical change!

What G-2/S-2s and Collection Managers Need to Know about OSINT to Improve Collection Management

For all the reasons described above, OSINT is a remarkably effective discipline for developing a holistic picture.

But are we properly and effectively planning for, executing, integrating, and streamlining a deliberate PAI collection effort in support of our everyday intelligence missions? Do we have the appropriate capability in place (defined as properly trained and equipped personnel) to effectively address information and intelligence gaps in a timely manner? Do G-2/S-2s and collection managers understand how to leverage that capability appropriately? How does one identify, describe, and nominate an OSINT collection requirement to an external OSINT activity? How do we consider the OSINT discipline's prime directive of "collect once, share broadly" to minimize redundancy and collection fratricide? In this area, doctrine and practice need to be updated. Here is a suggested path.

Going back to basics, the intelligence process, shown in Figure 1, begins with plan and direct. More time and effort must be devoted to this step in order to properly focus and leverage PAI collection and OSINT processing, exploitation, and dissemination (PED) to support all-source or single-source production. Let's begin the process of planning and directing by appreciating the discipline's unique challenges.

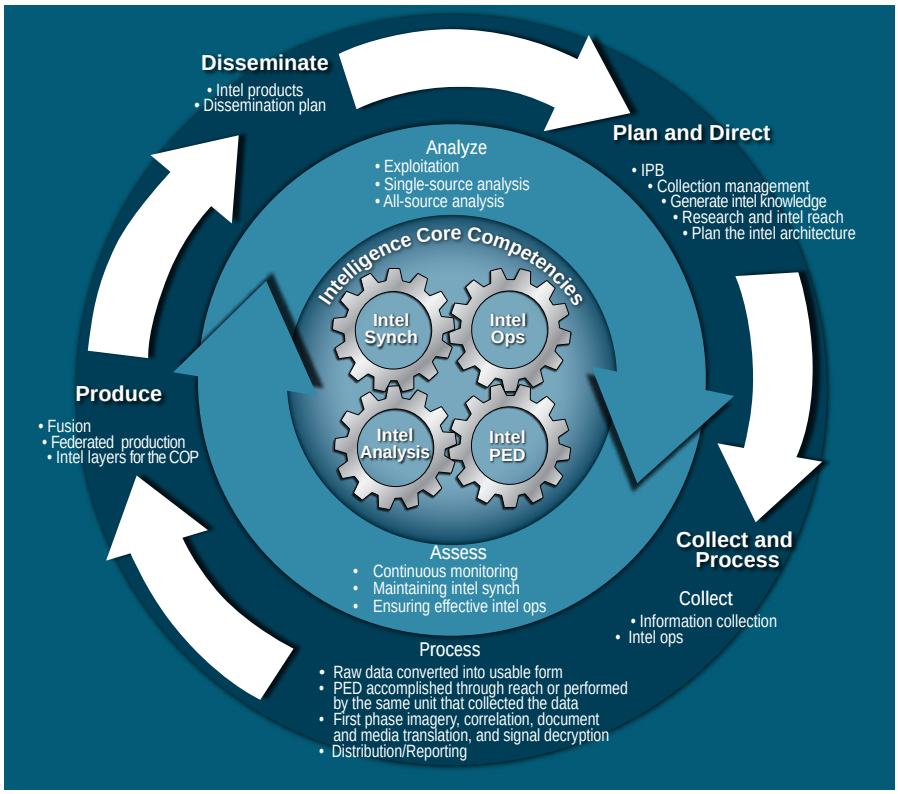


Figure 1. The Intelligence Process[6]

Collection managers must understand the supporting OSINT activities' capabilities, limitations, and constraints. OSINT-specific constraints include obtaining proper authorities and developing a plan to address all OPSEC and cybersecurity risks. The OSINT activity must have—

- A foreign intelligence or counterintelligence mission.
- An OSINT authority granted by a commander at the proper echelon.
- A validated intelligence requirement.
- An approved collection plan (including a risk assessment).

Time is another limiting factor. G-2/S-2s should understand that the time necessary for OSINT planning, initial research, collection, and PED is proportional to the complexity of the requirement and the scope of the question. Deliberately crafted, precise, and time-bounded questions are best suited for OSINT activities.

The digital information environment is dynamic, and its constant changes present a variety of challenges. The sheer volume of content and data generated each day is daunting. It requires skill, technical expertise, cultural knowledge, language capabilities, and technological aids, all of which are constantly evolving. Our experience in the U.S. Army Pacific area of responsibility shows we must be efficient and effective. Collection managers should understand each OSINT activity with a stake in their area of responsibility. Coordination and collaboration are critical to achieving success and avoiding redundant collection.

Geographical and operational boundaries are normal collection planning considerations; however, OSINT practitioners operate in cyberspace. Proximity to the target matters, but more important is the question, Which OSINT activity has the best capability and domain expertise to address this requirement?

Information control mechanisms vary across the operational environment. Nation states where censorship is high and freedom of the press is correspondingly low are often the highest risk targets. Therefore, risk versus reward is always a consideration. Hard targets require more precision, creativity, and tradecraft. Collection managers across the intelligence community should protect access to certain open sources for only the most advanced OSINT activities.

With continuing advances in technology and telecommunications, it is possible to address existing requirements in new ways and to develop new intelligence questions that were not considered in the past. Collection

managers should frequently consult with their supporting OSINT activity on emerging requirements to understand and appreciate what novel capabilities may be available and then update collection strategies and the staff accordingly during integrated planning sessions.

Collection managers must coordinate with joint, interagency, and multinational partners to avoid duplicate collection and ensure widest dissemination. Creating "swimlanes" for each partner's OSINT capability is a good way to organize a theater-wide OSINT effort, whether by topic, country, region, warfighting domain, or combat capability. Keep in mind that the goal is to avoid duplicative visits to the same resources in order to minimize risk. By collecting once and sharing broadly, we make the best use of resources and domain expertise, ultimately paying off in both effectiveness and efficiency.[7]

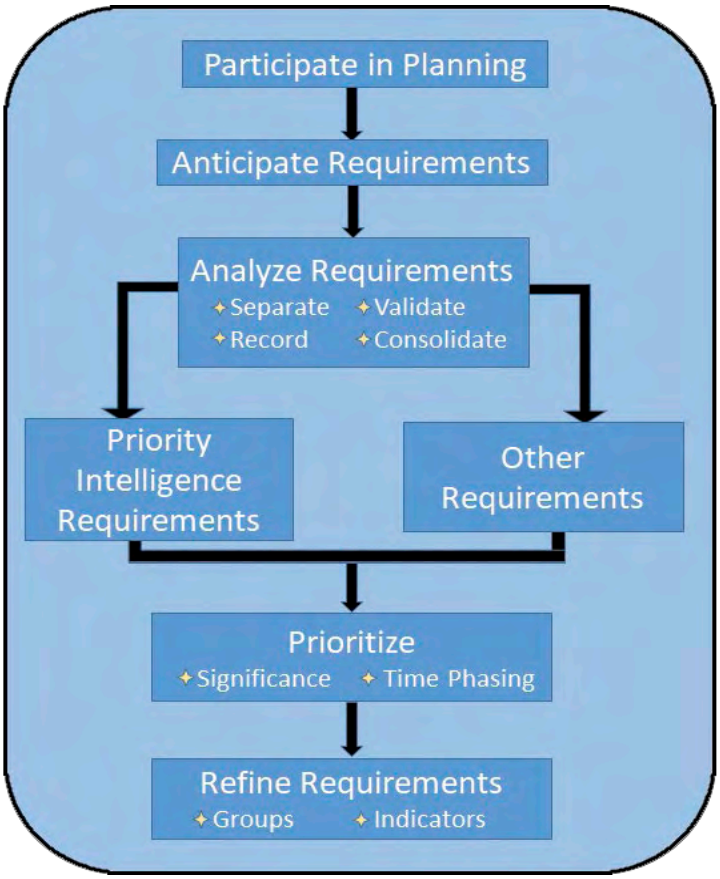
Design and Architecture Considerations

ATP 2-01 says requirements are constantly developed, consolidated, and refined throughout the planning process. Maximum efficiency in information collection is achieved when all the collection tasks are carefully synchronized with an appropriate mix of collection assets to satisfy as many distinct requirements as possible.[8] OSINT can answer initial requests for information (RFIs) that shape the mission, commanders' decision making, and time-phasing requirements management. Once multi-domain operations are underway, OSINT supports and informs information requirements and intelligence gaps, providing insights that might not be found on higher classification systems and are sometimes overlooked.

Effective requirements development depends on establishing the intelligence architecture and having effective network connectivity that provides situational understanding and input from the entire staff.[9] Design considerations include an important choice for commanders, specifically whether to—

- Organize an OSINT activity within an all-source team by integrating and embedding OSINT practitioners.
- Organize as a single-intelligence discipline team.
- Train and equip all-source analysts to collect PAI as part of their mission.

The all-source effort is directly supported, and OSINT is integrated into production. Disadvantages to the blended approach include burdening all-source analysts with OSINT training requirements, collection policy compliance, sustainment of technical proficiency, and record keeping. Embedding OSINT practitioners into an all-source team may be more effective but requires borrowed manpower (or contracted labor) and their efforts may get lost as merely a source citation at the end of a classified product.



Staff elements that develop requirements follow a development process that includes subordinate tasks and products.[10]

In the Indo-Pacific Theater, the single-intelligence discipline team design is preferred. Just like other intelligence disciplines, the OSINT activities respond to tasking through priority intelligence requirements, intelligence requirements, RFIs, directed requirements, and emphasis messages. Thinking broadly, production of OSINT reports is the best way to put points on the intelligence community scoreboard for the Army OSINT program. And when properly disseminated, OSINT reports support the "collect once and share broadly" mandate.

In terms of architecture, PAI collection requires seamless network connectivity. The DoD Non-classified Internet Protocol Router Network (NIPRNET), primarily an administrative and logistical network, is now an essential collection platform. Coordination with G-6/S-6 is required to ensure the dedication of sufficient connectivity, system flexibility, and bandwidth to OSINT activity.

Techniques for OSINT Collection Planning

In our experience, OSINT is an afterthought. When creating indicators and specific information requirements (see Figure 2 on the next page), consider where OSINT can contribute. Done properly, OSINT takes time. Planning and

coordination of emerging requirements provide a sufficient lead time essential to effective OSINT activities. The required risk management procedures and developed best practices require time to plan, prepare, and execute.

To use a human intelligence (HUMINT) analogy, OSINT practitioners must plan and prepare before collection, including the digital equivalent to planning routes and site selection. During collection, OSINT must follow specific procedures using tradecraft and technologies to manage risk. Like HUMINT collectors, they have plenty of production and administrative work to do after a source meeting in order to process, exploit, and disseminate what is collected. For example, OSINT practitioners are required to keep collection logs for audits.

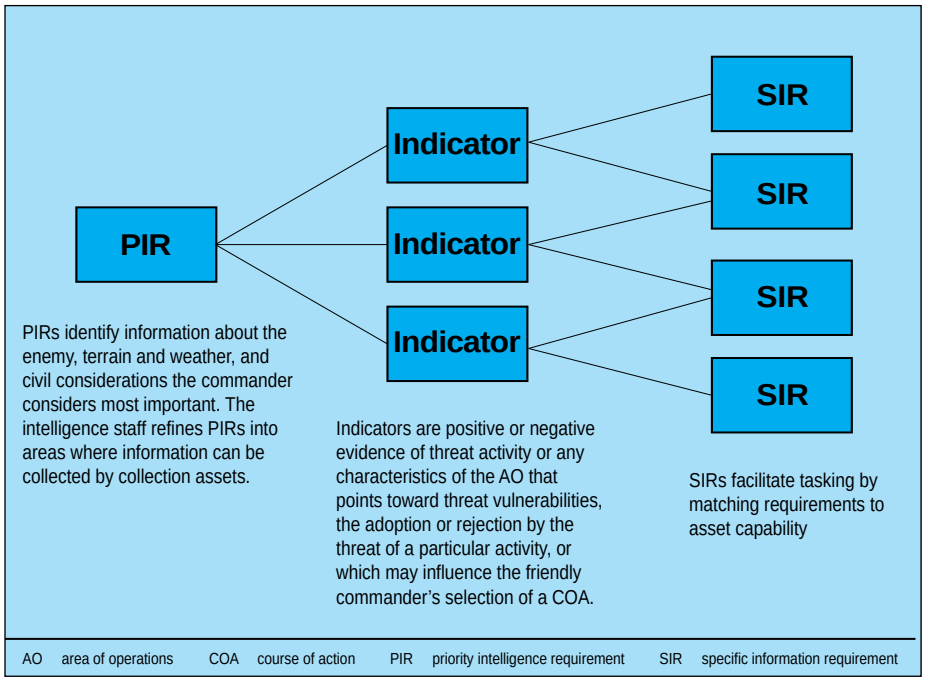


Figure 2. Relationship between Priority Intelligence Requirement, Indicators, and Specific Information Requirements[11]

Proper PAI collection and exploitation involve considering the validity of the source as well as the veracity of the information. Independent PAI sources with the same information give more credibility than a single item from an unverified source or suspicious social media account. In the age of fake news, misinformation and disinformation are ubiquitous. OSINT practitioners are trained to expose potentially false information and recognize fake social media accounts.

Well-prepared OSINT reports include a characterization of the sources and all relevant context about where information was found. This can include any translation capabilities applied to the original content. As everyone should know, machine translation services are imperfect with varying degrees of accuracy, depending on the language, context, and content. Sarcasm, emojis, shortcuts, local slang, and internet lingo add layers of complexity.

OSINT Enterprise Collection Management

Advice to G-2/S-2s and collection managers should include advocacy for the use of two systems of record in unison to achieve optimal OSINT integration and synchronization: the open-source collection acquisition requirement–management system (OSCAR–MS) and the community on-line intelligence system for end-users and managers (COLISEUM).

OSCAR–MS (The Asking System). The intelligence community's system of record for managing open-source requirements is called OSCAR–MS. Consumers input their requirements and request support from OSINT producers who advertise in the National Open Source Enterprise Capabilities Manual; it is not a formal tasking system.

OSCAR–MS lacks a mechanism to enforce an obligation to support. The OSCAR–MS portal resides only on the SECRET Internet Protocol Router Network (SIPRNET) and the Joint Worldwide Intelligence Communications System (the SIPRNET portal is far less popular). The default procedure for many consumers is to tag all the OSINT producers with the same requests (the shotgun approach). Producing organizations can then opt in, partially or completely, to accept the requirement. Generally, Army consumers at tactical and operational echelons lack consistent access to OSCAR–MS. Therefore, awareness of existing requirements, as well as knowing which producer accepted those requirements and where to find existing products, continues to challenge the force. We should all use OSCAR–MS because Army Directive 2016-37 requires it. A new and much improved OSCAR–MS is in development. The developers should consider a tactical to national hierarchy for collection requirements and collection operations, such as those that exist in geospatial intelligence, HUMINT, signals intelligence, and COLISEUM.

COLISEUM (The Tasking System). COLISEUM is a web-based application to provide for online RFI and production requirement registration. Collection managers can use COLISEUM to task OSINT resources, either organic assets or external, through requests for support to answer requirements. However, the requirements must be moved manually to OSCAR–MS at operational and strategic echelons in order to reach all potential producers.

Streamlining the Collection Management Processes for OSINT. The connection between collection requirements management and intelligence operations is fragmented because the two preferred systems do not talk to each other. OSCAR–MS should be updated to restructure and allow organizational validation down to the lowest levels and to streamline the hierarchy of support within theaters, not just at strategic and national levels. A shared data path between the two systems would streamline collection and mitigate collection fratricide.

Conclusion

Strategic competition means increased complexity in all warfighting domains. Hybrid warfare, including information warfare and other ambiguous actions in cyberspace, is the new normal. Therefore, we must make better use of the abundance of PAI to provide persistent information collection across our areas of interest. OSINT should be optimized in a dynamic fashion to increase the production of relevant intelligence while minimizing redundancies. Furthermore, we should harness technologies to decrease OPSEC and cybersecurity risks while increasing PAI collection and PED.

We challenge G-2/S-2s and collection managers to plan, integrate, and synchronize OSINT into all collection requirements and intelligence operations. We recommend echelons at brigade and above integrate OSINT into all plans and orders, so that requirements can be developed to leverage OSINT appropriately. OSINT requires a multifaceted joint, interagency, and multinational approach, coordinated by G-2/S-2s and collection managers at multiple echelons, to maximize the use of domain expertise, language capability, cultural understanding, proximity to the target, and sophistication of OSINT capability. Every OSINT organization in the DoD and intelligence community should collaborate and coordinate to achieve the "collect once and share broadly" objective.

Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-22.9, *Open-Source Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 15 August 2019) (common access card [CAC] login required).

2. National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-163, 119 Stat. 3411 (2006).

3. Department of the Army, ATP 2-22.9, *Open-Source Intelligence*.

4. Department of Defense (DoD), DoD Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities* (Washington, DC: U.S. GPO, August 8, 2016), 14.

5. Department of the Army, Army Directive 2016-37 (U.S. Army Open-Source Intelligence Activities) (Washington, DC, 22 November 2016) (CAC login required).

6. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019), 3-2.

7. "INTelligence: Open Source Intelligence," Central Intelligence Agency website, posted July 23, 2010, last updated August 6, 2018, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

8. Department of the Army, ATP 2-01, *Plan Requirements and Assess Collection* (Washington, DC: U.S. GPO, 19 August 2014), 3-1.

9. Ibid., 3-2.

10. Ibid., 3-3

11. Ibid., 2-3.

References

DoD. DoD Directive 3115.18, *DoD Access to and Use of Publicly Available Information (PAI)*. Washington, DC: U.S. GPO, June 11, 2019.

Department of the Army. ATP 2-33.4, *Intelligence Analysis*. Washington, DC: U.S. GPO, 10 January 2020.

Department of the Army. Field Manual 2-0, *Intelligence*. Washington, DC: U.S. GPO, 6 July 2018.

Department of the Army. *U.S. Army OSINT Handbook*. Fort Belvoir, VA: U.S. Army OSINT Office, 2016.

Office of the Secretary of Defense. *Summary of the 2018 National Defense Strategy of The United States of America*. n.d. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

1LT Moriamo Sulaiman-Ifelodun is the executive officer to the U.S. Army Pacific (USARPAC) G-2, and she has served more than 5 years in the U.S. Indo-Pacific Command area of responsibility. Before commissioning in 2017, she served and deployed with 1st Special Forces Group (Airborne) as an imagery sergeant and collection manager in Operation Inherent Resolve. She holds a bachelor of science degree in toxicology and is working on her master of professional studies in public relations and communications to better promote military intelligence in the information domain and its effect on the battlefield. She has completed Basic Open-Source Intelligence (OSINT) Courses 301 and 302 and is the presumptive candidate to lead the USARPAC OSINT team.

COL Robert Wilkinson (retired) is a contractor with Northrop Grumman, supporting the Army OSINT Office from Fort Shafter, HI. Bob served for 33 years in the U.S. Army Reserve and Army National Guard in a variety of operational and intelligence billets, including multiple deployments and two tours in combat. He holds a bachelor of arts degree in history and a master of arts degree in intelligence studies. Supporting the Army OSINT program since 2014, Bob's OSINT experiences include capability developer at the U.S. Army Intelligence Center of Excellence, OSINT practitioner for USARPAC G-2, and senior trainer for the Army OSINT Office.

New and Different: 2nd Security Force Assistance Brigade's Digital Strategy

by Chief Warrant Officer 3 Nick Rife and Staff Sergeant Joshua Brown

It's no longer the big beating the small, but the fast beating the slow.

— Eric Pearson
Former Chief Commercial and Technology Officer
InterContinental Hotels Group

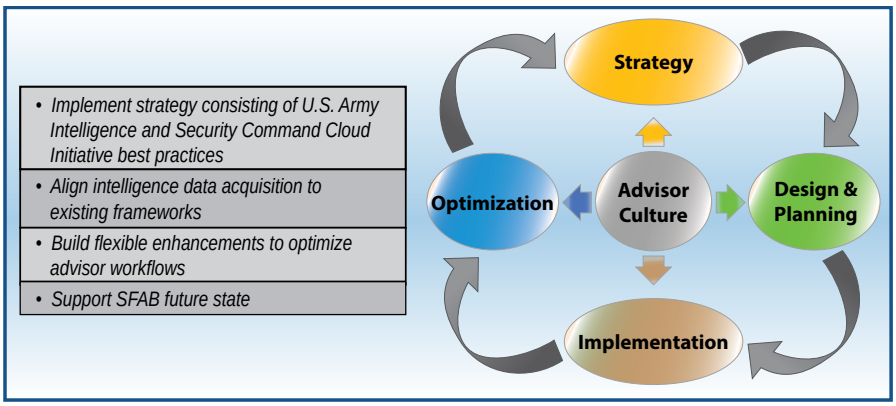
Overview

Digital strategy is a form of strategic management involving the integration and implementation of new technologies to optimize performance. When intelligence professionals consider their future operating environment and organizational capacity, they must ask a few key questions:

- What are the systems, networks, and services needed to connect to where we are going?
- Are the systems accredited and approved for where we are going—do they work and support the mission?
- Do we have enough people knowledgeable on the equipment to maintain and optimize it for the duration to provide intelligence support to mission command?

Deltas exist when modified table of organization and equipment maintenance requirements exceed the S-2's ability to maintain operational capacity. Additional deltas exist when an element's communications transport capacity is so limited that the only recourse for a disadvantaged user is to send a SPOT/SALUTE/RECCEXREP and hope for the best. Closing these deltas and answering the initial key questions is the heart of digital strategy. This is the plight of the intelligence Soldier struggling with digital technology to build the most robust intelligence picture with the fewest mouse clicks. The challenge among tactical Army organizations is creating a digital strategy that integrates commonly understood systems while filling gaps with innovative capabilities that meet the commander's intent.

The security force assistance brigade (SFAB) military intelligence company and brigade S-2 have limited resources, in both personnel and equipment, in comparison to their brigade combat team counterparts. Within the advisor teams, not all intelligence advisors are intelligence Soldiers, and of the ones who are, not all are all-source analysts. The 2nd SFAB provides these Soldiers with a baseline knowledge of intelligence preparation of the battlefield and an effective digital intelligence architecture that minimizes inefficiencies. This results in the ability to overcome gaps in knowledge and experience while maximizing end-user engagement and contributions at a global scale.



2nd SFAB Strategic Approach to Digital Intelligence Activity in Support of Advising

This article discusses the 2nd SFAB's approach to digital strategy in Afghanistan—a strategy scaled in accordance with global persistent or episodic intelligence support to advising. The ambiguity of advisor operations requires intelligence professionals to operate outside of normal comfort zones and maintain digital flexibility as operational conditions evolve. The SFAB established principal tenets through which to effectively apply effort and generate results. They include strategy implementation and refinement, data acquisition alignment, optimization of advisor workflows, and support to the SFABs' future state. Aligning global advising intelligence strategy to those four tenets curbs ambiguity, informs the future, and most importantly, generates results in support of the commander's objectives.

Mission

The Army has many technological capabilities that tactical units are often resistant to utilize due to their configuration-intensive operability. The output generated by legacy systems can be inadequate compared to the time invested, or the systems are cumbersome to maintain. Within the Army intelligence enterprise, "operationalizing" data to drive a commander's decision making is a primary source of user friction as they try to maintain relevance with information collection and analysis.

SFABs are unique in that they must provide multi-echelon intelligence support to develop foreign security force capacity and capability while maximizing interorganizational collaboration. Not only must SFAB intelligence advisors access enterprise information, they must also generate insights from the farthest reaches of the train, advise, and assist (TAA) efforts. Advisors are the SFABs' most valuable sensors with access to partner operational and intelligence information at echelon. Accordingly, SFAB intelligence advisors must develop key competencies, ingesting, enriching, and aggregating information derived from high-threat areas and providing it to the global enterprise.

During its inaugural deployment, 2nd SFAB headquarters, as a mission command element for Train Advise Assist Command-East (TAAC–E), conducted TAA and mission command to enable Afghanistan's security operations against threat groups, including the Taliban, ISIS–K, and the Haqanni Network. The SFAB and subordinate advisor teams established TAA efforts where needed, shaping the information space and supporting development of the Afghan National Defense and Security Forces.

Given 2nd SFAB's mission, brigade intelligence leaders sought to develop a digital strategy inclusive of partners across the Combined Joint Operational Area-Afghanistan (CJOA–A) but adaptable enough to be implemented globally by all SFABs. The digital intelligence environment in Afghanistan is not the same as in Africa. Similarly, the digital capabilities and requirements of Africa are unlike those of the European theater. However, all operational environments share fundamental characteristics, which 2nd SFAB Digital Intelligence Systems Master Gunners identified early on in strategy planning.

The 2nd SFAB's approach requires an understanding of the Army's programmatic and commercial-off-the-shelf digital capabilities. It harnesses best of breed concepts from across the digital technologies, including the Distributed Common Ground System-Army (DCGS–A), Palantir, and Automated Information Discovery Environment (AIDE), without the constraints of system-specific hardware and software. Further, all the SFABs can replicate this approach in Africa, Europe, or the Pacific under existing strategic intelligence support paradigms.

Strategy Implementation and Refinement

To address the challenges associated with enhancing the intelligence reach of an advising brigade, we need to look at digital transformation. Such modernization efforts can polarize staffs and desynchronize the common understanding at echelon. Unique opportunities to integrate emerging capabilities into existing processes commonly go underexploited because those capabilities cause compartmentalized access or generate isolated outputs. Consequently, users rely on unintegrated applications and portals to synthesize data, outsourcing value or extending intelligence fusion timelines beyond the data's value threshold. In both cases, the relevance of the resulting information is jeopardized.

Photo courtesy of SSG Mike Ream

2nd SFAB intelligence personnel at Forward Operating Base Fenty, Afghanistan.

In order to enterprise-enable its data, 2nd SFAB relies on U.S. Army Intelligence and Security Command (INSCOM) mission partners' service-enabled strategy INSCOM Cloud Initiative (ICI). Historically, regionally aligned U.S. Army Forces Command (FORSCOM) intelligence elements have increased their capacity by establishing a relationship with strategic INSCOM organizations with a similar alignment. With support from the FORSCOM G-2, 2nd SFAB and the INSCOM G-37 developed formal points of contact before and during deployment to optimize regional support to forward elements. As a template, this support model is replicable at no cost anywhere else the SFAB will deploy globally.

Major SFAB data products include partner reliability metrics in a purpose-built widget known as Dozer, and three-dimensional photo-mesh renderings processed from a system known as the Aerial Reconnaissance Tactical Edge Mapping and Imagery System (ARTEMIS). (Dozer and ARTEMIS are discussed further in a later section.) The requirement for tracking partner reliability and storing imagery existed before 2nd SFAB's arrival, but a standardized measurement and control mechanisms were lacking. Presenting the data in the browser-based ICI implies integration into a unified interface with the ability to port the ontology to other "like" capabilities. Not only does ICI act as a visualization tool, but it also serves as a low-overhead centralized data brokerage strategy, ensuring a common understanding across digital applications in Afghanistan and worldwide.

Military innovation often occurs from the top down, with a shortened acquisition process resulting in one-size-fits-all programs of record geared toward strategic priorities for pre-established windows of time. Although necessary to the acquisition process, the problem should (and can) define the toolkit rather than the toolkit defining the solution.

Increasingly, the intelligence warfighting function of the future must aggregate outputs from platforms/capabilities outside of program of record supported parameters and integrate them into supported technology frameworks, including for example DCGS–A, ICI, Palantir, and Integrated Tactical Network. This was 2nd SFAB's experience as it explored the current digital domain to drive the common understanding and TAA initiatives, and it represents a new norm for digital integration activities of an SFAB permanently engaged below the threshold of major armed conflict.

Align Intelligence Data Acquisition to Existing Frameworks

As talk of troop reductions and a changing counterterrorism effort permeates the media, opportunities to exploit 2nd SFAB digital strategy "wins" endure past a tactical reset and into the future of security force assistance. Intelligence architectural support is a high-overhead endeavor, which ostensibly will retrograde along with much of the architecture support the theater has enjoyed for nearly two decades. The ability to develop the enemy picture remotely will degrade as intelligence, surveillance, and reconnaissance assets reprioritize to other theaters. When enablers retrograde, the ability to ingest partner information into simplistic object-based production environments must remain. This key assumption and others, including the likelihood that SFABs will be employed in similarly architecture-deprived spaces, guide 2nd SFAB's approach.

Users supporting CJOA–A conduct object-based production with several digital tools. Strategic users might produce in AIDE/Augmented Reality Sandtable (ARES) or DCGS–A, while tactical users might produce in WinTAK or Palantir. Often, the echelon of intelligence support dictates the digital capability with which users conduct analysis. In the past, this simple fact relegated users at each echelon to the common visualization tool their organization had been fielded. Leveraging software as a service (SaaS) fundamentals, Palantir users can ingest data produced in the ICI, and ICI users can interact with objects derived from AIDE/ARES. With enough technical understanding and integration support, SaaS implementation reduces the traditional deltas associated with interoperability.

The approach is similar to the traffic application known as Waze, which has drivers that conduct object-based production as impacts to travel conditions change. With enough users and various other data points adapted to the interface, a robust "multi-intelligence" picture displays—complete with indications and warnings, fuel and resupply points, hazard zones, etc. As advisors either traverse the environment or gain those insights from partners, the same is applicable. The only exception is 2nd SFAB users might interact with the same data in two or three different interfaces.

Build Flexible Enhancements to Optimize Advisor Workflows

In partnership with INSCOM, 2nd SFAB evolved intelligence crowdsourcing techniques by enabling forward tactical intelligence production cycles but displacing enhanced processing and dissemination. This intelligence integration strategy aligns TAAC headquarters with current commercial approaches to data visualization, increasing its value and enabling rapid workflows with commensurate return on operational investment. More importantly, it builds flexibility in a strategically ambiguous environment, should conditions require a rapid shift in posture—matching digital capability to the realities of the operating environment.

One of the SFABs' most critical requirements is tracking the reliability of foreign security force counterparts. Partner reliability metrics exist behind firewalls, passwords, and hard-to-access enclaves. Partner engagement/reliability tools available in CJOA–A were built before the Army established a permanent advisor brigade that exists to deploy and advise at echelon. The expectation is everyone in these brigades will interact daily, in person, with reliable partners. It helps to know who the reliable partners are before arriving in theater. This requires a tool that is globally available and suited for multiple environments or geographic combatant commands, nested into existing technology frameworks.

Optimizing best practices from advisor teams, the 2nd SFAB S-2 and INSCOM developed the partner reliability widget known as Dozer (a play on the word dossier with a *Matrix* namesake, Dozer), which leverages the DCGS–A ontology but is accessible through a widget interface and is optimized with ICI analytics to equate "reliability scores" and develop reliability link diagram graphs. Perhaps the most appealing component to Dozer is the continuity it affords permanently engaged units. The 3rd SFAB now has a user-friendly approach to prepare for deployment from Fort Hood, Texas, with nothing more than a standard SECRET Internet Protocol Router connection. An additional benefit is the access afforded to partner data for wider enterprise use. For example, a Special Forces Operational Detachment Alpha team preparing for a rotation now has user-friendly access to their conventional advisor counterparts. The team also has a nested view of partners within the context of a comprehensive intelligence picture. In the near future, regionally aligned forces moving to U.S. European Command will benefit from the leadership the SFAB has interacted with in the past—all at no unit cost and insignificant training investment.

Additionally, 2nd SFAB discovered value in having all advisor team members input their engagement experiences into a historical intelligence user interface. The logistics advisor, the fires advisor, and the operations advisor all provide engagement information as well. Integrating multifunctional advising information directly into a single information repository correlated with the existing common intelligence picture provides a wealth of knowledge from an intelligence standpoint. In a sensor-deprived environment, Dozer effectively creates a sensor for each warfighting function.

SFABs' organic sensors are not limited to the human domain. ARTEMIS is an organic mechanism for 2nd SFAB to collect timely high-resolution and three-dimensional imagery in support of the commander, advising teams, and partners. It consists of an application workstation and two eBee X small unmanned aircraft system airframes. Furnished by the National Geospatial-Intelligence Agency, the data is processed and disseminated into TAAC–E's common intelligence picture and to the wider enterprise. It goes beyond TAAC–E and encompasses worldwide mission partners and enablers. Matched to the output of a comparable LIDAR (also known as light detection and ranging) sensor, ARTEMIS shortens the tasking, collection, processing, exploitation, and dissemination cycle from 6 days to 6 hours or less depending on data volume.

Advisors use ARTEMIS based on aligning the capabilities and limitations inherent to the platform with TAA priorities and then finding the appropriate mission window to achieve results. In deliberate execution, advisors accomplish airspace de-confliction through a standard concept of operations brief to air traffic control prior to launch, following through with real-time communications during the mission. Advisors accomplish expeditionary de-confliction through line of sight and with team joint tactical air controllers. Each discrete mission profile consists of a route to the target, the target mapping profile, a predetermined hold waypoint, and a landing profile.

In order to disseminate the data to the enterprise, 2nd SFAB retains the capability to process and exploit the data locally but relies on INSCOM to process and service-enable the three-dimensional mesh centrally in the ICI. Such an approach requires the team to be willing to use SaaS techniques. Adding a layer of high fidelity processing, INSCOM further refines the output for mission planning and three-dimensional visualization.

The three-dimensional data published in the ICI as a photo-mesh service provides users the ability to overlay enemy activity, drive mission planning efforts, or assist TAA partner efforts. Specifically, the three-dimensional data was a crucial component to TAA partners following successful security operations in Nangarhar Province. Between July and October 2019, 2nd SFAB captured the entirety of Jalalabad (37 square kilometers) in three-dimensional data using ARTEMIS, which is available in the ICI. The three-dimensional data continues to provide insights into a variety of user groups in and out of Afghanistan.

Support SFABs' Future State

Digital strategies flounder without the ability to maintain digital dexterity as priorities change. Building a theater-centric advisor metrics repository for reliable partners in CJOA–A provides little for advisors who might have to transition to an entirely different theater of operations 9 to 12 months later. Likewise, the applications, portals, and

Photo courtesy of CW3 Nick Rife

A 2nd **Security Force Assistance Brigade S-2 noncommissioned officer launches the eBee X platform at** Forward Operating Base Fenty, Afghanistan.

repositories filled with 18 years of CJOA–A data are increasingly irrelevant beyond Afghan borders. Leveraging INSCOM's service-enabled strategies broadens the SFABs' digital capability at a fraction of the resources. Under the existing strategic support framework that INSCOM manages, SFABs of the future can prepare to support multi-theater advising and scale seamlessly from home station or the operational environment.

In order to build an advising capacity, repetition and flexibility are critical aspects of the SFAB digital "kit." Traditional systems and processes create inherent filters through user access, permissions, and enclaves. All of these inadvertently establish barriers to understanding and continuity. Equally critical is the ability to integrate with existing FORSCOM and strategic architectures as employed in joint exercise lifecycle events and the broader joint simulation environment. The ICI routinely sets the integration precedent in these lifecycle events, creating opportunities for operational depth, should SFABs be introduced as regular training audiences.

The SFABs' future state requires a digital architecture that is engineered and managed to respond to requirements based on operational conditions. By 2026, 2nd SFAB should not still be saying that three-dimensional imagery services are an advancement in intelligence support to security force assistance. Rather, an entirely different set of operational challenges with new and different platform integration needs will emerge. Intelligence leaders will nest those with an ever-flexible strategy, innovating where necessary, to satisfy requirements.

Conclusion

The 2nd SFAB is not unique in its gaps or the ability to innovate strategies to fill those gaps. What is unique is the flexibility developed through SaaS dissemination techniques and the broadening of strategy effectiveness as a result. Analyzing costs and benefits, as well as expansion opportunities, is critical to problem solving in the digital environment. Saying "this is how we've always done it" has no place in the mindset of the 2nd SFAB intelligence warfighting function. Instead, it is time to ask, "What can I do to innovate, automate, and streamline the system?" More than a guide to inform the activity of security force assistance, 2nd SFAB's experience shows how we can improve digital intelligence strategy throughout our global operations.

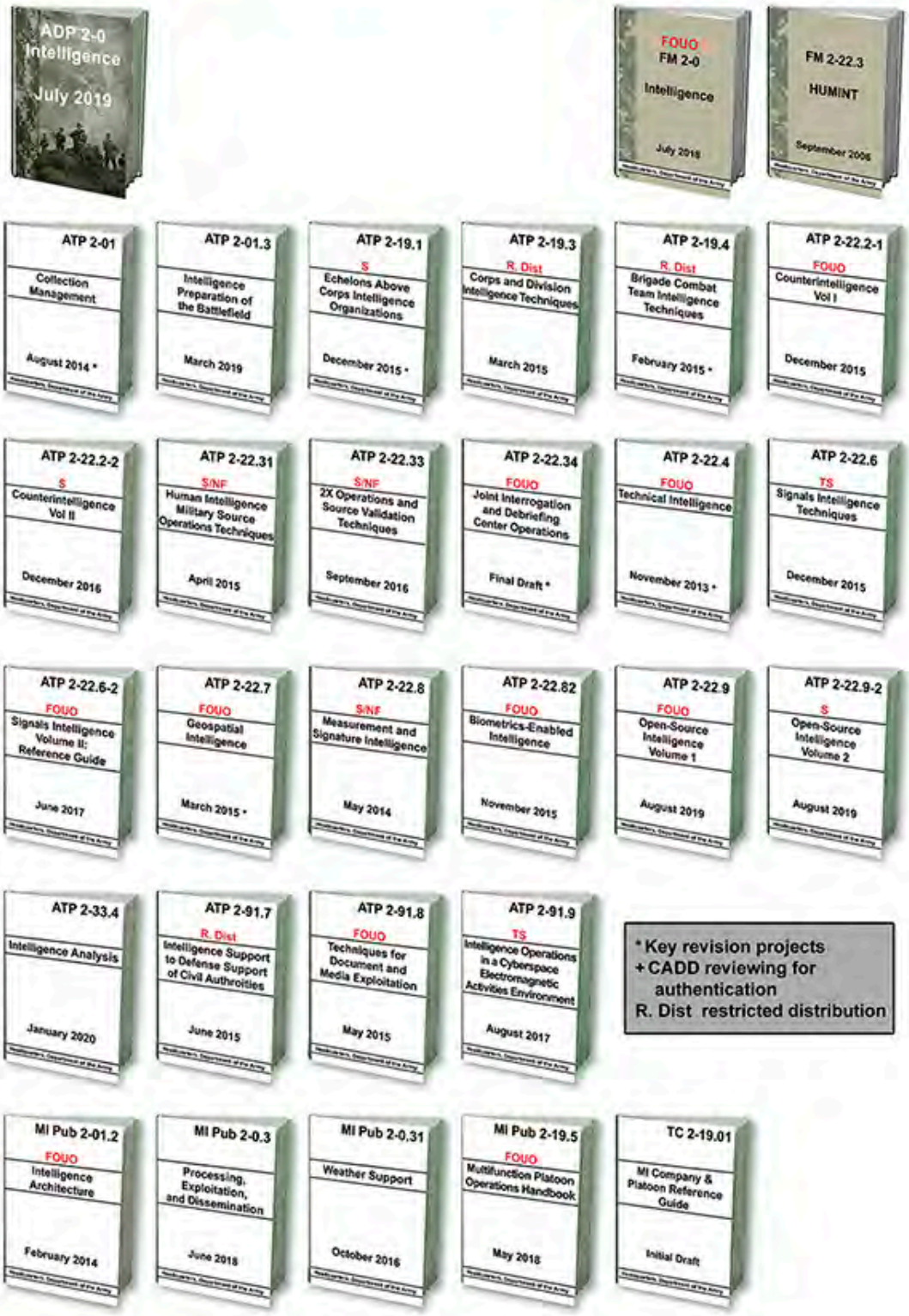
Epigraph

Howard Tiersky, "Navigating Digital Transformation," CIO from IDG Communications, May 25, 2017, https://www.cio.com/article/3198121/whats-now-in-digital-transformation.html. Eric Pearson made this comment at the Digital Transformation Summit. A few times each year, senior digital executives from around the world assemble at the summit to discuss the current state of digital evolution.

CW3 Nick Rife serves as the senior all-source intelligence technician for 2nd Security Force Assistance Brigade, headquartered at Fort Bragg, NC. He previously served at U.S. Army Forces Command G-2 as the principal developer of the Digital Intelligence Systems Master Gunner Course; and fusion chief at 82nd Airborne Division G-2 and 4th Brigade Combat Team, 82nd Airborne Division. His campaign support includes Operation Iraqi Freedom, Operation Inherent Resolve, and Operation Freedom's Sentinel.

SSG Joshua Brown serves as the senior signals intelligence sergeant and technical integrator at 2nd Security Force Assistance Brigade, headquartered at Fort Bragg, NC. His military education includes the Basic Operator Training Course, the Digital Network Exploitation Advanced Course, and the Security Force Advisor Course. He served as a flight trainer at Alpha Company, 3rd Military Intelligence Battalion (MI BN) (Aerial Exploitation) and as the Task Force Observe, Detect, Identify, and Neutralize (ODIN) liaison to the General Command of Police Special Units. He also served as the Headquarters and Headquarters Company platoon sergeant and operations noncommissioned officer at the 743rd MI BN. SSG Brown's campaign support includes Operation Freedom's Sentinel.

Are You Doctrinally Proficient?



* Key revision projects
+ CADD reviewing for authentication
R. Dist restricted distribution

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.icoe.mbx.doctrine@mail.mil

The Directorate of Training analyzes, designs, and develops intelligence training materials, unit mission essential tasks, and training programs that contribute directly to the combat readiness of military intelligence Soldiers, leaders, and their units.

by Ms. Beth Leeder

Training and education at the U.S. Army Intelligence Center of Excellence (USAICoE) have changed and will continue to change as a result of the coronavirus disease of 2019 (COVID-19) pandemic. Similar to the efforts of public schools and colleges to continue educating children during the pandemic, USAICoE has been working through the challenges of how to continue training and educating your Soldiers. But unlike most in public education, the Army was looking to change its training and education model before the pandemic hit. GEN Paul Funk, Commanding General of the U.S. Army Training and Doctrine Command, recently put it into perspective: "The long-term vision has always been to take the training to the soldiers, not the soldiers to the training, and this virus has actually caused us to focus on that long-term vision in a clear and present manner."[1] We, as a learning community, have a unique opportunity in this moment to invent the future learning ecosystem we want to have by creating new training models using all forms of learning available.

This edition of ***Training Readiness*** focuses on the changes coming to institutional training because of the COVID-19 pandemic and their potential long-term impacts. We will—

- Look at the difference between dL and DL (who knew the capitalization of a letter could make such as difference).
- Discuss near-term virtual learning models for the Military Intelligence Captains Career Course (MICCC) and the Senior Leader Course (SLC).
- Identify specific actions you can take to ensure your students are ready to succeed.
- Ponder a bit the effects all this might have on training moving forward.

What Are dL and DL?

Distance learning (dL) is the technology-enabled learning model with which most of us are familiar. It primarily uses the Army Learning Management System to provide access to an individual, isolated experience of the course materials, and there is no interaction with an instructor or other students. This model is asynchronous, which means students access the materials at different times and the only expectation is that the student will complete the training within a broadly set timeline such as "during the fiscal year." An example of dL is our annual cyber awareness training.

Distributed Learning (DL) is a full-time effort that requires a student to interact with an instructor and fellow students through multiple technologies. The virtual classroom is the place of duty for the entire period of instruction. DL uses tools like Microsoft Teams and Blackboard to foster critical thought, engagement, and discussion between students and instructors. During DL, the student interacts with both an instructor and other students. DL can be a blend of synchronous learning, which means all students log into the class at the same prearranged time, and asynchronous learning.

Near-Term Training Models

USAICoE is piloting two different training models, using both DL and dL to create a virtual classroom for students: one in the MICCC and one in SLC. The MICCC model uses both DL and resident training. Students complete a 5-week home station DL followed by temporary duty to Fort Huachuca, Arizona. After a student's arrival, USAICoE will quarantine students for 2 weeks (students will complete additional DL) followed by a face-to-face resident class for 14 weeks. SLC is taking the MICCC model one step further by

attempting to deliver the entirety of the course through DL. Currently scheduled for August 2020, the SLC pilot will use both Microsoft Teams and Blackboard.

So what might a DL course look like for the students? Let's consider an example from SLC. The current planning has students complete a Blackboard module for the 17 non-commissioned officer common core competencies (NCO C3s) using an asynchronous dL approach with an SLC instructor an email away for questions. Then, in order to reinforce key competencies of the NCO C3s, students will use synchronous DL to collaborate in the Microsoft Teams environment to figure out how to solve a situation in which a key member of their section fails the Army Physical Fitness Test (Army Combat Fitness Test) while the unit is preparing to deploy. This short example shows how USAICoE will use both dL and DL to create virtual classrooms.

Ensuring Success

There are two things you can do to support your students and ensure their success in these new models. The first and most important is…let them be students! I'm going to foot stomp this one. Your students cannot participate in DL and keep their day job. Remember, the virtual classroom is their place of duty. The content delivered through these new models is not less rigorous than traditional models nor is it less demanding. In fact, DL puts more responsibility on the student to manage time, complete assignments, and participate. Consider providing a workspace outside the normal area to minimize distractions, or let your students work from home. Second, ensure your future students have established their Microsoft Teams account before they enroll in a DL course. This will ensure they are ready to go on day one.

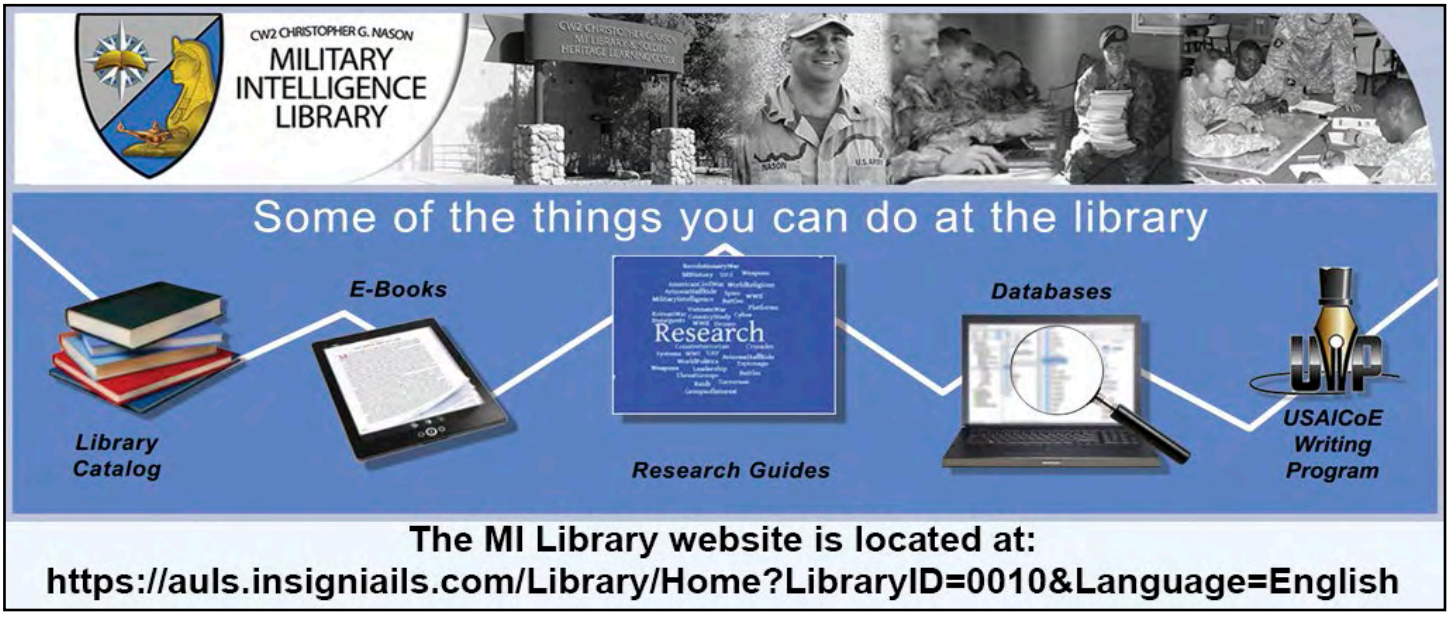
What Does the Future Hold?

Looking forward, we really have to consider both the COVID term and the post-COVID term. With the uncertainty surrounding potential outbreaks this fall or winter, we will keep the DL models viable and use them as needed to "catch up" on student load missed during the stop movement order and in the event of additional stop movement orders. Multiple efforts are underway through the Army University (ArmyU) and Combined Arms Center to figure out what this learning ecosystem looks like moving forward, including an effort to nest the Army Training Strategy, the Army Learning Strategy, and the Army People Strategy into a coherent concept currently called Army Learning Ecosystem 2035. Additionally, ArmyU is leading efforts to incorporate mission command capabilities through the virtual Command Post Computing Environment, which when fielded will enable professional military education students to work together on in-depth simulations.

One thing is for certain, training in January 2021 will not look the same as it did in January 2020. The Army will be using more dL, DL, and virtual classrooms to train and educate our military intelligence professionals. USAICoE will continue to advocate for the best learning experiences for our students, and we will use this department to keep you updated on our efforts. Till then, Always Out Front!

Endnote

1. Matthew Cox, "Army Eyes Permanent Shift to Distance Learning for Some PME Courses," *Military.com*, 22 April 2020, https://www.military.com/daily-news/2020/04/22/army-eyes-permanent-shift-distance-learning-some-pme-courses.html.



Collection Management: Five-Minute University Version

by Mr. Chet Brown, Chief, Lessons Learned Branch

Normally, the greatest challenge for commanders is to focus the intelligence effort, and to gain dissemination of intelligence to the right place in time for key decisions.

—*FM 34-2,* Collection Management and Synchronization Planning *(1994)*

Introduction

The response to the coronavirus disease of 2019 has me teleworking from my kitchen table, divorced from the references at arm's length in my cubicle. I apply the concept from *Saturday Night Live* comedian Don Novello's "Five-Minute University" skit of teaching only "what the average college graduate remembers 5 years after he or she is out of school."[1] I mimic his approach to offer the most pertinent collection management lessons and best practices.

1. Answer the Question. The Five-Minute University version of collection management is simple: "Determine what the commander needs to know about the threat/enemy, terrain, or weather to make a decision, and then provide the answers." More simply, answer the priority intelligence requirement (PIR). Deceptively simple concept in description, aggravatingly complex in execution. The difficulty is in planning, preparing, executing, and assessing collection while integrated and synchronized with operations. Collection management requires the full-time involvement of a trained and competent professional.

2. It's a Full-Time Job. A best practice is to place an Information Collection Planner Course (ICPC) graduate in the brigade combat team (BCT) collection manager position. ICPC instructs the fundamentals of military intelligence (MI) system collection capabilities, large-scale combat operations, and the application of collection management principles in practical exercises and presentations. Multiple units we observed in operations and training have lauded the performance of ICPC graduates serving as BCT collection managers. We see a positive trend in units selecting knowledgeable, skilled, and experienced personnel as the BCT collection manager. This reverses the trend of assigning the most recent MI lieutenant arrival to the BCT or MI company as the collection manager.

3. Know Your Unit. The collection manager must understand all of the unit's capabilities available to employ for answering the PIR. Which elements provide reliable and accurate reports? Which are prone to perform "drive-by" reporting? The collection manager should become familiar with the performance characteristics of organic elements when developing collection tasks. Will a Soldier operating from a vehicle in defilade be able to detect the enemy activity in the assigned named area of interest (NAI)? How will intervisibility lines and thermal crossover times affect differing systems? How does light data affect aerial reconnaissance? What is the impact of weather, vegetation, and terrain on Soldier performance or enemy signatures?

4. Intelligence Collection Management is a Continuous Activity. The introduction of ATP 2-01, *Plan Requirements and Assess Collection,* confirms that "although the discussions and descriptions in this manual may seem linear, planning requirements and assessing *collection is a dynamic, continuous, and interactive process requiring constant interaction between the commander and staff."*[2] Management is a noun, not a result. This also supports multiple units' recommendations not to assign the MI company commander as the BCT collection manager. The MI company commander and BCT collection manager duties are critical to the BCT's success—both require constant engagement and problem solving to ensure PIR satisfaction.

5. It's the S-3's Plan, but We Own It. FM 3-55, *Information Collection*, confirms operations owns information collection, yet intelligence takes ownership of the process. The collection manager must ensure the unit's collection plan is

postured and performing to answer the PIR before the latest time information is [no longer] of value (LTIOV) to the commander's decision making. The decision point graphically depicts the point in (the battle) space at which the U.S. commander can decide to employ a tactic or an effect before losing the opportunity. The graphic convergence of the U.S. commander's decision point, supported by a PIR, ***must*** be supported by an NAI depicted on the event template. Collection managers use the event template to track PIR satisfaction and forecast collection plan adjustments.

6. Intelligence Synchronization. Synchronizing intelligence activity with operations enables the intelligence warfighting function to be in the right places at the right times to fulfill the collection tasks assigned by the S-3. MI company collectors often arrive at a tasked grid location only to be told to go away or suffer fratricide because they failed to coordinate with the unit in whose areas they were operating. Coordination facilitates proper asset placement, reduces the potential for fratricide, and increases the probability of success. A best practice for both the collection manager and the MI company commander is to participate in the combined arms rehearsal to ensure tasked collectors are integrated into the scheme of maneuver.

For Want of a Nail[3]

For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the message was lost.
For want of a message the battle was lost.
For want of a battle the kingdom was lost.
And all for the want of a horseshoe nail.

7. "For Want of a Nail…" An MI company platoon shipped its mounted collection system to the National Training Center by rail, packing system peripherals and other gear in a Conex sent separately. The Soldiers had barely enough time to access the Conex, configure the system, move to the training area, and begin operating as ordered. It was then that a Soldier discovered a critical cable was missing. It was left at home station. The team leader, platoon leader, and MI company commander failed to perform a pre-combat check/pre-combat inspection before transport or upon arrival. The missing cable rendered the system incapable of detecting opposing force (OPFOR) activity linked to a PIR, resulting in the commander missing a decision point, leading to OPFOR success. It is not the collection manager's job to perform a pre-combat check/pre-combat inspection for every system; however, the collection manager can influence training and track the operating status of each collection system.

8. Collection Resource Status. The information collection synchronization matrix (ICSM) of many units we observe is a color-coded spreadsheet depicting who is doing what and when. Recent observations reveal unit standard operating procedures directing detailed status reporting, which includes—

- Personnel (number, crew rest, trained, suitable, etc.).
- Sensor functions and consumables (communications, nitrogen, batteries, fuel).
- Prime mover status (including consumables, communications, maintenance, etc.).

Deficiencies in one element could render the collection system useless, slightly impair operations, or have no effect on the current mission. An MI company best practice is to post—and push—collection asset operational status to maintenance personnel and BCT S-2/collection manager for situational awareness. Combining the MI company status report with maneuver element combat effectiveness (and reporting) allows the BCT collection manager to revise the collection scheme to answer the PIR in the dynamic and fast pace of large-scale ground combat operations.

9. Collection PACE Plan. Establishing a feasible primary, alternate, contingency, and emergency (PACE) plan for intelligence reporting is a best practice. Multiple examples exist of combat training center rotational training units detecting critical enemy information but failing to receive the information at the decisive point (time or location). The collection manager should understand how information moves from the point at which the sensor detects the expected phenomenology and processes and transmits the information to the commander before the LTIOV—through each element of the PACE plan. The ICPC cadre instructs that a critical PACE factor is evaluating the available network capacity (bandwidth) at the points in the operation when a report/product that answers the PIR is expected. Capacity or communication modes may only support a text message (particularly when command posts displace) when the commander expects an image. This is another reason for the collection manager and MI company commander to attend the combined arms rehearsal—to identify impediments to answering the PIR.

10. Clarity. We often observe elements operating in the open within meters of natural concealment. Invariably leaders state they are operating from the tasked location without understanding they should establish positions to increase performance, cover, or concealment. A six-digit

grid provides 100 meters of adjustment. Conversely, collection managers need to clarify what units are tasked to observe and report. For example, a polygon NAI containing a road intersection, several multistory buildings, a drainage culvert, and a hilltop resulted in a platoon leader telling the BCT S-2 and collection manager, "I need to know what you expect me to look at, observe, and report so I can prepare the squads for the mission." The S-2 responded by listing each NAI (in a spreadsheet) by number and including a grid location and a description of the specific feature (road intersection, building, bridge, terrain feature, etc.). The collection manager used the NAI spreadsheet to produce clear collection tasks and reporting requirements.

> What is a master but a master student? And if that's true, then there's a responsibility on you to keep getting better and to explore avenues of your profession.
>
> —Neil Peart, Rush Drummer, 1952–2020[4]

Conclusion

Collection management requires continuous self-development. ICPC and the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance are frequently cited as best practices. Read doctrine: Army and MI. Engage with your peers; the authors of collection management articles in this quarter's issue of *Military Intelligence Professional Bulletin* are great starting points. Share your collection management lessons with our profession; iron sharpens iron. In the words of Dennis Miller, a *Saturday Night Live* alumnus, "Of course, that's just my opinion. I could be wrong."

Epigraph

Department of the Army, Field Manual 34-2, *Collection Management and Synchronization Planning* (Washington, DC: U.S. Government Publishing Office [GPO], 8 March 1994 [obsolete]).

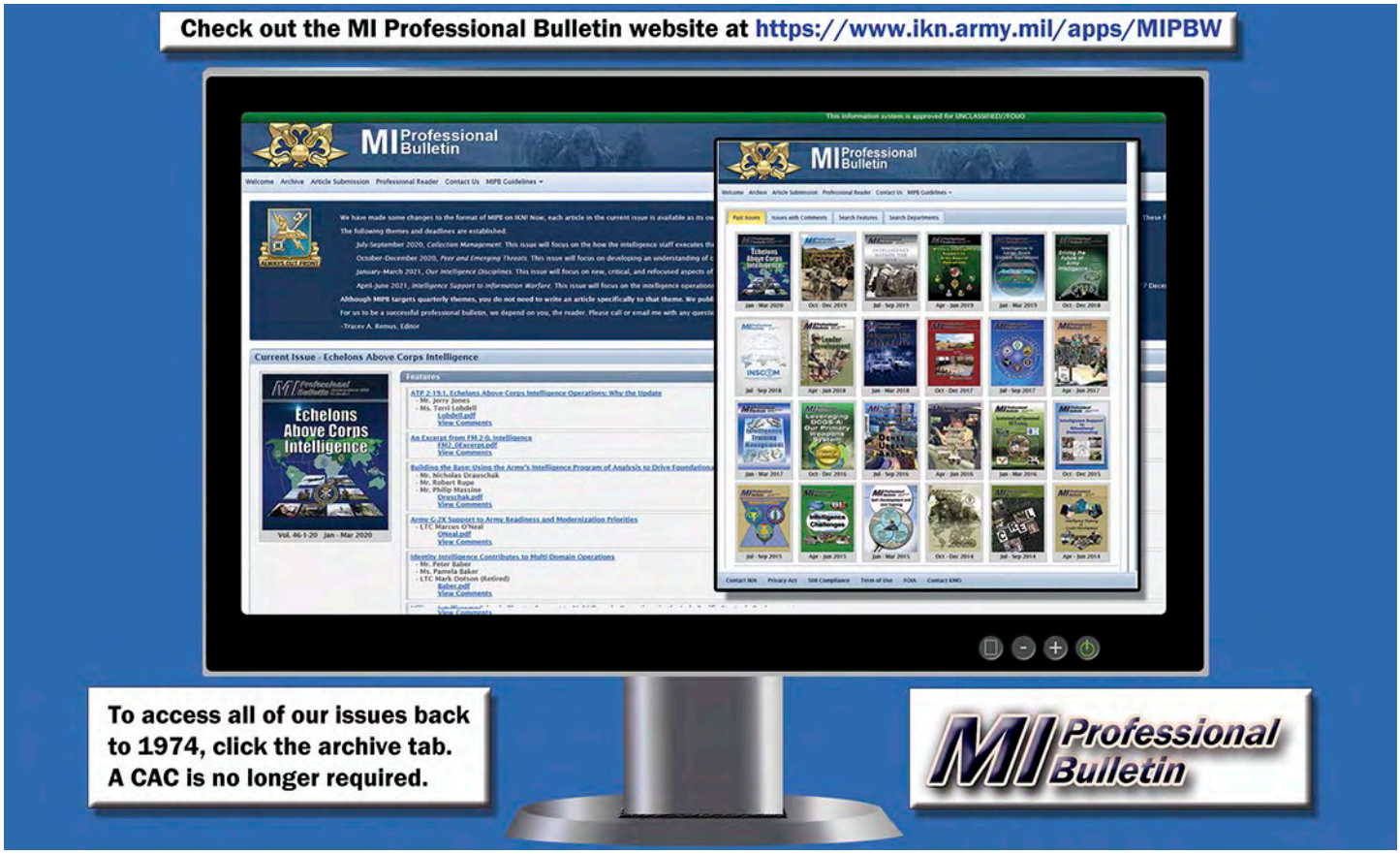
Endnotes

1. Don Novello, "Father Guido Sarducci's Five Minute University," YouTube video, 3:55, https://www.youtube.com/watch?v=kO8x8eoU3L4.

2. Department of the Army, Army Techniques Publication 2-01, *Plan Requirements and Assess Collection* (Washington, DC: U.S. GPO, 19 August 2014), v (emphasis added).

3. Wikipedia, s.v. "For Want of a Nail," last modified on 3 June 2020, 12:49, https://en.wikipedia.org/wiki/For_Want_of_a_Nail.

4. "Neil Peart," Rush website, accessed 18 May 2020, https://www.rush.com/band/neil-peart/.



Revival of the Attaché Intelligence Operations Technician Military Occupational Specialty

by Chief Warrant Officer 4 Nathan Dowling and Chief Warrant Officer 3 Erica Hunt

Introduction

The military intelligence community identified the need for a specialized warrant officer to be the conduit for operations forward and to support joint efforts in various international activities and objectives. This resulted in the creation of the military occupational specialty (MOS) 351Z (Attaché Intelligence Operations Technician). Members of this relatively small MOS make important contributions to the Department of Defense (DoD), Department of State, and other interagency organizations. The 351Z operates within the Defense Attaché System, an arm of the Defense Intelligence Agency (DIA) that represents the United States in defense- and military-related matters with foreign governments around the world. Defense attaché offices operate at U.S. embassies and are composed of both civilian and military employees.[1]

The Vital Role in Supporting U.S. Interests

The history of the defense attachés, including their technical functions and contributions, was recorded through various events that date back before the formal establishment of the MOS in 1948. During the Vietnam War, intelligence reports focused on Vietnam and the regional political-military climate inaccessible at the tactical/operational level. The 351Zs conducted predictive analysis of possible attacks by the Viet Cong, succession plans, Russian and Chinese influence, and political-military positions of neighboring countries Laos, Thailand, and Cambodia. These intelligence reports were invaluable, assisting the U.S. government with decisions about whether to deploy military forces to Vietnam and, if so, exactly where to send those forces. When the United States embassy was evacuated in 1975, 351Zs provided atmospherics through Vietnamese human intelligence sources managed remotely from neighboring countries.[2] This added another layer of difficulty in an already extremely restricted operational environment.[3]

The 351Z warrant officers are currently stationed at various locations at home and abroad; however, Attaché Intelligence Operations Technician accessions for this MOS ceased on 13 December 2011. The last two 351Z warrant officers graduated on 29 August 2012 and the total Army inventory of 351Zs reduced to 33.

Photo courtesy of the U.S. Embassy London

The U.S. Embassy in London is the largest American embassy in Western Europe, and it is the diplomatic mission of the United States in the United Kingdom. This new embassy, opened to the public in December 2017, resembles a crystalline cube.

Revival of the 351Z MOS

In 2018, LTG Robert P. Ashley, Jr., Director of DIA, recognized the contributions of 351Z warrant officers and launched efforts to end the debate over the utility of the MOS. He successfully advocated for the commencement of accessions in 2019, and currently 56 positions are authorized.

On 5 December 2019, the U.S. Army Warrant Officer Career College Class 20-002 (Scarecrows) graduated 92 new warrant officers, of which four were the newly designated presumptive Attaché Intelligence Operations Technicians. For the first time in 7 years, four Soldiers walked across the graduation stage and pinned on warrant officer 1 as 351Zs. These newly minted warrant officer 1s graduated with distinction. One was the distinguished honor graduate and the remaining three made the commandant's list. They marked the resurgence of the 351Z and will pave the way for the future support of multi-domain operations.

Photo courtesy of CW4 Nathan Dowling

On 5 December 2019, newly appointed 351Z warrant officers are celebrated at Fort Rucker, AL.

Attaché Intelligence Operations Technicians work in U.S. embassies around the globe, supporting joint operations and providing administrative support to defense attaché offices. While an obscure specialty, these technicians are a valued capability for the Army, DoD, and Department of State. They are unique because of their work in restrictive, nonrestrictive, and unconventional areas of operations. Currently, the 351Z MOS is sourced from all Services. Noncommissioned officers must possess a minimum of 3 years of experience working as an operations noncommissioned officer in a defense attaché office before applying for accession as a 351Z.

The Defense Attaché System

There are many ways to serve the nation, but one way most are unfamiliar with is the Defense Attaché Service (DAS)… DAS provides opportunities for…service members to serve in diplomatic assignments at U.S. embassies located worldwide…While working in a defense attaché office, these service members represent DoD to the host-nation government and military, assist and advise the U.S. ambassador on military matters, and coordinate other political-military actions within their area of responsibility. They serve as part of the embassy staff and contribute significantly to the U.S. diplomatic mission abroad…The defense attaché office [DAO] plays a vital role in supporting the U.S. interests. During a time of crisis or military contingency, the DAO is often at the center of the action.[4]

The Attaché Intelligence Operations Technicians serve as the Army's experts in interagency operations, often enabling DoD activities in foreign countries, advocating both DoD and U.S. foreign policy objectives, and advising DoD personnel on interagency processes. Their management responsibilities, with regard to strategic reporting and liaison roles, are to provide direct and indirect support to Army leaders and the force.

Conclusion

The current international security environment requires the Army and DoD to have an expeditionary and ready force. As such, we must capitalize on all human dimensions and capabilities in order to reach operational and strategic goals. It is imperative for commanders and leaders at all levels to know about the resources available to them. It is our hope that leaders will use the 351Z warrant officers as a valuable and unique force multiplier.

Endnotes

1. Wikipedia, s.v. "Defense Attaché System," last modified 3 April 2020, 05:56, https://en.wikipedia.org/wiki/Defense_Attach%C3%A9_System.

2. Y. Hunt, "Attaché Technicians in Vietnam" (unpublished paper, 26 November 2019).

3. "U.S. Relations with Vietnam," U.S. Department of State, January 21, 2020, https://www.state.gov/u-s-relations-with-vietnam/.

4. Scott H. Stalker and Joe DiMaggio, "Defense Attaché Service Offers Worldwide Job Opportunities for Elite Service Members," Defense Intelligence Agency, May 18, 2017, https://www.dia.mil/News/Articles/Article/1186808/defense-attach-service-offers-worldwide-job-opportunities-for-elite-service-mem/.

References

"Vietnam War U.S. Military Fatal Casualty Statistics," National Archives, last reviewed April 30, 2019, https://www.archives.gov/research/military/vietnam-war/casualty-statistics.

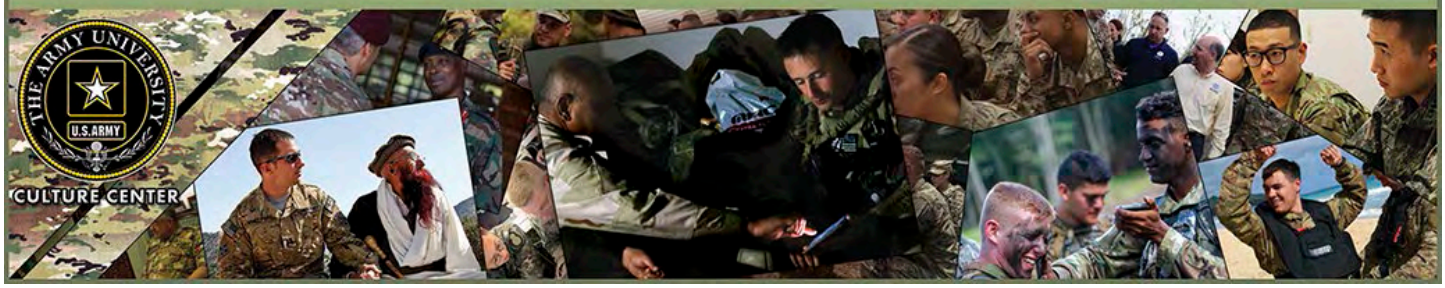
Y. Hunt, "Attaché Technicians in WWII" (unpublished paper, 26 November 2019).

CW4 Nathan Dowling is an Attaché Intelligence Operations Technician assigned to the U.S. Army Warrant Officer Career College where he teaches International Strategic Studies.

CW3 Erica Hunt is an Attaché Intelligence Operations Technician currently assigned to the U.S. Embassy Rome.

Why Culture Matters: Lessons from History

Culture Corner



by TCC Training Specialist/Developer Keith B.

***Editor's Note: This column is a follow-on to the Culture Corner column published in the April–June 2020 issue of* Military Intelligence Professional Bulletin.**

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.
—Sun Tzu

Introduction

The United States has often favored a decisive military engagement in which a strategic or operational victory destroys our enemy or renders it combat ineffective. Some of our decisive military engagements have eliminated threats and helped build and protect our country, people, and interests. However, in any operational environment, a military engagement or series of decisive engagements may not always be the best path to achieving our long-term goals. Military operations should be built on an in-depth understanding of the cultural, social, economic, and political realities of the environment. The beliefs, perceptions, lifestyles, and economic foundations of the society influence the operational environment and will affect planning and execution. Further, it is important to monitor the perceptions and reactions of the population, as these factors affect current and future operations.

Cultural awareness is an essential component of the Army's four strategic roles to shape operational environments, prevent conflict, conduct large-scale ground combat operations, and consolidate gains. It can also play a role in self-awareness, giving us a better assessment of our own strengths and areas for improvement. It can help us anticipate allied and enemy actions on the battlefield, as well as second- and third-order effects that allow us to better determine, plan for, and execute the next operation and help shape overall strategy. Moreover, applying cultural awareness can help commanders and their staffs to achieve greater situational awareness.

This article discusses some valuable cultural and situational awareness lessons from World Wars I and II.

- Russia/Soviet Union and Germany in World Wars I and II (need for accurate assessments of allies and adversaries).
- Pacific theater in World War II (tactical-level application).
- Post-World War II Japan (application of cultural awareness).

World War I—Russia and Germany

The March Revolution of 1917 resulted in the overthrow of Czar Nicholas II and the end of centuries of czarist rule in Russia. The Allied Powers (France, England, and United States) assumed that the new "democratic" Russia would become a more effective ally in the war against the Central Powers (Germany, Austria-Hungary, the Ottoman Empire, and Bulgaria).[1] However, Vladimir Lenin and the Bolsheviks took control of the government, and in March 1918 signed the Treaty of Brest-Litovsk, a peace treaty with Germany, taking Russia out of the war and conceding vast lands in Eastern Europe to the Germans. The treaty also freed up approximately one million German troops who could turn west and focus their efforts on fighting a one-front war against the Allied Powers. This had been facilitated in no small part by the Germans, who transported the revolutionary leader Lenin from exile in Switzerland back home to Russia in the hopes he could eventually remove Russia from the war against Germany. The Germans' analysis of the situation and their cultural awareness—which included their knowledge of revolutionary Russia's cultural landscape—proved accurate and effective.

The Treaty of Brest-Litovsk

In March 1917, demonstrations in Russia culminated in the abdication of Czar Nicholas II and the appointment of a weak provisional government that shared power with the Petrograd Soviet socialists. This arrangement led to confusion and chaos both at the front and at home, with the Russian army becoming increasingly ineffective. Discontent and the weaknesses of the provisional government led to a rise in the popularity of the Bolshevik Party led by Vladimir Lenin, which demanded an immediate end to the war. The Bolsheviks came to power and signed the Treaty of Brest-Litovsk in March 1918. The treaty was effectively terminated in November 1918 when Germany surrendered to the Allies.[2]

This historical example demonstrates the need to have an accurate assessment of one's allies and adversaries. In this case, the Allied Powers were not culturally aware of the severe impact the revolution had had on the Russian people and their renewed priorities. Although Lenin had openly stated he would withdraw Russia from the war, the Allied Powers did not anticipate the success and staying power of the Bolsheviks, which was not the most widely supported party in the tumultuous period after the March Revolution. In addition to needing a better situational awareness, a greater cultural understanding would have aided the Allied Powers in anticipating the Bolshevik success and withdrawal of Russia, a major ally, from the war. Cultural awareness would have included knowing the average Russian's needs, hopes, fears, anger, and mistrust of anybody and anything evocative of traditional authority figures (i.e., anything reminiscent of the czarist era). The Allied Powers would also have benefited from an accurate assessment of the competing elements' motivation and resolve, for example, Germany's grasp of Russia's renewed (revolutionary) mindset and Germany's intent to capitalize on it.

World War II—Nazi Germany and the Soviet Union

World War I ended in 1918. A mere 21 years later, cultural awareness would have once again helped the Allied Powers to foresee events in Russia, by then part of the Soviet Union. Nazi Germany and the Soviet Union were openly intense enemies because of their political and ethnic ideology, history, and national ambitions. However, Germany and the Soviet Union shocked much of the world when they signed the Molotov-Ribbentrop Pact in August 1939, which declared a state of nonaggression between the two countries and a promise not to aid an enemy of the other. Some observers—those who understood the contemporary circumstances and Russian culture—were not surprised. They knew that Russia desired a physical buffer zone between its vast western plains and Western Europe. Russia based this desire on its geographical awareness and a legacy of invasions by the English, French, and Germans. Astute observers also understood that England's and France's unwillingness to include the Soviet Union in the Munich talks was significant. The talks, which resulted in the Munich Agreement, allowed Hitler to take over the Sudetenland in Czechoslovakia. To the Soviet government, not being included in the talks was an indication of the capitalist powers' mistrust of communist Russia. To the Russian people, who culturally placed a great value on strong, unwavering leadership, the Munich Agreement also represented the weakness of the English and French governments in dealing with Hitler.

The Munich Agreement (Annexation of the Sudetenland)

By May 1938, Hitler and his generals were planning to occupy Czechoslovakia. The Czechoslovaks were relying on military assistance from France, with which they had an alliance. The Soviet Union also had a treaty with Czechoslovakia, and it indicated willingness to cooperate with France and Great Britain if they decided to come to Czechoslovakia's defense; however, the Soviet Union was ignored throughout the crisis. The Munich Agreement, signed in September 1938, was a settlement reached by Germany, Great Britain, France, and Italy that permitted German annexation of the Sudetenland, in western Czechoslovakia.[3]

The Molotov-Ribbentrop Pact

In August 1939, enemies Nazi Germany and the Soviet Union signed the Molotov-Ribbentrop Pact, in which the two countries agreed to take no military action against each other for the next 10 years. With Europe on the brink of another major war, Soviet leader Joseph Stalin viewed the pact as a way to keep his nation on peaceful terms with Germany, while giving him time to build up the Soviet military. Adolf Hitler used the pact to make sure Germany was able to invade Poland unopposed. Germany unilaterally terminated the pact in June 1941 when it launched Operation Barbarossa.[4]

The Molotov-Ribbentrop Pact was instrumental to the start of World War II, which began with Germany's invasion of Poland from the west and, a few weeks later, the Soviet Union's invasion of Poland from the east. With the pact in place, Germany could turn its full attentions to invading Western Europe, and the Soviet Union was free to dominate the Baltic States and invade Finland. For those among the Allied Powers who did not have a cultural and situational awareness, this nonaggression pact left them again unprepared for the consequences of losing a potential ally.

Then, in June 1941, the situation changed. Ignoring the terms of the Molotov-Ribbentrop Pact, Hitler launched the massive Operation Barbarossa against the Soviets with the goal of conquering the western Soviet Union for a variety of

ideological reasons.[5] Stalin had ignored repeated warnings that Germany was likely to invade and ordered no full-scale mobilization of forces even though the mobilization was ongoing.[6] Although Hitler had anticipated a quick victory within a few months, Operation Barbarossa was seriously flawed and resulted in Germany having to fight a prolonged two-front war.

This historical example demonstrates the need to have an accurate assessment of one's allies and adversaries. Even though Stalin was aware of Hitler's erratic personality and ambitious plans, he still entered into the nonaggression pact to secure a breathing space of immunity from German attack. "Red flag" indicators were there from the beginning, including the Nazis' anti-Slavic racism, the Nazis' potential interest in the Soviets' rich oil resources, and Hitler's well-known desire to obtain *lebensraum,* or "living space," for the Germans at the expense of the Slavic people.[7]

World War II—Pacific Theater

When fighting began in the Pacific theater during World War II, most Americans did not know about a strong Japanese military ethos—that surrendering was akin to what Americans would consider morally disgusting. Though the Samurai era had ended, that same historical sense of "death before dishonor" was present among most levels of the Japanese military; this sense of "saving face" was, and to some extent still is, a core part of civilian Japanese culture. To surrender rather than fight to the death was analogous to dishonoring the emperor, denying the unique and superior spirit of the Japanese over all others, and embracing shame and cowardice. Greater awareness and dissemination of this knowledge among the American rank and file might have led to some Americans not losing their lives attempting to take Japanese prisoners earlier in the war. This might have also helped American Soldiers and Marines in making decisions about surrendering, knowing that the Japanese would consider prisoners not only foreign enemies but also reprehensible, dishonorable, and something to be treated as less than human. It was a hard lesson in combat cultural awareness that Americans learned very quickly during World War II.

The Reconstruction of Japan after World War II

After World War II, the United States led the Allies in the occupation and rehabilitation of the Japanese state. In September 1945, GEN Douglas MacArthur took charge of the Supreme Command of Allied Powers and began the work of rebuilding Japan. This included widespread military, political, economic, and social reforms.[8]

While sometimes criticized for his handling of the Korean War, GEN MacArthur made brilliant use of cultural awareness to both consolidate gains and shape the strategic environment after America's defeat of Japan in World War II. Recognizing that the Japanese emperor represented Japanese culture and tradition, as well as the highest focal point of stability for a deeply hierarchical society, he allowed the emperor to retain his place in Japanese society. In this way, GEN MacArthur worked through the Japanese system and supplanted it—proclaiming that the largely United States-written post-war Japanese constitution, officially "approved" by the emperor, was Japanese in origin. Even by running post-war Japan from his isolated office, and rarely making public appearances, he used the familiar cultural image of the emperor, who before the war had been similarly inaccessible and perceived by the public as a nearly unknowable, mysterious figure of unquestioned power. Yet at the same time, GEN MacArthur also symbolically asserted his power by being the face of Japan's American conquerors, as illustrated by his casual dwarfing of Japanese Emperor Hirohito in their famous photograph together. This

Photo courtesy of the German Armed Forces

At the new border between the Third Reich and Soviet Union, September 17, 1939.

combination of upholding and reinforcing a traditional cultural role while simultaneously filling it, in part with an extremely untraditional person, was successful, as GEN MacArthur was relatively popular with the Japanese populace, and his actions solidified Japan as an American ally even today.

U.S. Army photo by LT Gaetano Faillace

GEN MacArthur and Emperor Hirohito at their first meeting, at the U.S. Embassy, Tokyo, 27 September 1945.

The Story Behind the Photo

In September 1945, Emperor Hirohito visited GEN Douglas MacArthur at the U.S. Embassy in Tokyo. During the visit, they posed for a photo that shocked the Japanese public. Up to 1945, the emperor had been a remote, mysterious figure to his people, rarely seen in public, whose photographs were always taken from a certain angle to make him look taller and more impressive than he really was. No Japanese photographer would have taken such a photo of the emperor being overshadowed by GEN MacArthur. The general intended the photo as a message to the emperor about who was going to be the senior partner in their relationship.[9]

In this culturally adept manner, GEN MacArthur consolidated American gains in Japan after World War II. At the same time, he both shaped the region politically and strategically by making Japan a key ally during the Cold War and, on an operational level, by creating a base of operations for America's military involvement in Asia, which included large-scale combat operations in the Korean War.

Conclusion

As illustrated by these examples, and by the myriad battles, operations, and wars throughout the centuries, history has shown us repeatedly the rewards of applying cultural awareness, which in turn can help achieve situational awareness, and the lethal consequences of ignoring it. When deciding whether large-scale combat operations can best achieve our macro objectives, cultural and situational awareness should be an important factor. While the decision may ultimately be the call of civilian-political leadership, military doctrine makes it clear that the armed forces are involved in this process and its implementation.

Epigraph

Lionel Giles, trans., *Sun Tzu on The Art of War* (Leicester, England: Allendale Online Publishing, 2000), 11, https://www.goodreads.com/quotes/17976-if-you-know-the-enemy-and-know-yourself-you-need.

Endnotes

1. Wikipedia, s.v. "Central Powers," last modified 8 March 2020, 20:18, https://en.wikipedia.org/wiki/Central_Powers.

2. "History of Western Civilization II," Lumen Learning, accessed 12 March 2020, https://courses.lumenlearning.com/suny-hccc-worldhistory2/chapter/the-treaty-of-brest-litovsk/.

3. Encyclopædia Britannica Online, s.v. "Munich Agreement," accessed 13 March 2020, https://www.britannica.com/event/Munich-Agreement.

4. "German-Soviet Nonaggression Pact," History.com, updated June 7, 2019, https://www.history.com/topics/world-war-ii/german-soviet-nonaggression-pact.

5. Wikipedia, s.v. "Operation Barbarossa," last modified 13 March 2020, 16:32, https://en.wikipedia.org/wiki/Operation_Barbarossa#Petroleum.

6. Wikipedia, s.v. "Molotov-Ribbentrop Pact," last modified 11 March 2020, 17:15, https://en.wikipedia.org/wiki/Molotov–Ribbentrop_Pact#Termination.

7. Ibid.

8. Office of the Historian, Department of State, "Occupation and Reconstruction of Japan, 1945–52," accessed 12 March 2020, https://history.state.gov/milestones/1945-1952/japan-reconstruction.

9. "Emperor Hirohito and General MacArthur meeting for the first time, 1945," Rare Historical Photos, December 7, 2016, https://rarehistoricalphotos.com/hirohito-macarthur-1945/.

Keith B. is a training specialist/developer for the U.S. Army Training and Doctrine Command Culture Center (TCC). He has authored several articles, papers, and training products related to culture and cultural issues. The TCC provides relevant and practical cross-cultural competency training and education in order to build and sustain an Army with the right blend of cross-cultural skills to facilitate the full range of military operations. The TCC maintains an extensive repository of cultural resources on their Army Training Network page at https://atn.army.mil/ (common access card login required).

by Lori S. Stewart, USAICoE Command Historian

Early on June 25, 1950, the North Korean People's Army crossed the 38th parallel and invaded the Republic of Korea (ROK). The capital, Seoul, fell by June 28, and ROK troops fled southward in retreat. The North Koreans nearly overwhelmed the peninsula before United States forces, under United Nations auspices, could land and establish a toehold at Pusan (now known as Busan).

The United States had a small intelligence-gathering capability on the ground in Korea in 1950. Officers of the Korean Military Advisory Group worked with every echelon of the ROK Army and compiled intelligence on the North Korean Army. Because the advisory group was assigned to the State Department rather than to GEN Douglas MacArthur's Far East Command (FECOM) in Japan, its information bypassed his headquarters and was instead reported directly to Washington. To collect the information GEN MacArthur needed, MG Charles A. Willoughby, the FECOM G-2, relied on the Korean Liaison Office, a detachment of intelligence specialists, in Seoul. Additionally, the U.S. Embassy in Seoul had military attachés and political analysts studying the military situation.

These intelligence organizations detected plenty of warnings leading up to the invasion. Between June 1949 and June 1950, FECOM intelligence dispatched 1,200 warnings to Washington of an impending North Korean attack. However, the North Koreans raided along the border so frequently that these incidents were referred to as "Sunday morning incursions." Additional evidence noted closer to the time of the invasion included the evacuation of civilians from the border area; the replacement of civilian freight shipments with military supplies; a large influx of troops, including concentrations of armor; and the stockpiling of weapons and equipment in forward areas. Still, no one thought these indicators to be out of the ordinary. Just 3 months earlier, MG Willoughby assessed that neither South

Courtesy of U.S. Army

MG Charles Willoughby, who had been GEN Douglas MacArthur's G-2 during World War II, continued in that role until May 1951. He retired from the Army shortly thereafter.

nor North Korea would initiate a civil war in the spring or summer of 1950. The embassy in Seoul likewise told the State Department that there was little possibility of a North Korean invasion.

One reason why North Korean activities raised little concern was that, since the beginning of the Cold War, Washington had focused more immediately on the Soviet Union. More likely problem areas were higher intelligence priorities. Korea was fifth on the Central Intelligence Agency's list for potential "explosiveness." Few analysts believed that North Korean leader Kim Il Sung would act militarily without direct Soviet assistance. The Department of the Army G-2, MG Leroy Irwin, stated in a March intelligence report, "Recent reports of expansion of the North Korean People's Army and of major troop movements could be indicative of preparation for aggressive action but Communist military measures in Korea will be held in abeyance pending the outcome of their program in other areas, particularly Southeast Asia." Analysts instead believed the North Korean leader would resort to more political initiatives to bring South Korea within its control.

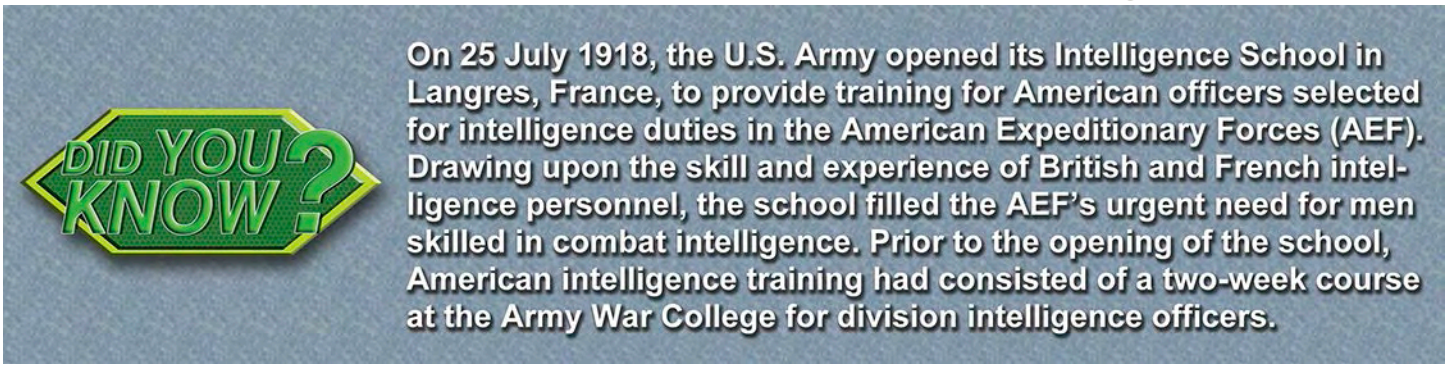
Courtesy of U.S. Army

A Soldier from the regimental headquarters S-2 debriefs a Soldier from a reconnaissance platoon just back from a nighttime mission into no-man's-land. The 1988 painting, titled *From Information to Intelligence*, is by Soldier-artist Anita Y. Sonnie.

Another reason American officials discounted indicators of an attack was an instinctive distrust of Korean sources who, they believed, overstated the threat for their own purposes. GEN Matthew Ridgway wrote after the war that GEN MacArthur's G-2 staff did not rate its local informants as reliable because they believed "South Koreans especially had a tendency to cry 'wolf' when there was no beast in the offing." Even more reliable sources were seen as self-serving. For example, when the American ambassador in Seoul reported a heavy buildup by the North along the 38th parallel, he was thought to be making a case for his recent request for armor for the ROK Army.

Finally, the U.S. Department of Defense simply minimized the potential threat because it was confident the ROK Army was so superior to its Communist neighbor that even if an attack occurred, the ROK could quickly defeat the North. It was commonly believed that North Korea did not have the power to attack the South unless equipped by the Soviet Union. Analysts unfortunately failed to evaluate accurately the significance of T-34 tanks amassed at the border.

During congressional hearings after the start of the war, Secretary of State Dean Acheson testified, "Intelligence was available to the Department prior to the 25th of June, made available by the Far East Command, the CIA, the Department of the Army, and by the State Department representatives here and overseas, and shows that all these agencies were in agreement that the possibility for an attack on the Korean Republic existed at that time, but they were all in agreement that its launching in the summer of 1950 did not appear imminent." Ultimately, the failure to predict the North Korean invasion was not one of failing to collect appropriate information concerning the enemy's capabilities. Instead, it seemed to be a failure at the higher echelons to analyze the enemy's intentions accurately.



Gallantry in the Korean War: MSG John R. Wilson

New Jersey native John R. Wilson joined the Army in 1942. He served in the Pacific theater during World War II, reaching the rank of major before being discharged in 1947. Shortly thereafter, he reenlisted as a master sergeant. When the Korean War began, MSG Wilson was assigned to the 25th Counter Intelligence Corps (CIC) Detachment, 27th Infantry Regiment, 25th Infantry Division.

Courtesy of U.S. Army

In 1952, the Counter Intelligence Corps Center at Fort Holabird, MD, dedicated a building to MSG Wilson and commissioned this painting of him. This painting now hangs in Wilson Barracks of the NCO Academy on Fort Huachuca, AZ.

After successfully defending Pusan, the Eighth Army broke out of the Pusan Perimeter and advanced up the Korean peninsula. By October, the 25th Infantry Division was mopping up operations to the rear, providing security for the Eighth Army's transportation network and clearing out enemy troops remaining in the area.

When alerted early in the morning of 13 October 1950 that enemy guerilla forces were moving to capture the small town of Pangso-ri, MSG Wilson quickly assembled his contingent of 30 Korean police officers and interpreters and organized them into teams surrounding the town. Taking four Korean officers with him, Wilson personally led an attack on a house from which enemy soldiers had opened fire. Although Wilson himself was killed by sniper fire, his actions facilitated the capture of 21 enemy soldiers.

For his gallantry under fire, Wilson was posthumously awarded the Silver Star. A fellow member of Wilson's CIC team later wrote, "John earned many Silver Stars, which he never received, and was one of those who the Corps could truly say was a hero in his own right." MSG Wilson was inducted into the Military Intelligence Hall of Fame in 1990.

On 4 August 1921, under the provisions of section 37 of the National Defense Act of 3 June 1916 (amended per 2 April 1921), the Military Intelligence Section, Officers Reserve Corps (MIORC) was established. The MIORC provided the Army's intelligence personnel through the interwar period. The MIORC initially was comprised of 286 experienced and trained officers who would be available for intelligence duties in the event of a full-scale mobilization. In the interwar years, that number peaked at 821 in 1927 before declining annually thereafter. By the time the United States declared war on Japan in 1941, the number of officers in the MIORC had dwindled to 573.

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 between 2,000 and 4,000 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 a 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.

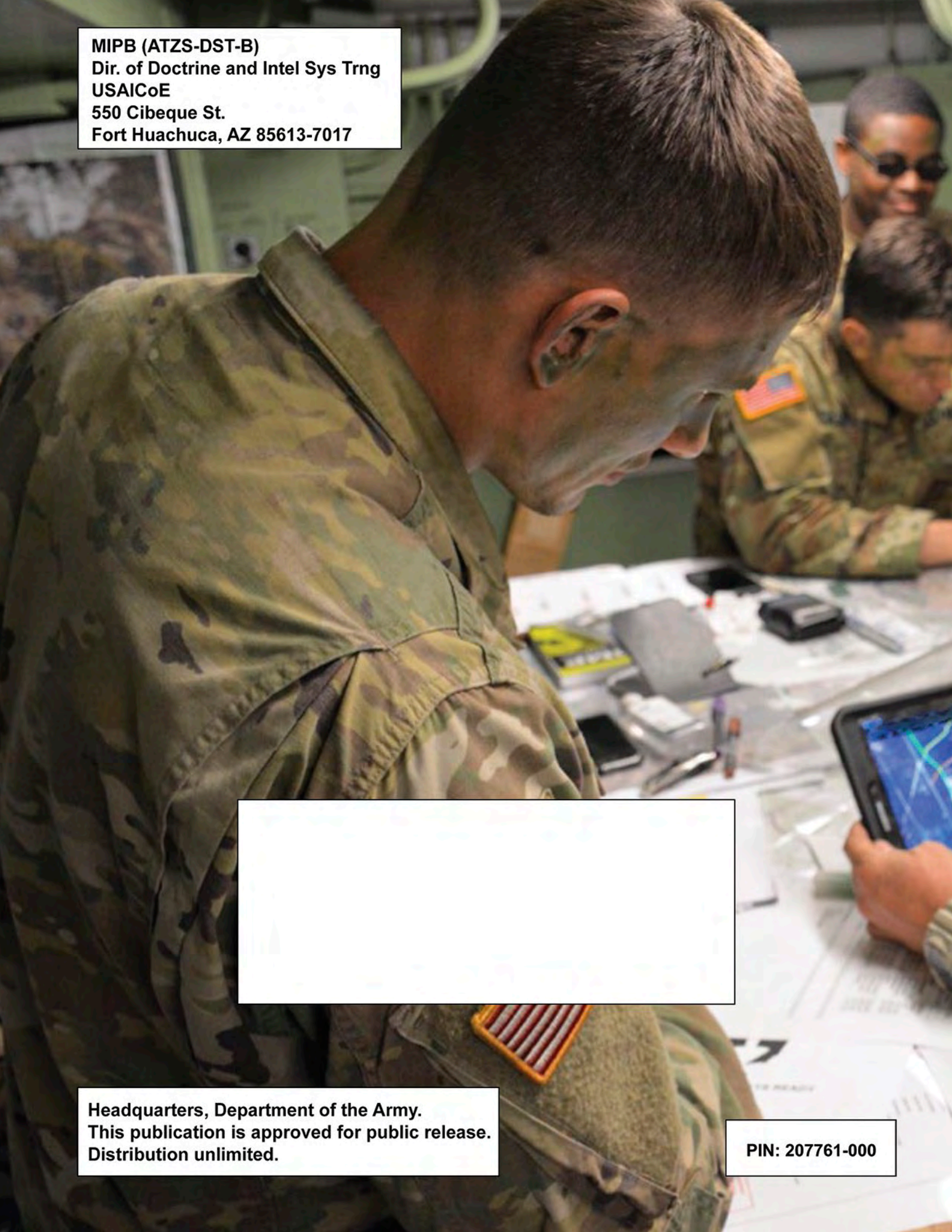
What we need from you:

- 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



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

PIN: 207761-000