MI PROFESSIONAL BULLETIN
January–June 2025
PB 34-25-1

SEMIANNUAL ONLINE COLLECTION

Manuscripts
Please send your manuscripts, including supporting documents, and any inquiries by email to—usarmy.huachuca.icoe.mbx.mipb@army.mil; visit our webpage for full article submission guidelines at https://mipb.ikn.army.mil.

Mailing Address
MIPB, DOTD, USAICoE, 550 Cibeque St., Fort Huachuca, AZ 85613-7017.

Reprints

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

The U.S. Army Intelligence Center of Excellence publishes the Military Intelligence Professional Bulletin (MIPB) under the provisions of AR 25-30. MIPB presents information designed to keep intelligence professionals informed of current and emerging developments within military intelligence. MIPB provides an open forum for the exchange and discussion of ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, and other topics for purposes of professional development.

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MATTHEW L. SANNITO
Acting Administrative Assistant to the Secretary of the Army

2520201

MI PROFESSIONAL BULLETIN
January–June 2025
Volume 51, Number 2

CONTENTS

U.S. soldiers assigned to 2nd Armored Brigade Combat Team, 1st Cavalry Division, supporting the 4th Infantry Division (4ID), alongside soldiers assigned to the Royal Lancers, Prince of Wales Troop, and Polish soldiers assigned to 15th Mechanized Infantry Brigade, all assigned to NATO eFP Battle Group Poland, provide rear security while breaching a building during a multinational urban assault exercise at Ełk, Poland, 2 March 2023. The 4ID's mission in Europe is to engage in multinational training and exercises across the continent, working alongside NATO allies and regional security partners to provide combat-credible forces to V Corps, America's forward deployed corps in Europe. (Photo by Sgt. Lianne M. Hirano, U.S.Army)

Ivy Intelligence (IVI) Large-Scale Combat Operations Targeting

Sergeant First Class Christian R. Ramsey, U.S. Army

Editor's Note: This article is reprinted with permission from Military Review, The Professional Journal of the U.S. Army, Combined Arms Center, Fort Leavenworth, Kansas. It was originally published in the November 2024 Online Exclusives on 6 November 2024. It has been modified to match MIPB's style and format.

The 4th Infantry Division G-2 Strike Cell operates "live" in Poland during a NATO multinational exercise on 15–19 April 2023. (Photo courtesy of 4ID Public Affairs Detachment)

Intelligence support to targeting at the division level faces several substantial challenges in large-scale combat operations (LSCO). First and most importantly, intelligence nodes often struggle to locate and identify high-payoff targets in the division's deep area. This fact is in large part a consequence of a habitual overreliance by the division's intelligence apparatus to leverage—near exclusively—its organic collection capabilities at the expense of other collection methods. This habit has almost certainly been formed and stabilized through twenty years of experience in the Global War on Terrorism. Second, Warfighter exercises (WFX)—the primary means through which a division headquarters executes its collective training—exacerbates this issue by failing to properly simulate otherwise available information derived through national technical means (NTM). By design, WFXs emphasize division organic collection to feed the division's targeting cycle. For instance, training audiences in a WFX enjoy the virtual video feed of an MQ-1C Gray Eagle but cannot obtain basic, satellite-provided electro-optical, infrared, or synthetic-aperture radar imagery. Third, the majority of analysts are not intimately familiar with the capabilities or duties of their single-source or all-source counterparts. As a result, the timeliness with which potential targets are verified and disseminated is diminished, ultimately allowing high-payoff targets to escape prosecution. Through a series of training and real-world experiences, the 4th Infantry Division (4ID) demonstrated that division G-2s can, in fact, mitigate these challenges by successfully incorporating and relentlessly exploiting NTM-derived information during its targeting process. This article argues that diversifying the types and levels of collection (i.e., tactical, theater, and national) results in a more robust and effective division collection capability—one that better facilitates situational understanding and targeting in support of the commander's objectives in a contested environment.

4ID currently employs a "strike cell" construct. The primary function of the strike cell is to leverage multiple intelligence disciplines to accomplish the "detect" phase in the Army's "Decide, Detect, Deliver, and Assess" process.[1] A secondary function is to feed the division's analysis and control element with timely and accurate information to inform the division's common intelligence picture. 4ID accomplishes these objectives by staffing the strike cell with signals intelligence (SIGINT), geospatial intelligence (GEOINT), and all-source intelligence analysts. These individuals are co-located in a mobile, modular command post trailer with no physical barriers to encourage cross-communication, rapid synchronization, cuing of information, and prioritization of targets (see figure 1). The analysts are managed and controlled by a strike chief, typically a chief warrant officer 2 all-source technician. The strike chief is responsible for validating and coordinating targets with the field artillery intelligence officer prior to their submission to the joint air-ground integration cell (JAGIC) for prosecution (see figure 2). To continue refining intelligence support to targeting and to better train analysts across the division, 4ID stood up an intelligence reach operations cell (IROC). The IROC is staffed by personnel from across Fort Carson, Colorado, which provides opportunities to all analysts, ranging from battalion intelligence shops to the division G-2. This mixture of experiences and skill levels provides a perfect test bed to innovate, experiment with, and validate the division's targeting procedures prior to implementation. Additionally, the diversity of knowledge provides multiple solutions to problems, which in turn typically results in the most effective selection process.

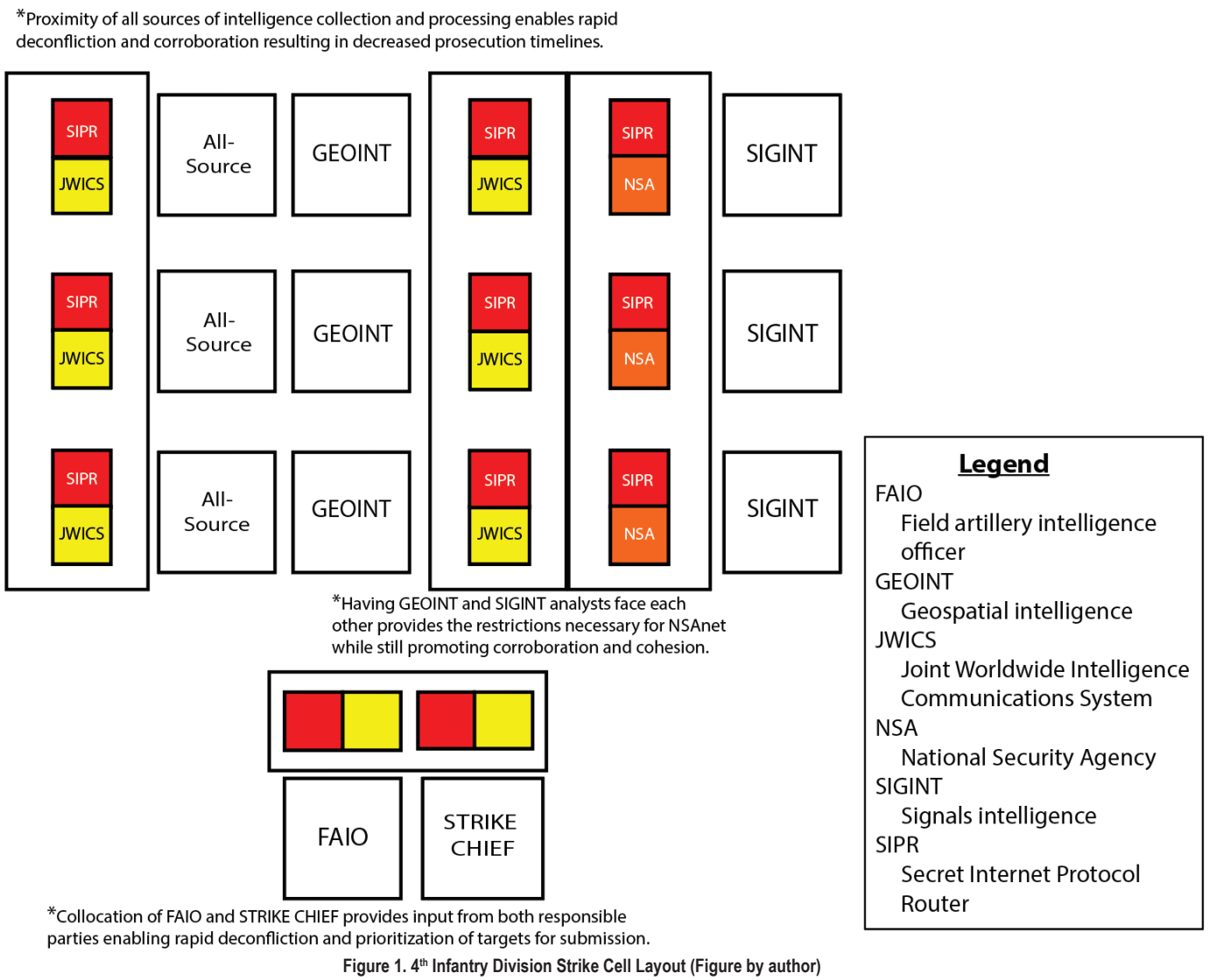


Figure 1. 4th Infantry Division Strike Cell Layout (Figure by author)

Problem Statements

When polling junior GEOINT soldiers and noncommissioned officers across the division, a common response is that after advanced individual training (AIT), most GEOINT professionals have limited or no exposure to NTM—the only exceptions are service members who enjoyed an initial tour of duty within an Intelligence and Security Command (INSCOM) unit. It is true GEOINT soldiers are taught processing, exploitation, and dissemination of imagery in AIT, but proficiency in this task is limited, especially when it is not prioritized during collective or section training events at home station. The typical response for the inclusion of this type of intelligence is "white card injects," which afford insignificant training value to the analysts and provides commanders with unrealistic expectations of the quality and confidence of the intelligence provided. The prioritization of ground moving target indicator and full-motion video is heavily encouraged due to the availability of simulations to support this training and the control offered at the division level. Currently, no such training tools are geared toward imagery processing, exploitation, and dissemination or other echelons above division collection. CW4 John R. Livesey III shares this sentiment in his article discussing geospatial intelligence support to targeting. Livesey writes, "GEOINT support to targeting primarily consisted of following targets with unmanned aircraft systems and conducting drone strikes. The Army, and joint forces, will require revitalized and refined GEOINT to support future multidomain operations."[2] Additionally, ground moving target indicator is commonly desynchronized from other war simulation inputs, leading to erroneous analysis and bad practices. In previous 4ID exercises, the strike cell has tipped-and-cued full-motion video assets (Gray Eagle) to positively identify ground moving target indicator detections and was surprised to find nothing in the immediate vicinity.

Separately, as the Army has transitioned to LSCO and multidomain operations, the division must ensure it is utilizing all aspects of collection to generate and maintain an accurate common intelligence picture regardless of what organic assets may be available. With operations conducted against peer adversaries, it is highly likely that airspace will be heavily contested and not easily traversed by unmanned aircraft and unarmed surveillance aircraft. This is echoed in CW3 Trent

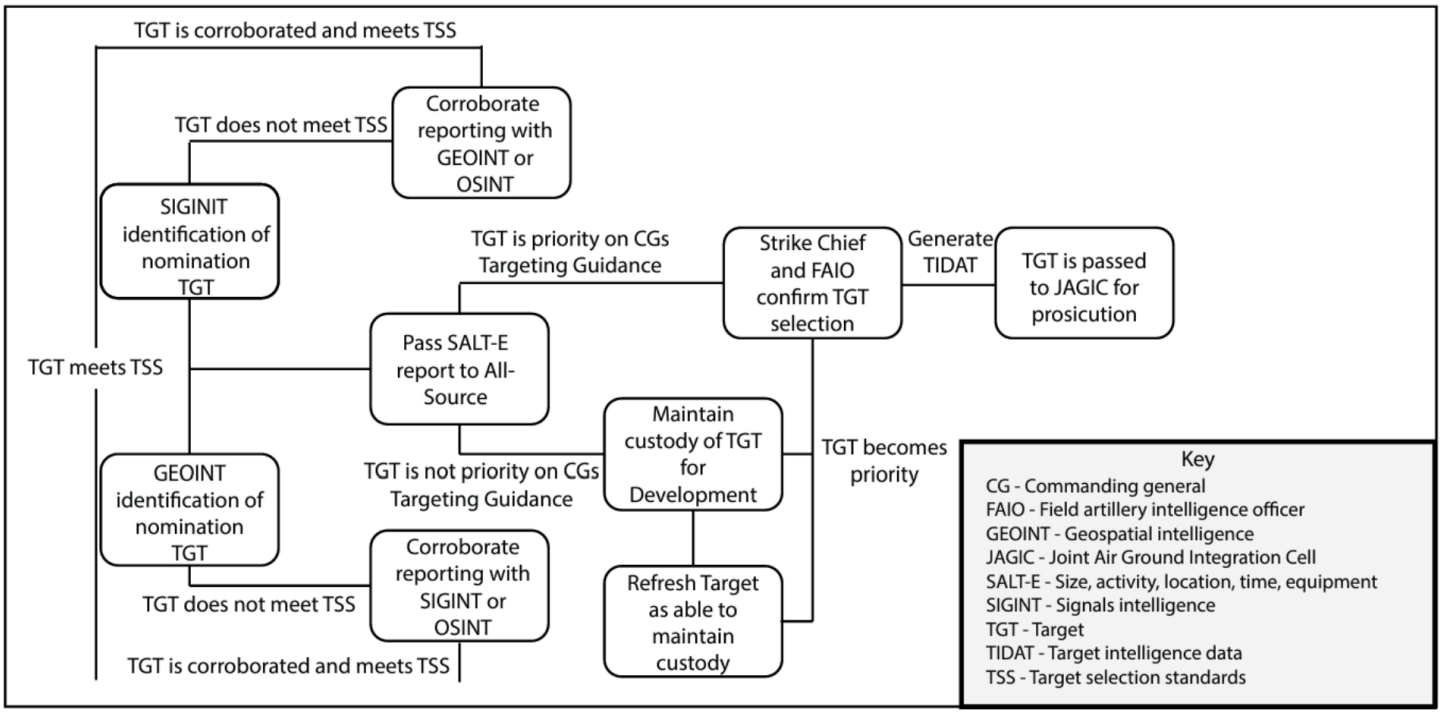


Figure 2. Intelligence Support to Targeting Flow Chart (Figure by author)

Taylor and WO1 Evan Lipp's publication on information collection support to targeting, in which they state, "Army forces will also contend with peer threats capable of employing long-range fires and denying freedom of airspace, compounded by the potential of a disconnected, intermittent, and limited communications environment."[3] Since many assets that divisions currently utilize may be ineffective in the initial stages of LSCO, there will be a gap in the common intelligence picture at that echelon. 4ID has had some success in supplementing its organic capabilities with NTM. The primary user of NTM at the division level is the SIGINT section. Analysis of SIGINT emissions can greatly increase the effectiveness of other NTM collection efforts by focusing search areas into a manageable sector that can quickly cue other intelligence disciplines, thereby reducing the amount of time required to positively identify critical targets. This is especially true of GEOINT analysts who are typically "snail trailing" through large images in search of possible targets. While the use of SIGINT to tip GEOINT does not completely remove the need to thoroughly exploit images, it does provide a much shorter sensor-to-shooter timeline. This increases the likelihood of successful strikes, especially when targeting highly mobile pieces of equipment such as surface to air missile systems. Cross-confirming with GEOINT is not always required depending on target selection standards and rules of engagement but is highly beneficial when target location errors (TLEs) are immature and require additional refinement to determine an acceptable aimpoint.

Last, through over three years of leading a division G-2 strike cell and IROC in both exercises and real-world operations, one thing has become abundantly clear to me: junior analysts and noncommissioned officers are not fully aware of the capabilities and duties of their counterparts. This has been true of over thirty individuals, many of whom were not on their initial contract. All-source analysts may obtain a baseline understanding of the other intelligence disciplines as a byproduct of their day-to-day activities. However, compartmented, single-source intelligence analysts are often limited in their opportunities to interact (and thus learn from) their peers.

Signals Intelligence

The challenges in operationalizing SIGINT at the division level are arguably the simplest to solve. Most SIGINT analysts at division are already practiced on drawing NTM-derived information, given the fact that division headquarters do not possess organic signals collection equipment. This creates a dependency on either the brigade organic Prophet system or NTM collection. By prioritizing NTM, division analysts can fill gaps when brigade elements are maneuvering or when their systems are nonmission capable. SIGINT sections at division can maximize situational awareness and understanding by leveraging NTM to look beyond the division deep area, providing additional information that will assist the analysis and control element in determining future enemy courses of action.

Notably, 4ID has had success utilizing a SIGINT-specific LSCO training pipeline developed by the Fort Carson Foundry platform, which included classes such as the Basic SIGINT Analyst Course (SI302), Advanced Threat Emitters Course (SI308), SIGINT Support to Counter-UAS (SI313), and Electro-Magnetic Preparation of the Battlefield (SI320). These courses, in conjunction with appropriate command and control, enabled SIGINT to be a more active participant in the targeting process.

Additionally, co-locating GEOINT and SIGINT personnel facilitated a free flow of information, greatly contributing to increased productivity and reduced timelines to develop and submit complete and accurate target packets.

4ID SIGINT primarily utilized the Fusion Analysis and Development Effort (FADE)/Multi-Intelligence Spatial Temporal (MIST) tool suite to conduct SIGINT support to targeting. While there were other programs used for refinement and additional context, most of the mission requirements were met with FADE/MIST. The interoperability of FADE/MIST enabled the importation of multiple data sets that informed assessments and provided additional context to emissions. 4ID SIGINT also utilized electronic order of battle analysis to feed the composition/disposition of enemy displayed on the common intelligence picture.

Another area in which SIGINT enabled success was cross-training all-source and GEOINT analysts on implementing and using FADE/MIST tools. This greatly increased the entire section's ability to locate and cross-cue potential targets with multiple intelligence disciplines, thereby increasing the strike cell's capability and capacity.

Geospatial Intelligence

In general, GEOINT imagery analysts receive the majority of their intelligence support to targeting training during AIT. Within the last year, analysts graduating from AIT enjoy the opportunity to pursue certification in target mensuration only and collateral damage estimation—two certifications paramount for targeting operations. That said, two classes that proved critical to 4ID operations but were (and still are) not part of the standardized training pipeline include Synthetic Aperture Radar Exploitation 1 and 2. The exploitation of synthetic aperture radar imagery is indeed a component of the AIT curriculum, with a specific focus on tactical identification at the onset of training. However, depending on whether the soldier is assigned to a Forces Command (FORSCOM) or INSCOM/Special Operations Command (SOCOM) formation upon graduation, the extent of synthetic aperture radar and electro-optical/infrared imagery exploitation and tactical identification training he or she receives varies significantly. FORSCOM-destined soldiers who attend a FORSCOM-specific training pathway later in AIT receive considerably more exposure to those skills than their INSCOM/SOCOM-destined peers. This reality ensures a large portion of AIT-graduates are considerably less practiced at perhaps the most important capability an imagery analyst provides during LSCO.

Decision-makers regularly discount synthetic aperture radar imagery due to the low-confidence assessments commonly associated with its exploitation. Numerous assessments employ confidence call language, such as "probable" or "possible" primarily because imagery analysts often cannot definitively specify the model or variant of equipment. 4ID has had success in utilizing visual aids such as measurements and side-by-side comparisons to further add validity to their analyst's assessments. Additionally, by utilizing other intelligence disciplines to bolster assessments, many "probable" pieces of equipment have been accepted by the JAGIC or higher headquarters for prosecution. This continuous fight to gain trust with the commander or decision-maker is not specific to intelligence support to targeting but can be the linchpin that separates an effective dynamic targeting cell from an ineffective one.

Processing, exploitation, and dissemination of imagery is one of the most time-intensive requirements in intelligence. Many images cover massive pieces of terrain that require considerable attention to detail and discipline to properly exploit. 4ID currently employs equal parts SIGINT and GEOINT imagery analysts due to a modified table of organization and equipment; however, it would be highly beneficial to staff two imagery analysts per SIGINT analyst to maximize the effectiveness of their coordination. While 4ID was able to complete the majority of its image exploitation before time limits set by target selection standards were met, some images past acceptable decay standards and were only exploited for situational awareness. Increasing the number of imagery analysts available would help to mitigate this issue. Additionally, having SIGINT cue GEOINT into search areas based on target location errors was highly beneficial and maximized the number of targets that could be confirmed via multiple sources. When prospective targets have been confirmed by multiple sources, the JAGIC is more likely to prosecute.

All-Source/Fusion Intelligence

All-source analysts in 4ID have acted as the connective tissue of the targeting cell. All-source analysts are expected to know the capabilities of equipment, the composition and disposition of enemy forces, and where the enemy is most likely to employ its critical systems. By integrating with the GEOINT and SIGINT sections, all-source analysts can effectively convey this information quickly. This leads to increased cross talk within the cell, further increasing the base skills shared by all analysts. 4ID SIGINT has had success in developing electronic order of battle to directly inform the composition and disposition of enemy forces in a combat scenario. The SIGINT personnel will analyze emissions and assess the likely location of accompanying equipment. If unable to identify the equipment via emissions, the GEOINT and all-source analysts will utilize imagery or reporting to provide additional corroboration. If the unit can be successfully identified, battle damage assessment can be properly allocated, enabling an accurate representation of enemy combat power and further informing the commander's targeting priorities. Additionally, identifying how the enemy forces employ key systems informs the electronic order of battle and order of battle, accounting for changes as adversarial forces improve their tactics, techniques, and procedures with inputs from

their successes and failures.

Additionally, all-source personnel in the strike cell provide direct input to the analysis and control element, which results in increased awareness of disposition of forces for future assessments. The simplest way to accomplish this is by generating message data in U.S. message text format and populating it into the intelligence fusion server. Targets that are under prosecution by the JAGIC are sent as an S305, a target intelligence data message; and equipment that is not actively targeted is sent as a S303, an enemy observation report; S309, enemy situation report; or a tactical report. Utilizing the U.S. message text format and populating it on the intelligence fusion server maximizes reach and provides a record to conduct in-depth analysis of movements over time.

Finally, the utilization of open-source intelligence (OSINT) will be necessary in a peer or near-peer contested environment. Adversarial actions may degrade organic collection assets and NTM to the point where intelligence gaps prevent the production of accurate assessments. OSINT will likely be available due to the sheer number of sensors providing information that are available and will likely serve as the primary resource used to fill these gaps. Multiple real-world conflicts have shown the prevalence of civilians reporting on military operations. This, in conjunction with poor operational security enforcement, results in a fairly accurate depiction of objectives and force posture via OSINT reporting. While some personnel serving within the 4ID strike cell and IROC have OSINT certifications (OS301/302), the operational tempo of the mission set often precluded full utilization of these tools by analysts already consumed with performing their primary occupational tasks. Additionally, OSINT-trained personnel should be included in a targeting cell's staff to enable additional avenues for collection and target information corroboration.

Conclusion

Overall, there are multiple ways that a division G-2 can diversify its collection efforts to better enable its intelligence support to targeting and to increase its analytic potential. Leveraging existing collection capabilities at echelons above division will mitigate gaps caused by a lack of organic assets or possible degradation cause by enemy actions. To fully utilize these assets, analysts should attend formal training and seek out opportunities to attend a live-environment training, or, if possible, stand up an IROC. Staffing the IROC from multiple organizations on a rotational basis will mitigate risk to the unit's day-to-day missions while simultaneously enabling enhanced intelligence training objectives. This also serves to broaden the knowledge and skillset of participants and facilitates the testing of new and more efficient solutions. Additionally, the more time analysts spend learning the duties and capabilities of their cross-discipline counterparts, the more agile and informed their analytic output will be. This will provide the commander or decisionmaker with the best assessment available and continue to improve the trust relationship that is so critical to the intelligence profession.

An ancillary but not insignificant benefit regarding 4ID's IROC initiative deals with soldier retention. Because 4ID's IROC allowed for the exploitation and processing of real-world data, analysts felt they were doing the job they signed up to do. Removing physical and cognitive barriers to streamline information sharing heightened cohesion within the cell. The potential to contribute to real-world missions likewise enhanced a common sense of purpose. Perhaps most importantly, analysts could visibly see their skillset proficiencies improve, bolstering confidence and pride in work performance. All of these factors underpinned not only an elevated level of job satisfaction among 4ID intelligence professionals (and retention rates) but contributed to the division becoming a faster and more lethal organization as an outcome.

During visits with multiple U.S. Army senior leaders, a singular, common question prevailed: "Why aren't other divisions doing this?" The easy answer is unit operational tempo. Most divisions are juggling operational deployments, training requirements, staff exercises, military intelligence training standards, and more. Justifying the removal of low-density military occupational specialty soldiers to attend a live environment training or stand up an IROC is a vexing task. However, 4ID has found it is possible through strong leadership and calculated manning decisions—namely by (1) establishing a ninety-day rotational cycle for IROC participants, (2) incorporating IROC experiences as part of standing military intelligence training standards requirements, and (3) resourcing participation from across multiple commands so that just one does not bear the entire burden. To be sure, 4ID continues to identify gaps in capabilities as it encounters new requirements or problem sets. However, its experience with its strike cell and IROC demonstrate the potential to improve division lethality beyond historic norms.

Notes

1. Field Manual 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, October 2023), 3-20.

2. John R. Livesey III, "Geospatial Intelligence Support to Targeting," *Military Intelligence Professional Bulletin* 49, no. 1 (April 2023): 3, https://mipb.army.mil/articles/spt-targeting-spec-ed/livesey-geoint.

3. Trent Taylor and Evan Lipp, "Information Collection Support to Targeting," *Military Intelligence Professional Bulletin* 49, no. 1 (April 2023): 2, https://mipb.army.mil/articles/spt-targeting-spec-ed/taylor-information-collection.

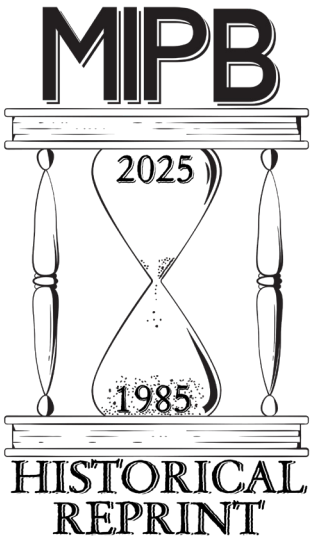
SFC Christian R. Ramsey, U.S. Army, is the 4th Infantry Division analysis and control element noncommissioned officer in charge (NCOIC). His assignments include two deployments to Afghanistan as an intelligence analyst and one deployment to Poland as the Fusion NCOIC. Ramsey has served as the 4th Infantry Division strike chief for two years, in addition to previously serving as the 500th Military Intelligence Brigade S-2 NCOIC and as a fusion analyst in the 3rd Cavalry Regiment.

If I were a lieutenant today in the 101st Military Intelligence Battalion (CEWI)

I WOULD

work hard to

"LEAD BY EXAMPLE!"



Lt. Col. James R. Riser

Editor's Note: In continuation of the historical retrospective that began with our 50th Anniversary Commemorative Compilation, every quarter, the Military Intelligence Professional Bulletin will highlight an article from the past that is still relevant today. This article first appeared in the July–September 1985 issue. The doctrinal and regulatory publications referenced in this article have either been superceded or rescinded.

WITH REGARD TO MY ARMY AND PROFESSIONALISM

I WOULD feel personally honored to serve my country as an officer in the United States Army.

I WOULD always remember that my mission Is to provide Intelligence support to the 1st Infantry Division. I would make sure that my troops know the critical importance of their contributions to the division's combat readiness and that they are physically and mentally prepared to go to war at any time.

I WOULD know the doctrine prescribing how intelligence "works" within a division. (Get copies of, and read, FM 34-1, *Intelligence and Electronic Warfare Operations*; FM 34-80, *Brigade and Battalion Intelligence and Electronic Warfare Operations*; and FM 34-103, *Division Intelligence and Electronic Warfare Operations*.)

I WOULD spend a part of each day studying some aspect of the proud institution in which I serve, the United States Army. (Read some history about our country and our army at war. It will give you some perspective on why intelligence and unit readiness are so vital. Start with *The Leavenworth Papers* from the Combat Studies Institute, Command and General Staff College: Number 3. *Not War, But Like War: The American Intervention in Lebanon* and Number 5. *Fighting the Russians in Winter*. Additionally, S.L.A. Marshall's books are super. Try *Battles in the Monsoons* to get an accurate picture of combat in Vietnam.)

I WOULD get my own personal copy of FM 27-1, *Legal Guide for Commanders*, and study up on the administration of military justice and administrative law at the company level. Also study, and get for each of your soldiers, FM 27-14, *Legal Guide for the Soldier*.

I WOULD acknowledge that senior officers and many NCOs have already experienced many of my problems, so I would seek their advice and help. (Make sure, however, their advice and help is based on a correct understanding of *your* particular problem.)

I would inspect myself thoroughly and frequently:

- Do I need a haircut? (Lieutenants should get haircuts before they need them – it helps in making captain.) If I wear a mustache, is it properly trimmed?
- Are my boot heels run down? (Good lieutenants and lieutenant colonels should wear out lots of boot heels. We need to replace them often.) Does my uniform fit? Buttons, nametags, patches okay? Hatbill clean? Field gear–would I be in uniform if I went to the field today? Overweight? Out of shape?
- How is my military bearing–do I stand up straight? How do I "shape up" as an officer? Good? Not so good? (Remember: Your troops are inspecting you whenever you are in their presence. You are expected to and must set the example. You can start with AR 670-1, *Wear and Appearance of Army Uniforms and Insignia*. Also be aware of and comply with appropriate command policy letters.)

I WOULD establish and maintain an open line of communication to my company first sergeant and my battalion command sergeant major. (These professional soldiers can take a lot of misery out of your life if you will let them.) I would not take myself too seriously nor get bogged down with worry. (No one will shoot you if you display a fleeting imperfection once in awhile.) I would have a pen or pencil and a notepad with me at all times and I'd develop a habit of writing notes to myself. I would write down good ideas as I thought of them or when someone else mentioned one. (Then you should use all the good ideas you have notes on, if you can. It also helps to jot down bad habits you might need to work on.)

I WOULD assemble my own up-to-date working tools for immediate use: ARs, FMs, SOPs, DA pamphlets, checklists, policy letters, and soldiers manuals. (Also get copies of IG and Command Inspection reports to see if your areas of responsibility passed or flunked–good place to start work. Also get appropriate policy letters published by higher headquarters–at least to division level. You can tell which ones you need by reviewing lists of published letters. Your company commander and battalion adjutant can help you on this one. Also, frequently review DA Pam 310-1, *The Consolidated Index to Publications and Forms*, to see if a new publication or change is available to help you in your work.)

I WOULD strive to become technically proficient in my principal and additional duties. I would, in addition to my principal duty, organize each of my additional duties with a mini-chain of command to ensure that each duty is, in fact, fully carried out. (Know the purpose of each additional duty and who or what the target is. Check feedback to see if your additional duty is on target.) I would coordinate with battalion staff officers having functional responsibility for my principal and additional duties to make sure I am meeting their requirements and expectations. I would also get with the IG inspector for each of my duties for guidance, direction, sympathy, or whatever help I may need. At the very least, I would get the list of references (to include dates of publication) used to inspect each area. (This works well for all duties, and it helps to show your commander that you've got it together and are professional.)

I WOULD not "look the other way" if I saw a uniformed soldier improperly dressed, sloppy, or who didn't salute. I'd correct him on the spot and report it to his commander if appropriate. Never pass by a mistake! I would require all subordinates to practice good military courtesy in my presence (for example, "Yes, Sir" or "No, Sir," proper responses to my questions, standing up when addressed by me, and so forth). I would not allow junior soldiers of any rank to call me by my first name or nickname. I would insist on military courtesy. (And don't address your subordinates or superiors by their first names. Use correct military titles in your professional dealing with others.)

I WOULD position myself to the left of any senior officer with whom I might be walking and I would require subordinates walking with me to do the same. (This is an old Army custom. Do your part to keep military traditions and customs alive in our Army.) I would return subordinates' salutes with a cheerful and hearty verbal greeting as well as a snappy return salute. (Remember, your soldiers expect you to speak when meeting them and how you speak is their clue to your attitude.)

I WOULD make sure that my word is my bond. I would take pride in having a reputation for truthfulness and honor that would allow my troops to say, "It has to be true, Lieutenant... said so." (Follow through with anything you tell your troops you will do and ensure feedback gets to them. Your credibility is in jeopardy if you don't.)

I WOULD be "up front" with my evaluations of subordinates. Don't "lay back" and let your subordinates think they are doing just fine and then destroy them with poor OERs or EERs. You must develop the courage to constructively inform others of their shortcomings. Do this in a timely manner so your subordinates will have time to react before an evaluation is written.

I WOULD recognize that I won't be a lieutenant very long and that I need to scope out my future on a time line. Career planning and development should be a topic of discussion with MILPERCEN and with senior officers in my branch. (Include your family development. Your family will have a big impact on your career as it progresses.) (A current list of MI Branch contacts was printed In the April–June Issue of *Military Intelligence*. You should personally visit MILPERCEN at your earliest opportunity and establish an "eyeball" relationship with your assignment officer.)

I WOULD keep handy, and frequently review, a list of leadership actions which I should be accomplishing as a professional leader. I would, at the very least:

- ✦ Lead by example.
- ✦ Be considerate.
- ✦ Tend to the needs of soldiers.
- ✦ Maintain loyalty up and down.
- ✦ Make quality a habit.
- ✦ Build "staying power."
- ✦ Cultivate credibility.
- ✦ Reward the deserving.
- ✦ Develop pride.
- ✦ Follow through.
- ✦ Be ready.

Look beyond these "bullets" for the *meaning*—then develop your own operating style which lets you carry out the actions in a way which is natural to your personality. Read your feedback constantly and carefully; it'll show you where you need to do some work in the leadership area.

I WOULD maintain a personal working file on all finance and personnel actions that pertain to myself. (You might want to put your important papers in a commercial depository for safekeeping.) I would make sure my checking account stayed straight and that I could do basic arithmetic. (Don't be careless with your finances and be especially watchful if a joint account is involved.) I would program periodic leave and take it. (Encourage your subordinates to do likewise. They need to "get away from it all" once in awhile just as you do.)

I WOULD continuously evaluate my professional strengths and weaknesses as a participating member of my own chain of command. I would ask myself, "Have I gained the trust and respect of my soldiers?" I would recognize that I have only

four categories of resources: people, equipment, time, and operating funds. (Most of your resources are fixed at your level. Your professionalism will be measured by how efficiently and economically you convert your resources into mission accomplishment.)

I WOULD not intentionally embarrass a fellow soldier in public. (Let the Individual know in advance when you plan to bring up a matter pertaining to his area of responsibility.) I would carefully avoid saying or writing anything I wouldn't want quoted back to me later. (And don't allege more than you can prove—you may be asked to do so someday.) I would understand that I live in a "fishbowl." Both my on-duty and off-duty conduct must be impeccable and beyond reproach at all times.

I WOULD learn how to write. I would be embarrassed professionally if my boss had to rewrite my correspondence. (Get AR 340-15, *Preparing Correspondence*; AR 310-50, *Authorized Abbreviations and Brevity Codes*; and a good dictionary and a good thesaurus. Use them all. Other useful books: **Harbrace College Handbook**, 7th Edition, and **Elements of Style**, 3rd Edition. I would require my subordinates to develop good writing techniques and I would proofread everything before sending it forward. (Extra training may be required; if so, lay it on.)

I WOULD make sure that I (and a spouse, if applicable) learned basic social graces, such as "RSVP" and "Regrets only." (Several books are available to help you in this area; check with your company commander or battalion adjutant. DA Pamphlet 600-60, A Gulde to *Protocol and Etiquette for Official Entertainment,* contains good Information and an excellent bibliography.) I would teach my spouse basic Army organization, the names of key people, and something about my job. I would keep my spouse informed and encourage social participation.

I WOULD evaluate my civilian education and seek opportunities for improvement, keeping in mind that my first goal is to be a good, solid leader.

I WOULD ensure that my personal affairs are kept in order, including finances, personnel records, will, and emergency data card. (JAG officers can help you with this one. Also, commercial organizations can be of great help. Carefully evaluate your own situation to determine if you need assistance. DA Pamphlet 360-531, *Your Personal Affairs—A Checklist*, should be part of your package.)

WITH REGARD TO MY COMPANY

I WOULD thoroughly know my company Emergency Deployment Plan, as well as the installation Emergency Deployment OPLAN, and be sure my subordinates know the plan and can execute it in a professional manner.

I WOULD fully and openly support the company commander and first sergeant, even if I might privately disagree. (You may express disagreement in private but, if overruled, then give 100 percent support. After all, they just might be right. And then, *issue orders in your own name*. Don't tell your troops they have to do something because "the old man" is making it happen. You lose respect and authority if you don't issue orders as if they were of your own initiative.)

I WOULD openly honor and respect the position of the company first sergeant. (He doesn't outrank you, but his unique title and position warrant your special professional consideration.)

I WOULD learn as much about the company structure that supports my platoon as I could. (To be really effective, you need to know about your unit supply, motor pool, orderly room, training, NBC, arms room, reenlistment, safety, and so forth.)

I WOULD make sure that what I think I am supposed to be doing is what my boss thinks I'm supposed to be doing. (Then see that you're "doing more doing" than "thinking about doing." A periodic joint review of your OER Support Form 67-8-1 can be helpful here.)

I WOULD actively support the unit sports program, both as a participant and observer, when possible.

WITH REGARD TO MY PLATOON

I WOULD use troop welfare, morale, pride, and esprit de corps as common denominators for every action I took in leading my troops. I would work hard to maintain an excellent working relationship with my platoon sergeant and I would openly support him. (You set the standards and polices to guide him, then let him function as an NCO. Ask for and consider his advice in your decisionmaking process and don't ever "put down" your platoon sergeant in front of your soldiers.)

I WOULD know what my NCOs are supposed to do, then I would see to it that they do it in a professional manner. (Don't do it for them—let them earn their titles and pay.) I would ensure my NCOs are maintaining high levels of order, discipline, and cleanliness in my troop work and billet areas. (Be especially attentive to the billets on weekends and holidays—a few uncaring soldiers can make billet living an unpleasant experience. Don't let that happen in your platoon—check it personally and frequently.)

I WOULD pay special attention to NCOs in section sergeant level positions and help them in their leadership roles. (Many of your junior sergeants are in their first leadership positions and will need help. Don't assume they know a

great deal—they may not, and it is simply a function of experience. Be patient, but make them study and work hard at being good leaders.)

I WOULD get my own copy of AR 623-105 and AR 623-205. (These ARs prescribe the evaluation reporting systems for officers and enlisted soldiers. Study them and evaluate your subordinates properly. Also, know how *you* are being evaluated.) I would establish and watch closely the rating scheme and submission times of OERs and EERs for my subordinates. (You can quickly get behind in this area. Pay attention to the paperwork aspects of your personnel management actions—most key personnel moves will generate multilayer EER or OER requirements.)

I WOULD insist on absolute control over the people and property allocated to me by the MTOE for my mission responsibilities. I would then lay out my platoon organization, match my people and property to it, and firmly fix responsibility and accountability for both through my chain of command. I would have secure areas constructed to store my platoon equipment. Field gear for off-post personnel would have to meet the same availability, cleanliness and storage criteria as for on-post personnel. (If you don't provide space and an SOP, field gear will be all over the place and much of it will get lost.)

I WOULD sort out my platoon equipment and make sure I have trained and licensed principal operators for every piece of equipment and that licensed back-up operators are available or in training. Reluctant soldiers, those not wishing to be honored with a military driver's license, would receive intensive extra training to help them obtain a license. (Don't let your equipment be dispatched without your control over it—could be that some untrained operator will "save" his equipment and ruin yours.)

I WOULD conduct frequent open-ranks and equipment layout inspections to verify that my chain of command has already achieved and is maintaining my high standards. (Make sure you are in line with the company and battalion SOP. Also keep in mind that we no longer have a simple "uniform" but rather "multiform'' when it comes to individual dress for our soldiers, for example, male, female, maternity, cooks' whites, and jungle fatigues.)

I WOULD study FM 22-5, *Drill and Ceremonies*, in detail and insist that drill and ceremonies conducted by my platoon were done properly. (Do it right and do it sharply.) I would learn how to prepare my platoon for inspection and how to report to a senior officer that my platoon was prepared for inspection. (Don't forget to actually prepare your platoon for inspection—you must personally check it out if you want to avoid embarrassment some day.)

I WOULD make sure my soldiers have appropriate soldier's manuals for their MOS and grade and that my sergeants know and can do everything their soldiers are supposed to know and do as outlined In the manuals. (Also ensure trainer's guides for each MOS in your platoon are on hand or on requisition and that they are being used by your trainers.) I would be able to personally do all the common tasks identified in FM 21-2 and FM 21-3. (If you don't know how to do some of the tasks, your troops will be proud to teach you if you let them. Don't worry about loss of respect If you tell them you don't know how to do something—they probably already know.)

I WOULD see that section chiefs and squad leaders make good use of available job books and, if a job book for an MOS in my platoon is not available, I would design one myself. I would get a copy of, and use, the division HIP Pocket Training Handbook. (Ensure that each of your leaders uses it too!)

I WOULD learn *The Army Maintenance Management System* (TAMMS) as it applies to my platoon. (Get TM 38-750, *The Army Maintenance Management System*, DA Pam 750-1, *Organizational Guide For Leaders*, and FM 29-2, *Organizational Maintenance Operations*, as a minimum and you can get a good start on your organizational maintenance program. Also get and read the monthly issues of ***P.S. Magazine***. Read FM 10-14-1*, Commander's Handbook For Property Accountability At Unit Level*, to help you understand unit supply.) I would get a copy of the "DASH 10" operator's manual for each major item of equipment in my platoon and be fully capable of performing proper Preventive Maintenance Checks and Services (PMCS) on that item. (The automotive and communications technicians, as well as the unit armorers, will be glad to help you.) I would ensure that when my platoon is at the motor pool, I am also at the motor pool (teaching maintenance techniques to my soldiers and ensuring the health of my PMCS program).

I WOULD set very high standards and demand compliance by my chain of command members first and then by every member of my platoon. (Don't worry about whether your soldiers like you at this point. Your first job is to set and achieve high standards. In the long run, your troops will respect you if you do.)

I WOULD try to have the same chain of command for mission accomplishment as for billeting control and personnel accountability, such as reporting in company formations. For example, I would want a maintenance section sergeant to be accountable and responsible for his section equipment and for what each member of his section does or fails to do. *His* promotion would depend on how well both technical and troop leading duties are carried out.

I WOULD Inspect my chain of command personnel on every contact and initiate corrective action on the spot. I would require that persons ordered to take corrective actions report back to me at a specified time and place to verify compliance. I would not hesitate to lay

extra training on any person under my command who was slow to shape up. I would stand in the last rank of my platoon occasionally to check the receiving end of verbal information—Accusative? Inspiring? (Think morale.)

I WOULD meet with each new soldier on the day he is assigned to my platoon, ensure his immediate needs are met (family settled, bunk assigned, bedding issued, meal card issued), and ensure he is familiar with the post recreation services. (Don't "lose" a soldier due to neglect during his inprocessing—first impressions are important.)

I WOULD vigorously seek appropriate school quotas for my soldiers and ensure they are ready to attend school. (Use recent attendees to get programmed attendees ready. Develop and have ready an Order of Merit list so if one of your troops can't make it, you've got the next in line alerted and ready to take his place. This reduces no-shows and failures.)

I WOULD know how to communicate in a tactical situation—for example, how to use automated CEOI, how to prepare and operate FM radio sets in secure and unsecure modes, and how to lay in a field telephone system.

I WOULD personally Inspect my platoon members' weapons. (Include the crew served weapons and check out the level of crew training. Remember, this is not the armorer's job, it's that of the chain of command.) I would take care of and clean my own assigned weapon.

I WOULD take PT with my platoon and watch closely the attendance of every soldier. I would see to it that everyone could pass the PT test unless medically excused. I would enforce the Army Weight Control Program.

I WOULD be tough on discipline, personal appearance, soldier training, and organizational equipment maintenance. I would be alert for and prohibit fraternization which might be detrimental to the morale of my platoon. (Watch out for *perceived* fraternization—it can do as much harm as the real thing. Be especially careful yourself—working late with only another soldier present, riding in POVs, innocent social affairs, and so on. All of these can create a perception of fraternization. Be alert and watch your own actions.) I would keep in mind that superior or subordinate fraternization can be just as devastating as sexual fraternization. (Make sure those in your chain of command keep their professional distance from subordinates, but balance professional distance with professional friendliness; this increases respect for everyone.)

I WOULD be alert for evidence of sexual harassment. Keep In mind targeted soldiers may be reluctant to complain for fear of reprisal. Offenders won't commit sexual harassment in your presence, only in the presence of targeted soldiers. Also, don't use or condone the use of obscene language by either sex. I would also be alert for sexual discrimination. (You might have a key person who deprives a subordinate of organizational and personal justice simply because the subordinate happens to be a member of the opposite sex. Racial discrimination can follow the same pattern. You must stay alert for both forms, caution everyone against them, and take swift and thorough action when you detect discrimination. Your job here Is to ensure that *all* persons under your control have equal chances to succeed.)

I WOULD watch my platoon chain of command for evidence of drug and alcohol abuse. (Remember, mind altering substances of any sort do not mix with leadership. And if you drink and have had "a few at the club," don't go to the barracks at night and try to be someone you aren't. Go home and behave yourself. Caution sergeants living in the barracks—they are more likely to bump into such situations than you are.)

I WOULD get involved in military discipline actions pertaining to any member of my platoon and strive for absolute justice. (Take the time to discover the truth about what happened or allegedly happened—don't allow an innocent soldier to be punished.)

I WOULD know, and watch closely, the promotion process in my platoon, especially the Promotion Eligibility Roster (SIDPERS C-01). No member of my platoon would be promoted nor go before a promotion board without my personal approval and I would personally make sure that every soldier knew and understood the platoon/company promotion process. (Include NCO and warrant officer input in your decisions to promote or not to promote. Follow through and ensure your soldiers know why you did whatever you did. Keep in mind that promotions are as important to individual soldiers as your promotion is to you.) I would know how promotion points are accumulated by my soldiers and then help the deserving ones. (For example, certificates of achievement from a lieutenant colonel are worth five points, but only a total of 10 points may be used in this category, and so on.)

I WOULD know the re-enlistment status of everyone in my platoon. If I had an undesirable soldier, I would initiate action to get him barred from re-enlisting and administratively removed from the Army, if appropriate. I would then vigorously encourage every satisfactory soldier in my platoon to stay *in the Army*. I would be dissatisfied with myself if I let a good soldier leave my platoon without knowing I had done everything possible to get him to stay in the Army.

WITH REGARD TO MY SOLDIERS

I WOULD be constantly on the alert for their safety—both on the job and where they live. (Be tough, insist on safety in everything you and your troops do.) I would seek to understand my soldiers in terms of what drives and motivates them. (Soldiers represent the best that America has to offer. Get to know yours well.)

I WOULD keep my soldiers informed of everything that affects them. (This is perhaps the biggest problem at platoon/section level—don't let it happen in your unit. Soldiers need to make plans for future events just as you do. You need to let them know how and when their time is going to be affected by your plans. Be careful about how you execute changes to your plans—big potential for morale problems.)

I WOULD teach my soldiers something about personal money management. (Find out who is broke two days after payday—chances are some help is needed. Also, check your soldier's Leave and Earning Statements for problems such as pay withheld or incorrect deductions. Pass on some of your smarts, demonstrate your concern for your soldiers' welfare. If you are broke two days after payday. You may also need some help.) I would recognize that soldiers have but two resources while in the Army—their free time and their money. I would not deprive my soldiers of either resource without full justification nor would I allow anyone else to do so. (UCMJ punishment locks in on these two resources—make sure personal, organizational, and military justice prevails.)

I WOULD ensure that my soldiers are receiving constructive counseling and I would personally review their counseling statements. I would frequently visit my soldiers in their billets during off-duty hours and take the time to stop and chat with them. I would make sure that I spent time "listening with them" rather than "talking at them." I would frequently visit and eat meals in the dining facility. (Sit down, chat, and have your meal with your soldiers. Although your presence might give them indigestion, it also gives them something to write home about. And don't "buck the line." Your own soldiers may be on a tighter schedule than you are. Bucking the chow line is no way to win friends and influence people—especially your own.)

I WOULD be aware of signs of alcohol and drug abuse in my soldiers. (If abuse is detected, take immediate action, remembering to balance disciplinary action with professional medical help, as appropriate.)

AND FINALLY...

I WOULD recognize that the above "I woulds" deal with setting high standards for myself and my soldiers. And, Lieutenant, always remember that the day you compromise a standard, you've set a new one—lower.

Lt. Col. James R. Riser graduated from Pennsylvania Military College as a distinguished military graduate in 1967. Commissioned as a second lieutenant in Military Intelligence, he initially served a two-year combat arms detail in Armor. His previous assignments have included: Tank Platoon Leader and Battalion S2, 1/13th Armor, 1st Armored Division, Fort Hood, Texas; Cavalry Platoon Leader, 2/17 Cavalry (ABN), 101st Airborne Division, Vietnam; Special Security Officer, HQDA, the Pentagon; Assistant Brigade S2, 2nd Brigade and Assistant Division G2, 101st Airborne Division (Air Assault), Fort Campbell, Ky.; Detachment Commander, 2nd MI Detachment, 2nd Infantry Division, Korea; Senior Combat Intelligence Instructor, The Infantry School, Fort Benning, GA.; Research and Development Project Officer, Center for Systems Engineering and Integration, Fort Monmouth, N.J.; Battalion Executive Officer and Battalion Commander, 501st Military Intelligence Battalion (CEWI), 1st Armored Division, Ansbach, Germany; Chief, Intelligence Division (ASIC), G2, VII Corps, Stuttgart Germany. Riser is a graduate of the airborne and Ranger courses, Armor Officer Basic Course, MI Officer Advanced Course, and the Command and General Staff College. He received a master's degree in Public Administration from Western Kentucky University in 1975. Riser currently serves as commander of the 101st MI Battalion (CEWI), 1st Infantry Division (M), Fort Riley, Kansas.

These tips were adapted from a similar version originally authored by Col. Robert H. Pratt who developed them as a guide for his officers in 1982.

LEVERAGING IMAGERY COLLECTION AT THE TACTICAL LEVEL

BY MAJOR JUSTIN T. DELEON
AND CAPTAIN FREDERICK ELVINGTON

Discussion of the commercial products and services in this article does not imply any endorsement by the U.S. Army, the U.S. Army Intelligence Center of Excellence, or any U.S. government agency.

Introduction

During the Joint Pacific Multinational Readiness Center's (JPMRC's) Rotation 24-01, the 3rd Infantry Brigade Combat Team (IBCT), 25th Infantry Division (ID) sought to operationalize and exploit commercial imagery in a large-scale combat operation fight. The goal was to leverage commercial imagery as a dependable collection platform to cue other sensors to support brigade targeting and decision making. Several challenges and obstacles emerged, among them a time-intensive request process through multiple bureaucracy chains and self-imposed barriers to dissemination that made it difficult to harness commercial imagery's advantages. This article discusses the 3rd IBCT attempt to use commercial imagery at the tactical level. Moreover, it illuminates the challenges encountered and provides recommendations to aid future use of commercial imagery to gain a relative advantage during large-scale combat operations.

The National Geospatial-Intelligence Agency (NGA) and the National Reconnaissance Office (NRO) are the two organizations that manage satellite imagery collection requirements for the Department of Defense (DoD). The NGA drives collection efforts and ensures collection aligns with national intelligence requirements; the NRO then allocates space-based assets and ground systems to meet those requirements.[1] During the Global War on Terrorism, it was routine for units to receive satellite imagery consistently as tactical priority intelligence requirements were often nested with national intelligence requirements. However, with the operational shift from counterinsurgency to large-scale combat operations, relevant satellite imagery has become more difficult to obtain at the tactical level as units struggle to tie fluid local collection requirements to national level requirements.

The DoD incurs no added financial cost to obtain national technical means imagery, but competing priorities limit their ability to fulfill dynamic requests. Commercial imagery, however, has become widely available and increasingly relevant on the contemporary battlefield, so a solution to the challenge of competing priorities is to purchase imagery from these commercial entities. The DoD has contracts to purchase commercial imagery with requests using the same submission process as requests to obtain national technical means imagery.

Companies such as MAXAR Technologies, Planet Labs, and Black Sky are leading providers of commercial imagery solutions. Using these products can bring transparency and awareness to the battlefield, making it difficult for disinformation campaigns to be successful.[2] This effect has been demonstrated in the Russo-Ukraine War, where MAXAR has consistently provided services that facilitate Ukraine's targeting of Russian Forces.[3] These commercial imagery solutions have enabled Ukraine to stay ahead of, or at least keep pace with, its adversary.

The power of modern-day commercial imagery is twofold. First, the scaling of commercial satellite constellations allows almost continuous observation with visual, radar, and electromagnetic sensors, which enables the industry to provide low-latency coverage.[4] Second, commercial imagery is inherently unclassified and can be shared rapidly across echelons and with allies and partners.[5] When used properly, commercial imagery can greatly enhance targeting and awareness across the joint and combined force.

Exercise Preparation

In preparation for the JPMRC 24-01 rotation, the 3rd IBCT, 25th ID sought to leverage commercial imagery to enhance situational awareness and targeting operations. Lessons learned from Ukraine and the Middle East were the driving

force of this initiative. The brigade required access to low-latency imagery to aid the commander's decision making and support the targeting process as an initial cueing sensor. The plan was for the brigade to develop a direct relationship with MAXAR Technologies, allowing it to request imagery directly from the provider and receive timely support.

The intelligence team, however, was unable to execute this plan for several reasons:

- Establishing a direct request relationship with MAXAR could violate NGA or intelligence oversight policies.
- The cost of commercial imagery collection was more significant than anticipated.
- NGA's imagery collection requests were likely to take priority over the brigade's requests.

Instead, the 3rd IBCT obtained low-latency imagery of JPMRC exercise training areas using the 25th ID collection management team, following the established request process. The brigade initiated requests for collection 60 days before JPMRC 24-01 began.

Certified collection managers do not typically reside below the division level. To acquire a geospatial intelligence collections account and the required credentials, requestors had to complete up to four months of training across multiple installations. Once submitted by the brigade, the imagery requests traveled through an arduous chain of vetting and validation at the division, corps, army command, and combatant command levels before making their way to the NGA where the final determination about support for the requests was made.

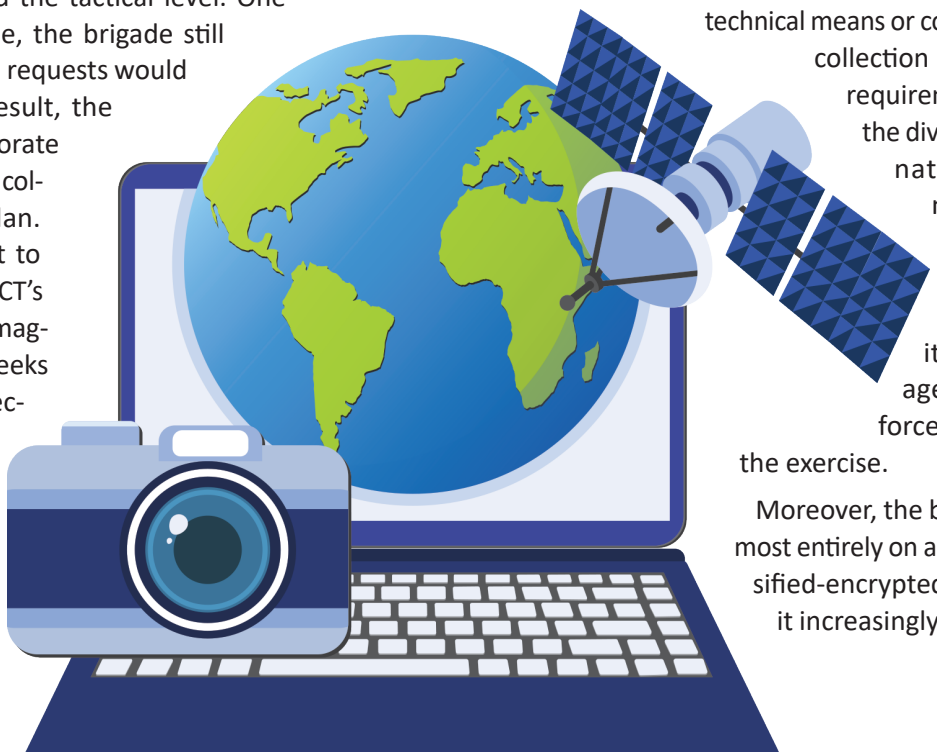
Knowledge gaps in the request process across echelons degraded awareness of the status of the 3rd IBCT's requests. Typically, the NGA notifies users when to expect support for collection requests; however, during JPMRC 24-01, this information never reached the tactical level. One week before the exercise, the brigade still did not know whether its requests would receive support. As a result, the brigade could not incorporate commercial imagery in its collection and targeting plan. While the NGA did elect to support some of the 3rd IBCT's collection requests and imagery began to populate weeks before the exercise, collection management teams across echelons were unaware that the imagery was available until a few days before the exercise.

Exercise Execution

Upon confirmation of the imagery's availability, the 3rd IBCT attempted to retrieve it for processing, exploitation, and dissemination (PED) with the aim of using perishable information from the low-latency imagery to help drive operations and targeting. However, once the 25th ID conducted its initial PED, only individuals with an approved nondisclosure list (NDL) account were authorized to view the imagery due to interpretations of DoD intelligence oversight policies regarding collecting information on U.S. persons, complicated by training on U.S. soil. The 3rd IBCT immediately submitted applications for the NDL accounts, and, in the meantime, the division collection team obtained an exception to policy that allowed the 3rd IBCT's intelligence Soldiers to view the commercial imagery that fell within the 25th ID's purview.

PED operations proved to be slow and cumbersome. The large-scale combat operations environment in which the 3rd IBCT found itself was extremely fluid, and the commercial images provided little value to decision making and targeting. Moreover, inconsistent receipt of commercial imagery added to the challenge. For example, the brigade might receive images of half of the training areas one day and none on another day. This made using the imagery as a sensor or cuing apparatus complicated. As before, knowledge gaps across echelons made it difficult to anticipate when the brigade could expect support.

The final challenge the 3rd IBCT encountered involved the classification of the imagery the team received. Commercial imagery is inherently unclassified; however, all the imagery received was classified. An investigation revealed that the imagery collected to support JPMRC was derived from national technical means instead of commercial assets. The team discovered this occurred because the imagery requests 3rd IBCT sent stated that either national technical means or commercial imagery collection would satisfy the requirements. As a result, the division only received national technical means imagery, which unfortunately limited the team's ability to share imagery with partner forces participating in the exercise.



Moreover, the brigade worked almost entirely on a secure but unclassified-encrypted enclave, making it increasingly complex to share

classified imagery with subordinate elements. Operations officers and commanders throughout the brigade did not have regular access to the SECRET Internet Protocol Router Network. Therefore, even if the imagery had been more relevant to decision making, the classification barrier alone would have disrupted the brigade's ability to share it promptly with key players across the team.

A Way Forward

While commercial satellite imagery has the potential to provide tactical formations with a pivotal advantage, adversaries that are willing to pay can leverage similar capabilities. For example, in 2020, Iran purchased low-latency commercial imagery to enable its targeting of Ain al-Asad Air Base in Iraq following the killing of Islamic Revolutionary Guard Corps General Qassem Soleimani. The subsequent attack resulted in over 100 American Service members injured. Reporting does not identify the company from which Iran purchased the imagery; however, we know that Iran acquired the imagery on the same day as the attack.[6] The bottom line is that by using commercial imagery, an organization with fewer barriers and the means to pay can maintain real-time awareness to help drive operations and targeting.

Solutions to these challenges are worth exploring, as finding a path that effectively manages this resource at the tactical level could prove critical on the future battlefield.

Recommendations for the IBCT. The following are recommendations for using and exploiting commercial imagery at the IBCT level in the future.

Request Access for Brigade Collection Managers. Although it takes time and training, brigade collection managers should be encouraged to obtain the credentials to request commercial imagery. This training does not currently decrease the request chain requirements, but it allows brigade-level intelligence professionals to advocate more effectively for their commanders' information requirements.

Close the Knowledge Gap. Battalion-, brigade-, and division-level intelligence professionals should educate themselves on the current imagery request process. Understanding this process can help intelligence professionals manage their commanders' expectations and better identify the lead times required for imagery requests. Many U.S. Army divisions have NGA representatives attached to their organizations. They are a wealth of knowledge and can play a pivotal role in closing knowledge gaps within organizations.

Communicate a Shared Understanding of the Required Imagery Classification. The tactical element requesting imagery should clearly communicate its need for national technical means or commercial imagery and the desired classification level of the product. Once analyzed and exploited, even commercial imagery can become classified above the end user's clearance, making sharing with partners on the ground difficult. All parties must understand whether they should distribute an intelligence product or only basic imagery. The requesting element needs to systematically describe and fully justify its collection requirements. This offers a further rationale to authorize requesting capabilities at the brigade level.

Train Intelligence Analysts and All-Source Intelligence Technicians. Division, brigade, and battalion intelligence analysts should receive training on accessing and disseminating commercial imagery. They should also be well versed in using NGA and NRO tools such as iSpy[7] and learn how to quickly access and disseminate unclassified imagery. If tactical formations are going to use commercial imagery to drive tactical targeting, they cannot depend solely on the two or three brigade-level geospatial intelligence imagery analysts to meet all needs.

Recommendations up and out. The following are recommendations for using and exploiting commercial imagery at levels above the IBCT in the future.

Treat National Technical Means and Commercial Imagery Requests Differently. It may be valuable to begin differentiating national technical means from commercial imagery. Currently, the process for requesting national technical means support and commercial imagery support is the same. Establishing separate request processes for national technical means and commercial imagery might allow tactical formations to use commercial imagery more effectively.

Shorten the Request Chain. The current multi-layered review process for tactical formations to request imagery through NGA is lengthy and cumbersome. While it serves an essential purpose, auditing the process to determine where it could be shortened would enhance tactical formations' ability to leverage the resource. Additionally, as the battlefield becomes more fluid, tactical formations may require more direct communication with commercial imagery companies to keep pace with proficient adversaries. These commercial imagery requests may not require the same level of vetting as national technical means.

Conclusion

The 3rd IBCT, 25th ID's efforts during JPMRC 24-01 illuminate the current obstacles to operationalizing commercial satellite imagery. Although the 3rd IBCT received several packages of national technical means imagery during its JPMRC rotation, the information needed to be more timely to be of operational value to decision makers. A challenging request, dissemination, and classification process made it difficult for imagery to support decision making and targeting on a fluid battlefield. Nonetheless, with informed intelligence professionals, refined processes, and mitigated systemic barriers, commercial imagery is a resource that could provide a relative advantage. This may be critical as tactical formations look to outpace adversaries on an increasingly transparent battlefield.

Endnotes

1. "About Us," National Geospatial-Intelligence Agency, last modified October 30, 2024, 11:20, https://www.nga.mil/about/About_Us.html; and "About the National Reconnaissance Office," National Reconnaissance Office, https://www.nro.gov/About-NRO/.

2. Maxar Technologies, "New Documentary on Ukraine Underscores the Importance of Maxar's Commercial Satellite Imagery and Capabilities," *Maxar Technologies Blog: Earth Intelligence*, March 02, 2023, https://blog.maxar.com/earth-intelligence/2023/new-documentary-on-ukraine-underscores-the-importance-of-maxars-commercial-satellite-imagery-and-capabilities.

3. Ibid.

4. Gary Dunow, "The Game-Changing Role of Commercial Satellite Imagery and Analytics in Ukraine," *Maxar Technologies Blog: Earth Intelligence*, April 12, 2023, https://blog.maxar.com/earth-intelligence/2023/the-game-changing-role-of-commercial-satellite-imagery-and-analytics-in-ukraine.

5. Sandra Erwin, "U.S. Military and Allies Get a Feel for the Value of Commercial Satellite Imagery," Space News, August 13, 2023, https://spacenews.com/u-s-military-and-allies-get-a-feel-for-the-value-of-commercial-satellite-imagery/.

6. Nathan Strout, "Report: Iran Used Commercial Satellite Images to Monitor US Forces Before Attack," C4ISR Net, March 1, 2021, https://www.c4isrnet.com/intel-geoint/2021/03/01/report-iran-used-commercial-satellite-images-to-monitor-us-forces-before-attack/.

7. Adam Goodman, "NGA Brings Products Closer to Action in Middle East," *CHIPS*, March 2, 2020, https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=13225. iSpy is "a web-based, image-viewing application that provides tools for imagery analysis and exploitation."

MAJ Justin DeLeon is the S-2 for the 3rd Infantry Brigade Combat Team (IBCT), 25th Infantry Division (ID), Schofield Barracks, HI. He previously served as a plans officer for the 25th ID, an intelligence officer in the 1st Cavalry Division, and a rifle platoon leader in the 172nd Separate Infantry Brigade. His service includes overseas tours in Germany, the Republic of Korea, and Afghanistan. He holds a master of science in management, strategy, and leadership from Michigan State University, a master of military studies from the Marine Corps University, and a master of arts and military operations from the School of Advanced Military Studies.

CPT Frederick Elvington is the S-2 for the 2nd Squadron, 6th Cavalry Regiment, 25th Combat Aviation Brigade, 25th ID, Wheeler Army Airfield, HI. He enlisted in the Army in 2013 and served as a 35F, Intelligence Analyst, with the 173rd Infantry Brigade Combat Team (Airborne). As a commissioned officer, CPT Elvington has served as rifle platoon leader and brigade collection manager in the 3rd IBCT, 25th ID. He holds a bachelor's degree in political science from the University of Tampa.

MULTINATIONAL AND COMBINED INTELLIGENCE AT THE DIVISION LEVEL

BY MAJOR ED PECORARO

Republic of Korea Army (ROK) Army Soldiers assigned to 2nd Infantry Division/ ROK-U.S. Combined Division secure simulated intelligence after conducting a company-sized attack on objective at Twin Bridges Training Area, South Korea.

Introduction

According to the *2022 National Defense Strategy*, close collaboration with allies and partners is essential for advancing U.S. national security interests and bolstering collective capacity to confront traditional challenges while managing recent threats.[1] Military operations will rarely be unilateral, especially in response to opposition from the People's Republic of China, Russia, Iran, North Korea, and violent extremist organizations.[2] Establishing defense relationships with allies and partner nations is crucial for accomplishing national security objectives, preempting conflict, and mitigating risks to U.S. military forces engaged in conflict.[3]

The U.S. Army should expect that all future operations will be multinational.[4] Intelligence will drive those operations, and they, in turn, will enable intelligence.[5] Successful multinational and combined intelligence at the division level requires executing the intelligence process in collaboration with mission partners. The opportunities presented by this collaboration, including legitimacy, cultural awareness of the operational environment, unique capabilities, and an added perspective on complex problems, can far outweigh the challenges.[6]

The United States and the Republic of Korea (ROK) have conducted combined operations since the Korean War. Their lessons learned and methods of operating as a multinational force can provide understanding to others working in mature alliances, as well as to those planning and implementing new organizations. Unlike the partnership between the International Security and Assistance Force and the Afghan National Security Force during Operation Enduring Freedom, which focused solely on information sharing, the 2nd Infantry Division/ROK-U.S. Combined Division (2ID/RUCD) conducts comprehensive multinational intelligence operations as a combined team.

The 2ID/RUCD provides timely, relevant, and tailored intelligence to supported commanders by recognizing a shared purpose, using a combined workspace, employing a mature mission partner environment (MPE), and capitalizing on the capabilities of both nations' higher and adjacent headquarters. The insights and lessons in this article can benefit other divisions that conduct intelligence operations with multinational partners.

Definitions and Doctrine

Discussing combined intelligence in Korea requires understanding key definitions: multinational, combined, and alliance. Multinational operations are "conducted by forces of two or more nations, usually undertaken in the structure of a coalition or alliance."[7] Combined is an older term used by the North Atlantic Treaty Organization (NATO) and the ROK that shares the multinational definition.[8] An alliance is "the relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members."[9] Within Korea, 2ID/RUCD is a combined headquarters operating under the *Mutual Defense Treaty Between the United States and the Republic of Korea; October 1, 1953* and a 2014 memorandum of agreement between the U.S. Forces Korea/U.S. Eighth Army and the ROK Army Chief of Staff.

The doctrine that guides U.S. military forces employed in multinational operations is Joint Publication 3-16, *Multinational Operations*. It describes the strategic context, nature, and tenets of multinational operations at the joint level.[10] This publication also describes various command and coordination relationships and outlines how commands can conduct multinational operations in all domains.[11]

Army doctrine for multinational operations is Field Manual 3-16, *The Army in Multinational Operations*, which describes the fundamentals of multinational operations as they relate specifically to the Army. It includes considerations for command and control, intelligence, planning, sustainment, medical support, special operations, civil-military operations, and other operational considerations.[12]

Field Manual 3-16 identifies several concerns relating to intelligence in multinational operations including intelligence, surveillance, and reconnaissance synchronization, information sharing, and intelligence architecture.[13] The manual includes a checklist of questions that staff should be capable of answering while participating in multinational operations, such as:

- Has the military decision-making process been employed?
- Have liaison officers been identified and established?
- Have processes for intelligence exchange been determined?
- Have rules of engagement relating to intelligence aspects of the operation, such as human intelligence, been established?[14]

Combined Intelligence Operations

Since 2014, 2ID/RUCD has been a combined division with the infrastructure of a mature theater to accommodate its multinational operations. Its C-2 succeeds at combined intelligence operations for several reasons, including:

- The analysis and control element (ACE) fully integrates the ROK Soldiers, specifically in the areas of fusion, targeting, and collection management.
- The network architecture enables collaboration for operations and intelligence.
- The U.S. and ROK forces both leverage higher and adjacent headquarters.
- The liaison officers (LNOs) are a priority for all combined theater exercises.
- The ROK Soldiers integrate easily into the division.

The combined division conducts at least three division or higher exercises yearly, so there are frequent opportunities for staff, command post, and digital crew process training. The ROK Soldiers within the C-2 are critical to executing all stages of the intelligence process.

Analysis and Control Element

U.S. and ROK officers in the 2ID/RUCD ACE share workspaces during armistice and exercises. They jointly conduct intelligence analysis and production, knowledge management, information management, collection management, and intelligence architecture support. They also have a workspace in the headquarters specifically for combined intelligence operations, which includes workstations for the fusion cell, geospatial intelligence cell, and collection management. Additionally, all ROK Soldiers assigned to 2ID/RUCD are fluent in English and hold the appropriate security clearances, reducing barriers to sustaining rapid intelligence analysis. The ROK Army's investment in interoperability demonstrates its organizational commitment to the success of 2ID/RUCD. As a combined team, the C-2 updates the armistice intelligence estimate, with the U.S. and ROK analysts alternating weekly to provide a situation development brief to the division commander.

To plan and direct intelligence, the C-2 sections use the shared workspace and, as a team, produce intelligence preparation of the operational environment products to support the combined staff's military decision-making process. The ACE's ROK Soldiers have a better understanding of the threat, so their input is crucial to the C-2's ability to achieve situational understanding; however, both the ROK and U.S. Soldiers participate in planning briefings for the commander and staff. This ensures shared understanding within the ACE and guarantees equity in producing intelligence products that inform the commander's decision points. Any differences in analytical judgments and assessments are considered during intelligence production and are presented as necessary; however, disagreements are typically resolved through fair-mindedness and intellectual empathy.

U.S. and ROK Soldiers in 2ID/RUCD can leverage their nations' intelligence enterprises as well as other members of the combined staff. For example, when 2ID/RUCD was preparing for a division warfighter exercise, the area of operations (AO) differed from the AO in which 2ID/RUCD usually operates. The C-2 ROK officers were able to coordinate with adjacent ROK units to acquire existing products relating to the new operational environment.

Another area where the combined ACE team integrates well is in support of the targeting process and battle damage assessment (BDA). The ROK members coordinate with higher and adjacent headquarters to develop the high-value and high-payoff target lists, ensuring that 2ID/RUCD aligns its analysis for enemy units and systems. Additionally, the combined team cooperates on the ACE's BDAs, especially when developing and executing the mechanism through which the

ACE evaluates the target system assessment during division exercises. The combined team then provides an accurate correlation of forces and means analysis daily during the commander's update assessment that helps inform senior leaders' decision making.

Network Architecture

Another critical component of multinational operations is the MPE, and one of its key components is the mission partner network (MPN). The MPE is "an operating framework enabling command and control and information sharing for planning and execution."[15] The MPN is "a network portion of an MPE and is a specific partnership or coalition-wide area network, planned and implemented using standards and protocols agreed to by participants."[16] Each mission command and intelligence system exists on an MPE that the C-2 uses daily and during theater exercises. 2ID/RUCD operates daily on a robust MPE and architecture that enables combined intelligence.

2ID/RUCD executes the intelligence process on a single combined network. This greatly enhances its ability to analyze, collaborate, produce, and disseminate products to U.S. and ROK subordinates and higher and adjacent units. While an MPE can be limiting when working with networks of higher classification, the C-2 uses cross-domain solutions and cross-domain chat programs to process and disseminate data. This allows single-source cells within the ACE to quickly collect and process releasable reporting. The 2ID/RUCD ACE refined its knowledge and information management procedures to operate effectively within an MPE. It established sources and delivery methods for information and data to analyze and update intelligence estimates, situation templates, event templates, common intelligence pictures, and BDA.

Organizational Coordination and Liaison Officers

Another strength of the combined intelligence team is its ability to leverage higher and adjacent military headquarters and intelligence agencies from each nation. The ROK Soldiers communicate directly with other ROK units to inform intelligence estimates and update the common intelligence picture and the intelligence portion of the common operating picture. The team quickly establishes intelligence handover lines with other ROK Army headquarters, allowing 2ID/RUCD to better posture its collection and targeting capabilities. Our nations' respective intelligence communities have unique capabilities and focus; through our combined efforts, the C-2 can better answer intelligence requirements.

A critical aspect of 2ID/RUCD's ability to coordinate with adjacent and higher units is its employment of LNOs. 2ID/RUCD provides personnel during command post exercises, including intelligence warfighting function representatives. These LNOs integrate with their supported headquarters to facilitate information collection planning and intelligence report dissemination and to provide both headquarters with a shared understanding of intelligence assessments. The adjacent and higher headquarters with whom 2ID/RUCD coordinates do not all have the same access to information and intelligence that is critical for large-scale combat operations. Since MPEs are not guaranteed to exist within some partner tactical command posts, LNOs are postured to share releasable intelligence, such as intelligence reports from division collection assets and finalized intelligence products.

Recommendations

Recognizing that multinational operations are a realistic probability for U.S. Army divisions in the future, Army divisions should prepare to conduct multinational intelligence during the planning and preparation phase. Integrating into similar militaries should be a focus during planning for multinational operations, and divisions should perform regular assessments during enduring operations. Challenges such as language, interoperability, culture, caveats, and authorities are obstacles to address early. Overcoming them will make multinational intelligence possible.

Critical Thinking. Critical thinking is an essential skill that must be developed in a multinational team. When conducting multinational intelligence, differences in doctrine, culture, equipment, and history can impact the ability of a combined intelligence organization to share knowledge and build consensus.[17] Logical fallacies, such as fallacies of relevance, can lead to poor assessments and cause friction within a multinational team.[18] Specifically, the genetic fallacy (claiming that a report or assessment is right or wrong because of its origin) and an appeal to tradition (asserting that an idea must be accurate because one has always believed it) can make working in a multinational team delivering assessments to a commander more difficult.[19] To address this, a multinational intelligence team must value the essential intellectual traits of fair-mindedness and intellectual empathy.[20]

Military intelligence professionals should strive to appreciate the strengths and weaknesses of reasoning from the point of view of others, especially those from a nation that may be closer to the threat or who have studied the threat longer than U.S. Soldiers.[21] Additionally, one must actively consider assessments from different perceptions and strive to reconstruct the reasoning behind those assessments.[22]

Write for Release. Another recommendation is that the Army must prioritize writing for release as it increasingly operates with unified action partners.[23] Army Techniques Publication 3-16.02, *Write for Release*, outlines the importance of this practice, as it improves shared understanding with a partnered force, makes sharing information faster, can be adaptable to sharing requirement changes, and facilitates MPE usage.[24] The 2ID/RUCD C-2 creates a releasable version of all intelligence products when possible. Writing for release is essential to

creating shared understanding among the combined staff. Because it writes for release, 2ID/RUCD can better integrate ROK units into the division and rapidly enter a command or support relationship with a higher ROK headquarters.

Although both Army and joint doctrine emphasize the importance of writing for release,[25] it is not a widespread practice. However, an intelligence organization *must* write for release. Finalized intelligence reports or information collection reporting often cannot be shared within 2ID/RUCD because external organizations do not write for release when even a single sentence tear-lined report can enable a combined headquarters to create shared understanding.[26]

One way to improve writing for release is reviewing and revising how the U.S. intelligence community classifies open-source reporting. Intelligence agencies, combatant commands, and Army Service component commands regularly publish open-source intelligence (OSINT) reports with restrictive distribution caveats. For example, unclassified open-source reports on relevant threats to 2ID/RUCD that can inform the commander's decision-making process often have restricted distribution caveats that inhibit production and dissemination. Every request for release for an OSINT product has been approved, but it takes time, and often there are no changes to the original report. OSINT regularly answers 2ID/RUCD's intelligence requirements, but restrictive distribution caveats impact collaboration and the ability to have shared understanding.[27]

Prioritize Use of the Mission Partner Environment/Network. During multinational operations, as much of the intelligence process as possible should exist on an MPN. Establishing an MPN can be costly, time-consuming, and difficult due to compatibility and security issues.[28] Additionally, the functionality of MPNs can be limited solely to information dissemination rather than allowing collaboration. Nevertheless, the Army should prioritize intelligence systems capability and fielding on MPNs. Intelligence systems are often established first on U.S.-only networks with little initial consideration for MPNs. These systems, however, have limited use in 2ID/RUCD's combined environment. The Army must consider MPEs when testing and fielding new digital systems–2ID/RUCD provides an excellent testing environment for MPE implementation of new intelligence systems. The division's C-2 is postured to provide the best bottom-up refinement as it operates daily on an MPN and conducts up to three division- or theater-level exercises yearly.

Conclusion

The integration of multinational and combined intelligence at the division level, as demonstrated by 2ID/RUCD, is crucial for the future of Army operations. Successfully executing the intelligence process with mission partners ensures prompt, relevant, and tailored intelligence support to commanders, which is essential for shared understanding and operational success in a multinational context. The experiences and methodologies of 2ID/RUCD highlight the importance of shared workspaces, mature MPEs, and leveraging higher and adjacent headquarters to enhance intelligence capabilities. Divisions can foster a collaborative and effective multinational intelligence team by proactively addressing challenges such as language barriers, interoperability, and cultural differences. Additionally, prioritizing writing for release and integrating it into MPNs are pivotal for facilitating collaboration. As the Army prepares for the complexities of future operations, these insights and recommendations may aid divisions in collaborating with multinational partners to achieve mission success.

Endnotes

1. Department of Defense, *2022 National Defense Strategy of The United States of America* (Washington, DC: U.S. Government Publishing Office [GPO], 27 October 2022), 14. https://apps.dtic.mil/sti/trecms/pdf/AD1183514.pdf.

2. Ibid., 2.

3. Joint Chiefs of Staff, Joint Publication (JP) 3-16, *Multinational Operations* (Washington, DC: U.S. GPO, 01 March 2019), I-5. Change 1 was issued 17 June 2024.

4. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. GPO, 01 October 2022), 2-13.

5. Department of the Army, FM 2-0, *Intelligence* (Washington, DC: U.S. GPO, 01 October 2022), xi.

6. Ibid., 2-13.

7. Joint Chiefs of Staff, JP 3-16, *Multinational Operations*, I-1.

8. Department of the Army, FM 3-16, *The Army in Multinational Operations* (Washington, DC: U.S. GPO, 15 July 2024), vii.

9. Joint Chiefs of Staff, JP 3-16, *Multinational Operations*, I-1.

10. Ibid., ix-x.

11. Ibid., II-1.

12. Department of the Army, FM 3-16, *Army in Multinational Operations*, iii-iv.

13. Ibid., 43-45.

14. Ibid., 47-48.

15. Department of the Army, Army Techniques Publication (ATP) 6-02.61, *Expeditionary Mission Partner Network Operations* (Washington, DC: U.S. GPO, 06 December 2023), 1-1.

16. Ibid.

17. Department of the Army, FM 3-16, *Army in Multinational Operations*, 2-2; and Department of the Army, ATP 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. GPO, 10 January 2020), 9-7.

18. Department of the Army, ATP 2-33.4, *Intelligence Analysis*, B-9.

19. Ibid.

20. Ibid., B-7.

21. Ibid.

22. Ibid., B-8.

23. Department of the Army, ATP 3-16.02, *Write for Release* (Washington, DC: U.S. GPO, 26 September 2023), vii.

24. Ibid., 1-2.

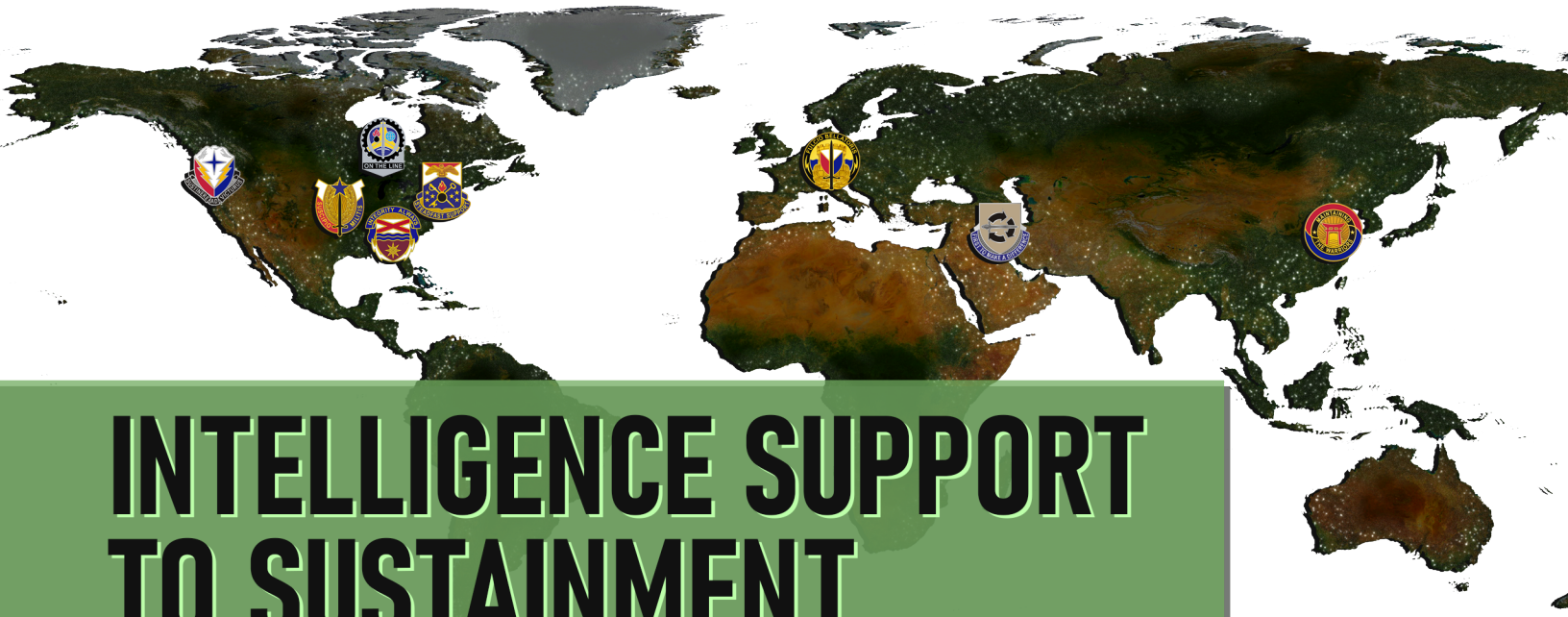
25. Joint Chiefs of Staff, JP 3-16, *Multinational Operations*, VI-3; and Department of the Army, ATP 3-16.02, *Write for Release*, 1-2.

26. Department of the Army, FM 2-0, *Intelligence*, A-6.

27. Ibid.

28. Todd C. Lopez, "Mission Partner Environment Cuts Decision Making, Kill Chain," News, Department of Defense, November 29, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2854238/mission-partner-environment-cuts-decision-making-kill-chain/.

MAJ Ed Pecoraro is the executive officer for the 524th Military Intelligence (MI) Battalion, 501st MI Brigade in Camp Humphreys, Korea. He previously served as the analysis and control element chief for the 2nd Infantry Division/Republic of Korea-U.S. Combined Division (2ID/RUCD) and in multiple intelligence and planning positions at 2ID/RUCD, U.S. Army Cyber Command, 1st Stryker Brigade Combat Team, 25th Infantry Division, and 2nd Brigade Combat Team, 10th Mountain Division (Light Infantry). MAJ Pecoraro holds a master of arts in military operations from the Advanced Military Studies Program at the School of Advanced Military Studies and a master of operation studies from the Command and General Staff Officer Course.



INTELLIGENCE SUPPORT TO SUSTAINMENT

by Lieutenant Colonel Alexander D. Corbin,
Captain Ariel Ayala,
Captain Tyler Eagan,
and Captain John Seman

Introduction

In today's volatile geopolitical climate, it is crucial to emphasize intelligence support for sustainment operations when building partner capacity. In conflict, tactical sustainment elements are likely to be near the front lines, where partners may not have the same level of protection as that provided by large coalition forces. In these circumstances, intelligence analysts use threat reporting to provide sustainment forces with updates necessary to mitigate the threat. Intelligence drives sustainment operations by providing timely and accurate analysis so that sustainment forces can effectively and efficiently reduce risk and increase operational success. Integrating intelligence into sustainment operations is a strategic requirement of today's complex and dynamic geopolitical landscape. Organizations like the U.S. Army Sustainment Command (ASC) have a multi-echeloned perspective on maintaining global situational awareness of impacts on sustainment. Within organizations that are force providers like ASC, intelligence support to sustainment requires situational awareness from the strategic to the tactical level.

ASC, a two-star major subordinate command of U.S. Army Materiel Command, is headquartered at Rock Island Arsenal, Illinois. It is not just a logistics integrator but also manages sustainment operations worldwide. Its global footprint consists of 7 Army field support brigades (AFSBs) in 20-plus countries and 32 states committed to sustaining Army, joint, and multinational forces through adaptive logistics.

The scope and complexity of ASC's responsibility is a testament to its crucial role in global logistics. Field Manual 4-0, *Sustainment Operations*, states:

> ASC integrates and synchronizes the delivery of [U.S. Army Materiel Command] USAMC and materiel enterprise capabilities at echelon from the theater strategic level of warfare to the operational level of warfare. ASC delivers materiel readiness, force generation, and power projection and sets the conditions for future readiness at home station. ASC forward-stationed capabilities provide command and control to all USAMC assets in theater, shape the logistics environment, and help set the theater to accelerate force reception into theater. Deployable logistics support elements (LSEs) provide expeditionary corps and divisions the ability to rapidly integrate into the theater delivery of USAMC capabilities at echelon for responsive support to Soldier priorities....It is responsible for integrating logistics support with strategic partners and links the national sustainment base with the expeditionary Army. Major mission areas include logistics synchronization in support of the Regionally Aligned Readiness and Modernization Model, [Army pre-positioned stocks] APS, materiel management, and the Logistics Civil Augmentation Program (LOGCAP). Mission execution is through a global network of organizations to include the ASC staff, Army field support brigades (AFSBs), Army field support battalions (AFSBns), logistics readiness centers (LRCs), and LSEs embedded at the division and corps levels.[1]

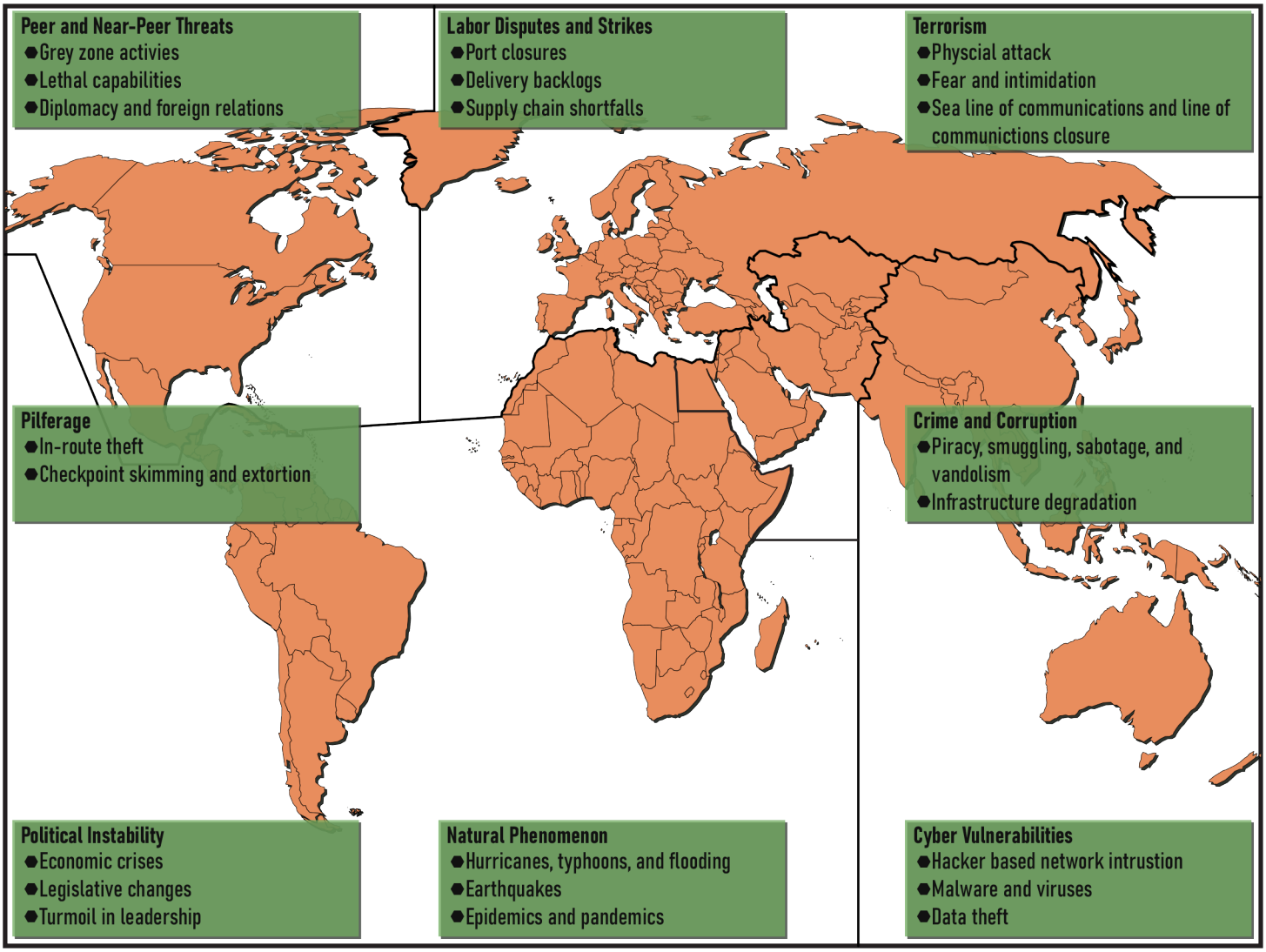


Figure 1. Threats to the Global Sustainment Enterprise

ASC G-2 Intelligence Support Element

With a mission that has global implications, the ASC G-2 intelligence support element provides ASC leadership with insights concerning threats to sustainment operations. Notable threats to the global logistics enterprise *and* ASC operations include near-peer threats (i.e., China, Russia, and Iran), labor disputes and strikes, political instability, and terrorism. For example, increased Chinese aggression since the January 2024 Taiwanese elections could result in new operational requirements for ASC. Furthermore, labor disputes or strikes at notable ports or border crossings can delay vital shipments to the intended recipients, which could impact the sustainment enterprise.

The ASC G-2 intelligence support element provides comprehensive intelligence products, delivering timely, accurate, relevant, and tailored intelligence analysis and assessments to the ASC commanding general, headquarters staff, and subordinate units to mitigate these threats. To aid command decision making, the intelligence support element produces strategic and operational intelligence that addresses both lines of effort and priority intelligence requirements, while prioritizing the most important issues with potential wide-ranging impacts on the sustainment operational environment. These products can include the assessment of critical regional and national actor capabilities, intentions, and strategies, as well as emerging enemy capabilities likely to affect logistics operations, economic stability, and foreign trade and development. The intelligence support element also provides intelligence and threat data supporting the command's antiterrorism, force protection, operational security, and training programs.

The intelligence support element conducts in-depth research and detailed analysis to integrate intelligence from all intelligence community sources. It then meticulously filters the intelligence through a sustainment operations "prism" to prepare its analytical products. The intelligence support element's intelligence production is not focused solely on threats to manning, arming, fueling, maintaining, transporting, and protecting sustainment forces but also emphasizes threats to sustainment operations from the point of embarkation to the point of need, underlining the inherent complexity of their task.

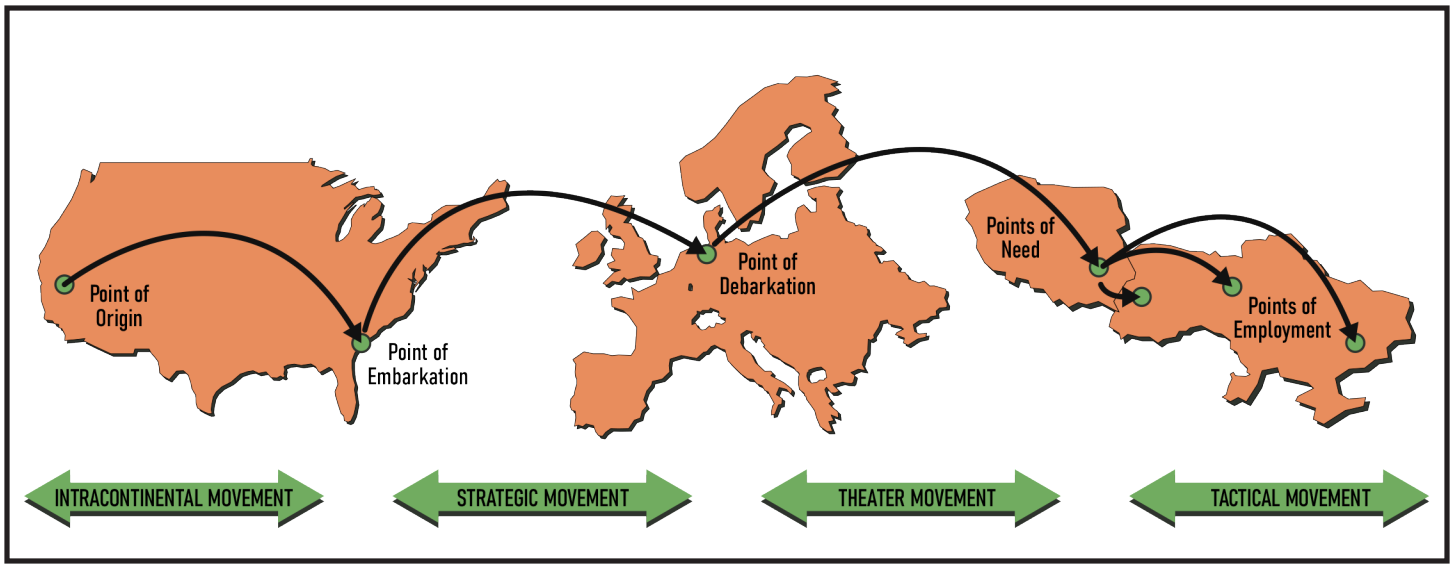


Figure 2. Materiel Distribution System

While not robust in number, the intelligence support element is task-organized to provide global intelligence support. Company-grade officers and noncommissioned officers conduct in-depth analysis of threats to ASC operations within the combatant commands (CCMDs), collaborating with organic sustainment organizations such as theater or expeditionary sustainment commands to provide tailored support for CCMD intelligence analysis. Additionally, the intelligence support element provides intelligence support to ASC plans and operations through daily updates to decision makers on the impact to current operations. This support comes in the form of tailored briefs covering geopolitical effects on current operations and predictive analysis of potential operational requirements that could result in presidential directives for materiel support. The intelligence support element can also provide topographic and terrain analysis support to ASC leaders through its geospatial engineer in the form of maps and graphics.

Intelligence Support to Sustainment

AFSBs have specific mission sets that focus on providing a link between the generating force and the operational force within their assigned areas. AFSBs are also crucial to coordinating strategic capabilities from the Army Materiel Command and the ASC to the operational force while supplying Logistics Civil Augmentation Program (LOGCAP) support throughout all phases of operations.

AFSB S-2s have a unique intelligence mission set as they provide pertinent information to the brigade commander, emphasizing sustainment and power projection. AFSB S-2s must deliver more than the traditional threat action reporting; they also must provide predictive analysis on possible LOGCAP or Army pre-positioned stocks (APS) requirements. The reachback support they receive from the intelligence support element and the S-2's connection with their respective theater or expeditionary sustainment commands enables this analysis. By synchronizing with the theater or expeditionary sustainment commands and ASC, the AFSB S-2s can understand the sustainment picture within their area of responsibility to focus on predictive analysis rather than reactive analysis.

The Power of Open-Source Intelligence

Open-source intelligence (OSINT) has recently become a discipline vital for information and intelligence collection within ASC because it provides opportunities for real-time updates on operational impacts such as maritime traffic, port delays, and rail information. Additionally, due to ASC's unique structure and sizable civilian workforce, most of whom do not have access to classified networks, disseminating analytical products at an unclassified level maximizes the intelligence support to the available audience and allows the intelligence support element to serve most ASC personnel better. Accordingly, the intelligence support element utilizes OSINT in support of sustainment operations in several ways:

- Situational Awareness: Publicly available information and OSINT allow analysts to monitor real-time information. This provides context and a comprehensive understanding of threats to global military logistics.
- Risk Assessment: Publicly available information databases provide information on potential risks to military logistics, allowing ASC to mitigate risk and maintain operational continuity.
- Geopolitical Analysis: Analytical data on international relations, global crises, and regional tensions can inform ASC leaders of potential impacts to military sustainment operations. This analysis is essential for mitigating risk and strategic planning.
- Predictive Analysis: OSINT can provide analysts with historical context and current public sentiment, enabling intelligence professionals to provide predictive analysis on future sustainment support requirements.

As OSINT has become established as an intelligence community discipline, ASC increasingly utilizes it to create daily intelligence products focused on global threats to logistics in the form of a daily intelligence summary and a global update, which the intelligence support element disseminates to over 500 personnel within Army logistics organizations and a myriad of organizations that focus on threats to logistics, including Transportation Command, Development Command, and sister services. Upon establishing its OSINT mission and authorities, ASC broadened its scope of intelligence product dissemination to the greater intelligence community as the only Army organization focused solely on intelligence support to sustainment.

Intelligence Support to the Logistics Civil Augmentation Program

LOGCAP provides sustainment, minor construction, and other services through Army contractor assets to CCMD commanders, joint operations, allies, and federal agencies. Typically, LOGCAP provides tailorable packages of base logistics services in austere or hostile environments with little or no Army support infrastructure to enable military operations. Some previous LOGCAP operations include:

- Base logistics support to the U.S. Central Command in Afghanistan, Iraq, Kuwait, and Saudi Arabia.
- Exercise support to the U.S. Africa Command.
- Mission and installation support to the U.S. European Command.
- Mission and installation support to the U.S. Northern Command at the National Training Center.
- Construction and operations support for five living areas during Operation Allies Welcome, a noncombatant evacuation operation.

The intelligence support element enables LOGCAP operations by providing support through predictive analysis to identify threat activities and trends that could impact the mission. These efforts inform the intelligence products produced for LOGCAP leaders and planners. These products can range from topographic imagery analysis and identification of potential threats to proposed LOGCAP site locations to threat briefs for activated LOGCAP personnel, directly impacting the level of personal protective equipment their mission will require. The intelligence support element additionally supports LOGCAP noncombatant evacuation operations by monitoring indicators for events of unrest or national disasters, thereby providing LOGCAP personnel with indications and warnings to support their preparation, planning, and risk mitigation efforts, ensuring successful operations. Simply put, the intelligence support element provides detailed intelligence support from the strategic to the tactical level, enabling LOGCAP operations to have the greatest impact.

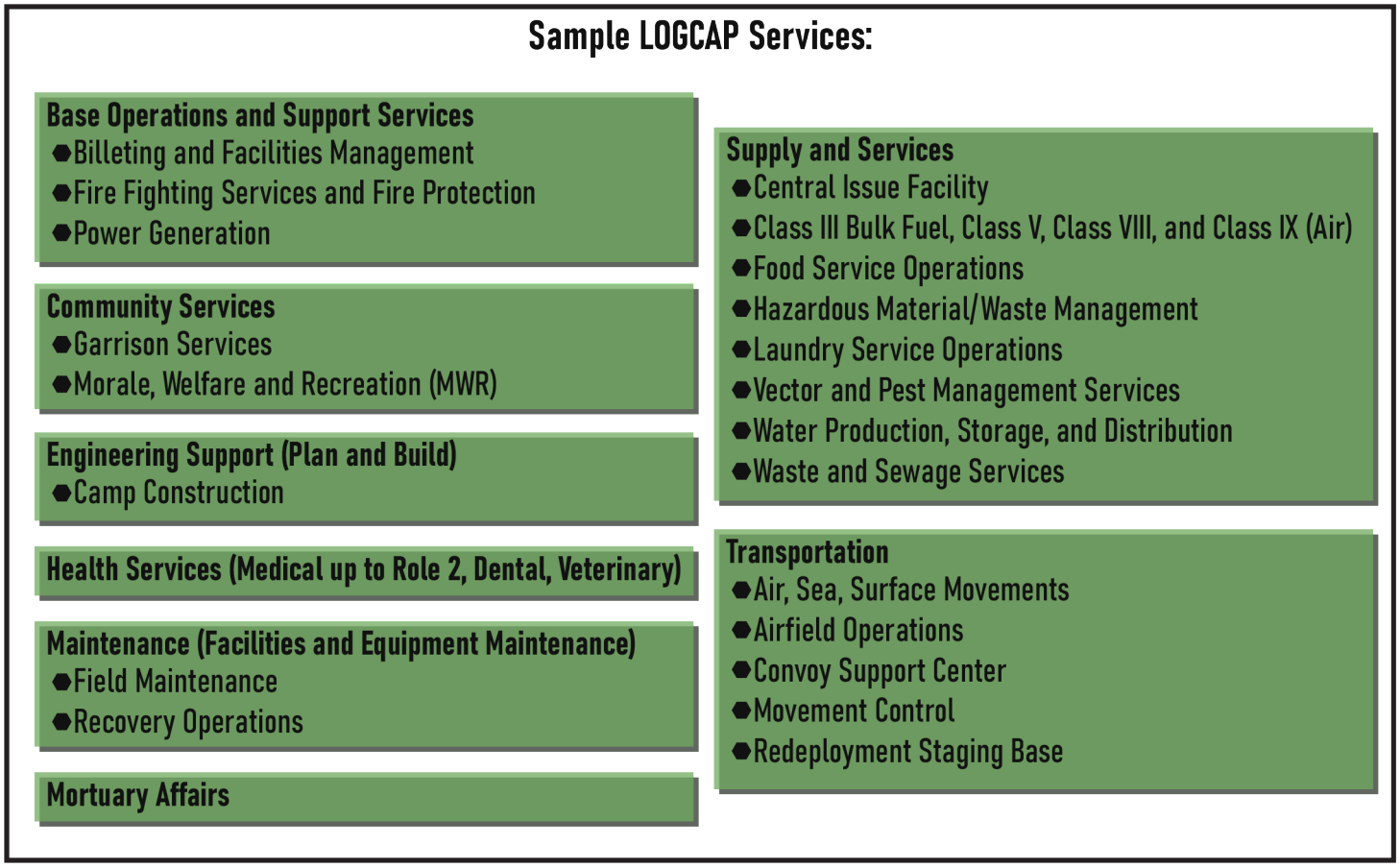


Figure 3. Logistics Civil Augmentation Program Capabilities

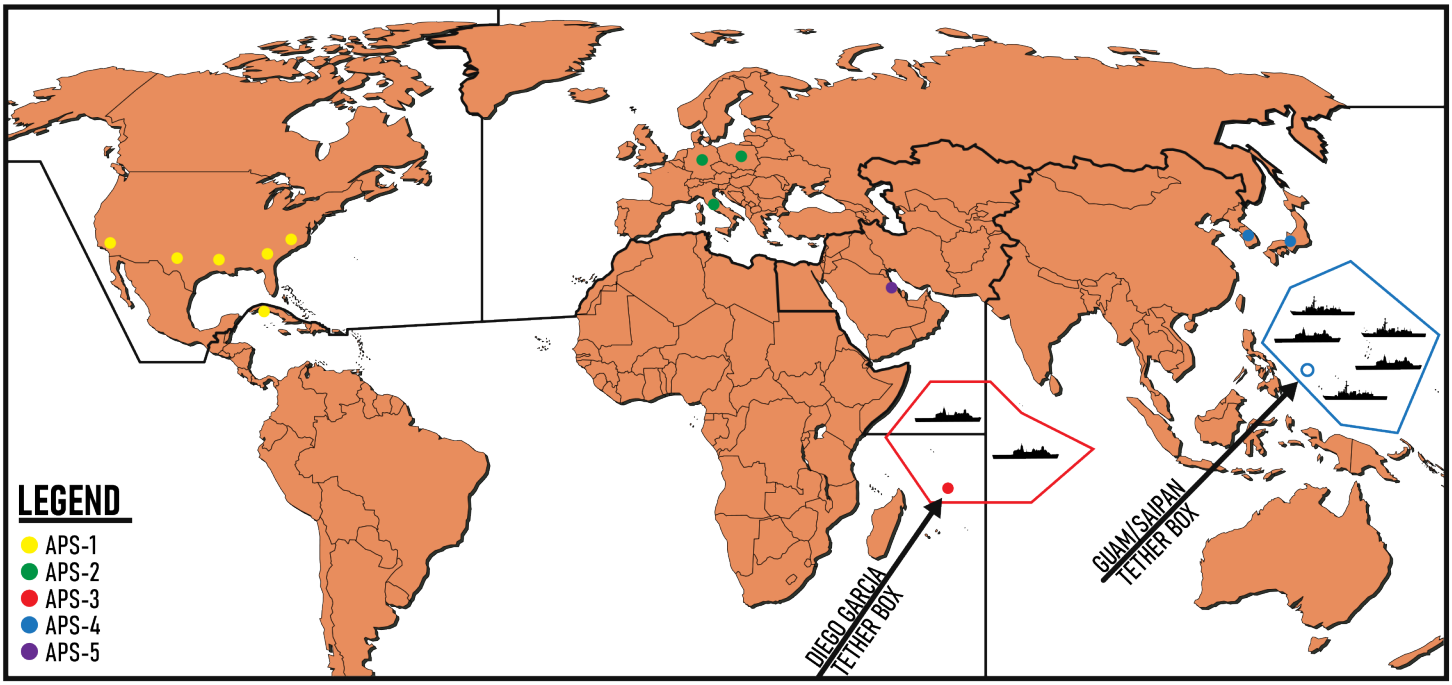


Figure 4. Army Prepositioned Stocks

Army Pre-Positioned Stocks Intelligence Support

APS is an Army program that stores and maintains equipment sets around the globe for use when a CCMD commander requires additional capabilities. These stocks—identified as APS-1 (United States), APS-2 (Europe), APS-3 (Afloat), APS-4 (Northeast Asia), and APS-5 (Southwest Asia)—are available to support all CCMD commanders' missions, not only in contingencies but also for major exercises and humanitarian missions. The sustainment enterprise utilizes exercises such as Operation Pathways (formerly Pacific Pathways) in the U.S. Indo-Pacific Command to test operational and tactical employment of logistics and the use of APS in a large-scale combat operation. This exercise program requires sustainment headquarters, such as the 8th Theater Sustainment Command, to coordinate with multiple AFSBs and the ASC for APS requests and dynamic employment.

The intelligence support element enhances APS operations by delivering tailored intelligence products for each existing and projected APS location and its corresponding AFSB. This ensures that the AFSB, APS, and ASC leadership receive up-to-date threat reports, enabling them to make informed decisions on safeguarding the APS assets. The intelligence support element also provides the ASC leadership with predictive analysis within the individual areas of responsibility, allowing them to anticipate and address emerging APS requirements effectively and efficiently.

Support During a Crisis

With a global response mission, the ASC G-2 maintains situational awareness to provide the most up-to-date information and predictive analysis on global crises. Since Russia began its invasion of Ukraine in February 2022, the United States has issued presidential directives aimed at providing military assistance to Ukraine. The 405th AFSB is critical to this mission because it provides materiel enterprise support to U.S. forces in Europe and Africa.

In support of the 405th AFSB, the ASC G-2 intelligence support element communicated with other intelligence units in the theater, including the U.S. European Command J-2 Joint Analysis Center, the 66th Military Intelligence Brigade (Theater), and the XVIII Airborne Corps G-2, to ensure that commanders at all levels were aware of threats to shipments from the point of embarkation, to the myriad points of debarkation, to the final point of need. Additionally, the dynamic threat environment, coupled with automation and the inception of real-time troubleshooting telemaintenance, required an emphasis on the cyberspace threat to all ASC assets in the theater to identify any potential delay to the requested military assistance. As the conflict in Ukraine continues, the ASC G-2 intelligence support element and the 405th AFSB continue to monitor threats to military aid, ensuring the uninterrupted flow of materiel support to Ukraine.

Conclusion

Through this article, we have offered broad examples of how intelligence professionals support logistics in no small part due to the unique nature of the logistical challenges. Because sustainers must meet the warfighter's needs worldwide, there cannot be a "one size fits all" approach to how the Military Intelligence Corps supports the sustainers. Looking toward tomorrow's fight, the information that logisticians require will undoubtedly become more diverse. As the U.S. military continues its focus on large-scale combat operations, intelligence support to sustainment must meet the increased demand for

relevant and timely intelligence. The emerging requirements may take the form of analyzing sea states for their shipping capacity and capability to load and unload goods, analyzing secondary and tertiary effects of modernized militaries on the battlefield, or monitoring environmental and social threats that could lead to a noncombatant evacuation operation.

The intelligence support provided to the logistics field can take the form of intelligence support for APS, LOGCAP, and interactions with partner nations; however, it is not limited to these topics. We can expect the demand from the sustainment enterprise to increase as warfare continues to evolve. Therefore, in order to enable the sustainment community to guarantee the continuation of force projection and the capacity to "fix forward," the scope and scale of intelligence support to sustainment must expand to provide intelligence from the tactical to the strategic level.

Endnote

1. Department of the Army, Field Manual 4-0, *Sustainment Operations* (Washington, DC: U.S. Government Publishing Office, 14 August 2024), 30.

LTC Alexander Corbin is the Deputy G-2 for the U.S. Army Sustainment Command, Rock Island Arsenal, IL. He previously served as the Director of the Joint Intelligence Support Element, NATO Special Operations Component Command–Afghanistan/Special Operations Joint Task Force–Afghanistan, Bagram Air Base, Afghanistan. He holds a master of science in strategic intelligence from the National Defense Intelligence College and a master of arts in military history (intelligence) from the American Military University.

CPT Ariel Ayala is an intelligence production manager for the U.S. Army Sustainment Command, Rock Island Arsenal, IL. He previously served as an intelligence officer for the 513th Military Intelligence Brigade (Theater), Fort Eisenhower, GA. His deployments include Afghanistan and the U.S. Central Command areas of responsibility, serving as an operational management team officer in charge and horizontal engineer. CPT Ayala holds a master of arts in intelligence and security studies from the Citadel and the open-source intelligence and theater sustainment planner skill identifiers.

CPT Tyler Eagan is an intelligence production manager for the U.S. Army Sustainment Command in Rock Island Arsenal, IL. He previously served as the S-2 for the 401st Army Field Support Brigade at Camp Arifjan, Kuwait. He deployed to the U.S. Central Command area of responsibility, where he supported Operations Inherent Resolve and Spartan Shield.

CPT John Seman serves as the G-2 operations officer for the U.S. Army Sustainment Command, Rock Island Arsenal, IL. He previously served as an assistant professor of military science in the Golden Lions Army Reserve Officers' Training Corps Battalion at California State University, San Bernardino, CA. He deployed to Afghanistan in support of Operation Freedom's Sentinel.

Aerial view of Rock Island Arsenal, IL.

201st Expeditionary-Military Intelligence Brigade and I Corps G-2 Soldiers set up a Temporary Sensitive Compartmented Information Facility perimeter in support of corps intelligence operations for Warfighter 25-02 at Camp Asaka, Japan, November 23, 2024. (Photo by 1SG Olga Kudervayets)

THE EXPEDITIONARY-MILITARY INTELLIGENCE BRIGADE: ENABLING CORPS AND DIVISION LETHALITY

BY COLONEL DAVID C. HAZELTON, MAJOR ROBERT P. REES II AND MAJOR DANIEL R. TUTHILL

"Intelligence drives the conduct of operations and operations enable intelligence, making intelligence and operations inseparable. Additionally, intelligence supports Army leaders in creating complementary and reinforcing effects against enemy formations across all domains."[1] Operational aspects, from competition activities to deployment to lethality and protection during conflict, start with intelligence.

Army doctrine has long recognized several aspects of intelligence that each echelon must account for to provide effective intelligence at and across echelons. For example, in different locations, Field Manual (FM) 2-0, *Intelligence*, discusses the intelligence enterprise, intelligence architecture, intelligence operations, intelligence planning and coordination across echelons, collection management, deployment of intelligence capabilities, and intelligence training. It is easy to list these aspects of intelligence, but to apply them at echelon effectively is complex. Effectively employing these aspects is why the expeditionary-military intelligence brigade (E-MIB), including its headquarters and headquarters company (HHC), is essential to corps and division intelligence.

Corps Intelligence

The corps G-2, aided by the E-MIB, provides intelligence support to its corps headquarters during large-scale combat operations as part of a joint campaign. It must be prepared to support the subordinate two to five divisions of the corps. The corps G-2 manages the integration of joint and multinational intelligence capabilities into the ground operational and tactical fight and coordinates U.S. Intelligence and Security Command and U.S. intelligence community partnerships through the theater army G-2 and military intelligence (MI) brigade-theater.[2]

"To create unity of effort, the corps G-2 and E-MIB must collaborate to—

- Effectively execute intelligence activities.
- Continuously and mutually support intelligence training to create cohesion across the [echelons corps and below] ECB intelligence warfighting function.
- Routinely integrate higher-level augmentation, including joint and multinational intelligence elements.
- Task-organize intelligence capacity to subordinate divisions and units according to the corps commander's intent.
- Sustain intelligence activities across multiple command nodes to support the corps commander's decision making, targeting, and other staff processes."[3]

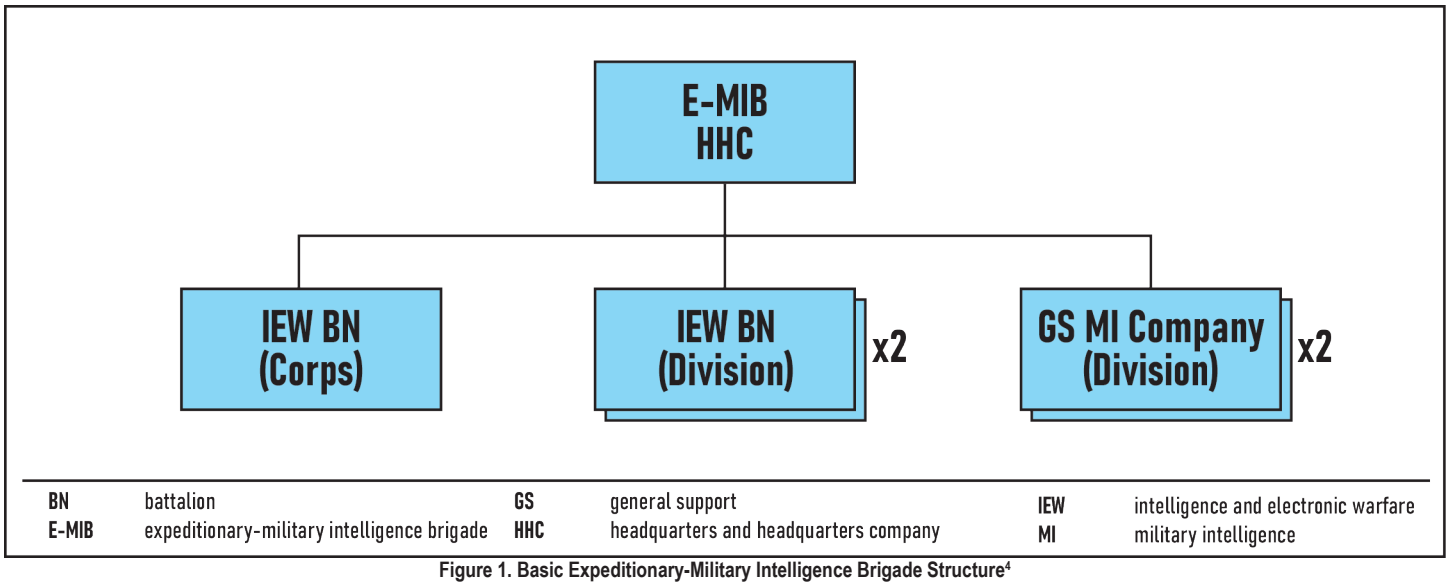


Figure 1. Basic Expeditionary-Military Intelligence Brigade Structure[4]

The Expeditionary-Military Intelligence Brigade and Its Headquarters and Headquarters Company

The E-MIB is the primary MI unit assigned to the corps; the E-MIB commander is the principal advisor to the corps commander and works with the G-2 to execute intelligence operations. E-MIBs conduct multidiscipline intelligence operations to support the corps and subordinate divisions. Each E-MIB has collection capabilities that include open-source intelligence (OSINT) teams, signals intelligence (SIGINT) collection teams, counterintelligence (CI) teams, and human intelligence (HUMINT) collection teams. Additionally, the E-MIB assists the corps G-2 in planning and executing the intelligence task organization of assigned and attached intelligence elements, including support to divisions and select brigade combat teams. Figure 1 shows the basic structure of the E-MIB.

There is a unique relationship between each echelon's G-2/S-2 and the MI unit. In general, the G-2/S-2 synchronizes and fights the intelligence warfighting function under the commander's direction. At the same time, the MI unit conducts intelligence operations using the operations process, like any other unit, based on that unit's mission.[5] However, the role of the E-MIB and E-MIB HHC is different than the role of other MI units because the E-MIB is comprised of a mix of subordinate MI units: an intelligence and electronic warfare (IEW) battalion (corps) that also supports the corps, and an IEW battalion (division) or general support (GS) MI company that supports each division.

So, given that the E-MIB comprises an IEW battalion (corps) and IEW battalions (division) and/or GS MI companies, what is the role of the E-MIB HHC? The quick answer is that the E-MIB HHC is designed to receive, integrate, employ, and sustain organic and supporting intelligence enterprise elements and allocate capabilities across the corps according to the G-2's concept of intelligence. However, the roles of the E-MIB commander and HHC are far more extensive, as illustrated in Figure 2 (on the next page). Figure 2 groups the roles into those conducted to support intelligence training, those performed during operations across the strategic contexts (competition, crisis, and conflict), and those designed to help transition corps intelligence to the Army of the future. It is important to understand that the corps G-2 staff is not resourced to perform these functions, and the corps and division warfighting function would be severely challenged to function effectively without the E-MIB HHC.

The 201st Expeditionary-Military Intelligence Brigade's Experiences and Deep Sensing

Over the past several years, I Corps and the 201st E-MIB have grappled with the role of the E-MIB and E-MIB HHC. The results of past and ongoing planning, exercises, and operations are exciting. Some of the most exciting I Corps intelligence advancements center on what HHC, 201st E-MIB has learned about planning and executing the reception and integration of external units and capabilities.

A key capability of the E-MIB is to see and sense beyond the divisions to enable corps shaping and situational awareness. Apart from the corps combat aviation brigade, there are no organic intelligence, surveillance, and reconnaissance (ISR) platforms that a corps can task to conduct collection operations beyond its subordinate divisions. How then does the E-MIB conduct collection operations for the corps area of operations that extends beyond the reach of its organic collection capabilities? A corps must rely on requests for theater, joint, or national intelligence assets to answer its priority intelligence requirements, support targeting, conduct battle damage assessments, and provide situational understanding. E-MIB HHC requests for higher-level intelligence are clearly integral to operating as a joint force and conducting multidomain operations; however, wholesale reliance on external

Training

- Technical review authority for subordinate intelligence units to include certification, training, control, and oversight necessary to access CSA and IC information, systems, and databases for mission execution.
- Aligns standard Army training with corps and division commander priorities and the IC technical certifications.
- Provides, manages, and maintains multi-enclave access to intelligence assets and networked capabilities, ensuring equipment readiness and Soldier training/certification for maintenance, administration, and systems integration.

Intelligence Across the Strategic Contexts

- Provides the corps with a senior field grade intelligence commander for legal oversight and to make sensitive risk decisions while performing intelligence operations in competition, crisis, and conflict.
- Executes RSOI, mission integration, and C2 of theater intelligence forces on the corps commander's behalf.
- Supports G-2 adjustments to the ECB intelligence architecture and PED execution.
- Orchestrates and certifies multi-echelon, multidiscipline intelligence operations from brigade-level to corps/JTF-level; repositions assets across the AO/AOR as directed by the corps commander.
- Conducts mission management/collection operations management for specialized intelligence collection/activities (TECHINT, CI, HUMINT) assets and teams.
- Performs intelligence overwatch as corps elements deploy into theater during competition and crisis.
- Conducts IEW systems maintenance, logistics, and sustainment.

Army of the Future

- Integrates modernized and emerging intelligence systems and capabilities into the corps intelligence architecture.

AO/AOR	area of operations/area of responsibility	**ECB**	echelons corps and below	**JTF**	joint task force
C2	command and control	**HUMINT**	human intelligence	**PED**	processing, exploitation, and dissemination
CI	counterintelligence	**IC**	intelligence community	**RSOI**	reception, staging, onward movement, and integration
CSA	combat support agency	**IEW**	intelligence and electronic warfare	**TECHINT**	technical intelligence

Figure 2. Expeditionary-Military Intelligence Brigade Headquarters and Headquarters Company Roles[6]

requests does not offer the same flexibility, reliability, or consistency that tasking organic capabilities provide. LTG Xavier Brunson, former I Corps Commander, alluded to this during a U.S. Senate Hearing on 17 September 2024:

> "Senator, I think space can do a great many things for us . . . but as the Army has learned over time, there's a need for a little bit more granularity than the bigger platforms of days gone by . . . I know that we're achieving great, great results as we continue to campaign through the Pacific and Operation Pathways by using small aperture, UAS [unmanned aircraft systems] quadcopters and the like to be able to provide the granularity needed to finish actions. The find and the fix can be done by larger assets, but when it comes time to finish, which is the aim of our operations, when we're on the ground, it takes something a little bit smaller."[7]

According to FM 2-0, "a corps usually receives reinforcing capabilities and units from theater army, joint, or multinational echelons to conduct operations."[8] Because of their limited organic capabilities, corps require this external augmentation to close the deep sensing gap. A corps furnished with enablers to close the deep sensing gap must have the capability to plan, command and control, and integrate the operations of the reinforcing units. The corps G-2 generally does not have the operational or administrative capacity to provide the command and control necessary for newly aligned units; this is where the E-MIB HHC steps in.[9]

Request for Forces–A Solid Technique

Since 2022, I Corps has experimented with placing various external enablers and Reserve MI units under the 201st E-MIB during Operation Pathways' campaigning operations through a request for forces (RFF). An RFF is a formal request made by a military command, and typically, it is submitted when the current units assigned cannot meet a requirement for additional forces or resources.[10] In this case, the external resources temporarily provided necessary collection capabilities to conduct deep sensing across the I Corps area of operations. With these resources allocated, the 201st E-MIB trained on its mission of providing deep sensing to I Corps. This experiment created a symbiotic dependency between the 201st E-MIB HHC and the I Corps G-2 (and other I Corps staff) in which the G-2 focused on developing the collection requirements for the corps, freeing up the 201st E-MIB to plan and execute the collection operations. This actualized the corps G-2 and E-MIB responsibilities advocated by the U.S. Army Intelligence Center of Excellence (USAICoE) in its 2024 white paper *How to Fight Army 2030 Echelons Corps and Below (ECB) Intelligence:* "The corps G-2 is responsible for allocating intelligence forces across ECB [echelons corps and below] and delegating intelligence authorities."[11] and "The E-MIB is designed to receive, integrate, employ, and sustain external intelligence enterprise capabilities."[12]

Before the RFF supplied more enablers, the 201st E-MIB primarily provided intelligence uplift to the G-2 by offering capabilities such as OSINT, SIGINT, and processing, exploitation, and dissemination (PED) teams. The collection resources assigned to the E-MIB provided minimal deep sensing for I Corps, consisting only of HUMINT teams, CI teams, and a

limited number of Prophet-based SIGINT teams. Under this model, the primary value of the E-MIB to the corps lay in its capacity to contribute additional personnel as a force provider to the G-2 section.

Since 2022, the 201st E-MIB's support to the I Corps G-2 evolved from a force provider to a capability provider, generating a more flexible, responsive, and efficient use of intelligence assets. The 201st E-MIB organized itself to provide essential collection functions associated with command and control over the ISR resources externally allotted to I Corps. The 201st E-MIB provides trained and ready capabilities to the I Corps G-2, including collection operations management, ISR operations, ISR assessments, PED, multidomain operations targeting support, and battle damage assessment teams for integration throughout I Corps.

The E-MIB must be ready to receive, optimally employ, and sustain each intelligence asset provided to the corps.[13] The 201st E-MIB partners with multiple organizations to build the processes, expertise, and training that produce the capabilities to support the I Corps collection enterprise and properly execute the RFF for additional intelligence capability. To leverage the aligned resources of the I Corps intelligence warfighting function, the 201st E-MIB HHC organized an ISR Academy. This forum invites trainers from external units (such as the 116th MI Brigade [Aerial Intelligence], 5th Battlefield Coordination Detachment, 1st Air Support Operations Group [Air Force], and 1st Multi-Domain Task Force) to familiarize and educate 201st E-MIB personnel and other I Corps units' S-2s and G-2s on the subjects of their collection capabilities, structure, and processes.

Additionally, the 201st E-MIB routinely trains in partnership with the 373rd Expeditionary MI Battalion (Army Reserve) to operate consistent with expectations for large-scale combat operations. Proliferating intelligence knowledge and expertise before any potential conflict is a vital function of the E-MIB that impacts units across the corps. Understanding how to fight for intelligence before the fight begins is essential to the adage "training as you fight".

Theory Applied: Warfighter Exercise 25-02

During I Corps many iterations of Operation Pathways, the 201st E-MIB validated the key function of integrating external intelligence units. During its Warfighter Exercise 25-02 (WFX 25-02), I Corps took this training to the next level by integrating externally allocated units: the Army Reserve's 373rd Expeditionary MI Battalion, an aerial exploitation battalion, and an electronic warfare company. (See Figure 3.)

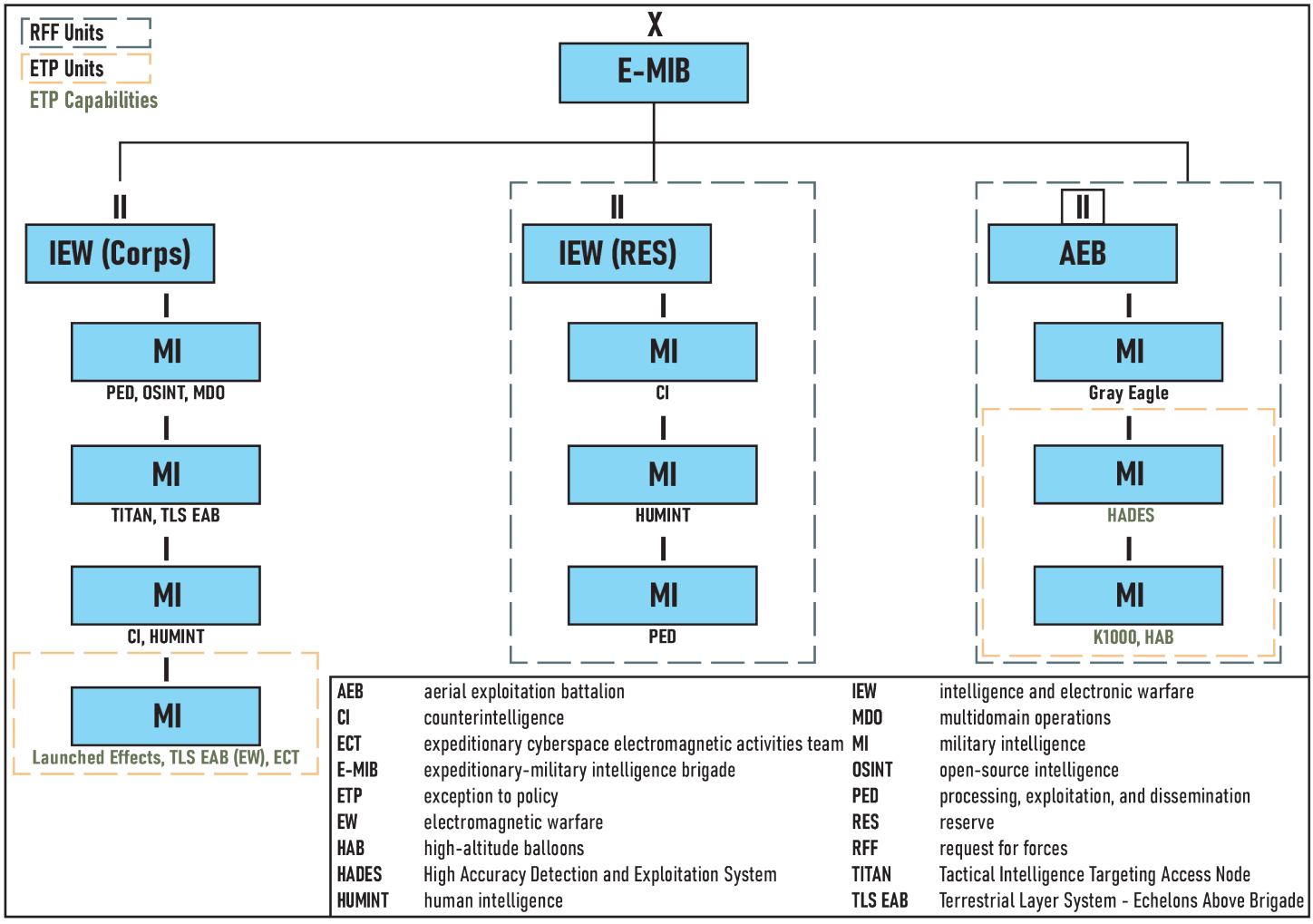


Figure 3. Proposed Expeditionary-Military Intelligence Brigade Task Organization Concept[14]

Object in the top left is a stationary Gray Eagle Extended Range (GE-ER), top right shows a High Accuracy Detection and Exploitation System (HADES) concept image, bottom left is a high-altitude Balloon (HAB), and bottom right shows a Kraus 1000 (K1000) in flight. (U.S. Army photos)

By augmenting the organic collection capabilities of the E-MIB (i.e., OSINT, SIGINT, HUMINT, and CI), I Corps is rehearsing the concept of using the 201st E-MIB as the primary integrator of externally aligned intelligence assets as crises escalate into armed conflict. These external assets are more than a "warfighter dream sheet" of capabilities; they manifest the requirements of the corps to see and sense beyond divisions during large-scale combat operations. Focusing on the E-MIB's responsibility to integrate external intelligence assets has enabled I Corps with a capability to find, fix, and finish its high-payoff targets, answer its priority intelligence requirements, and provide situational awareness. This deliberate approach to integrating external assets is how I Corps can operate as a tactical corps. It is charged not just with situational awareness but also with the capabilities to fulfill its purpose in decisively completing the kill chain.

In the lead-up to WFX 25-02, I Corps submitted exceptions to policy to outfit the requested aerial exploitation battalion with both existing and future exquisite capabilities. This strikes a deliberate balance between how the E-MIB conducts collection with existing Army inventory and how it conducts training with assets that are in development. These capabilities included:

- GE-ER (Gray Eagle Extended Range).[15]
- Kraus 1000 (K1000).[16]
- High Accuracy Detection and Exploitation System (HADES).[17]
- High-Altitude Balloon (HAB).[18]

Using a mix of existing and future capabilities trains the E-MIB to employ the tools it has today as it prepares to integrate new sensors and platforms as they reach maturity. Operationally employing these future capabilities and educating the corps on their use is challenging for the E-MIB. By leveraging the 201st E-MIB as the primary integrator, the doctrinal and organizational aspects of the new equipment are advanced, and I Corps is better able to rehearse its wartime role of sensing and shaping.

Expeditionary-Military Intelligence Brigade Headquarters and Headquarters Company and Collection Management

The 201st E-MIB's trained and ready capabilities work with the I Corps G-2 and take a central role in enabling the corps collection enterprise. The 201st S-2 is charged with collection operations management—turning the G-2's collection requirements into an operational activity—and spearheads this critical integration with the I Corps G-2. USAICOE's 2024 white paper makes note of this G-2/MI Commander balance: "The G-2/S-2 synchronizes and fights the intelligence warfighting function."[19] and "The MI unit commander is the chief of intelligence operations."[20] The E-MIB has the inherent responsibility to conduct intelligence collection operations that fulfill the requirements specified by the G-2 on behalf of the corps. The white paper hints at this tenuous balance: "The corps G-2 and E-MIB must collaborate to effectively execute intelligence activities . . . [and] task-organize intelligence capacity."[21] This dependency between the G-2 and MI command cannot be superficial: collection assets are limited, and bottom-up refinement is essential to best achieve the corps' requirements for situational awareness, targeting, and battle damage assessment.

Conclusion

The E-MIB is not only the primary source of collection assets for a corps and division, but the E-MIB HHC also plays a pivotal role in enabling deep sensing. Without external augmentation, the E-MIB cannot fully achieve its purpose of deep sensing to find, fix, and finish the enemy. Any corps operationally employed with an assigned area of operations will require collection capability commensurate with that responsibility.[22] External enablers will be critical to providing a corps with the ability to find, fix, and, most importantly, finish its targets.

The E-MIB HHC plays a critical role in the planning, reception, and integration of allocated external assets, enabling the corps to see beyond the divisions' area of operations and achieve effects. These external enabler units and capabilities will vary based on the specific mission of a corps and

the nature of the conflict. However, this ambiguity should spur the E-MIB to train more, not less, on the critical task of integration. Only then can the E-MIB fulfill its role of supporting a corps during large-scale combat operations. E-MIBs must prioritize continuous training and experimentation with various non-organic capabilities that will enable their corps to fight and win during large-scale combat operations. With this mentality, the E-MIB can "train as you fight" at the corps level of warfare.

Endnotes

1. Army Training and Doctrine Command, Army Intelligence Center of Excellence, *White Paper: How to Fight Army 2030 Echelons Corps and Below (ECB) Intelligence* (Fort Huachuca, AZ: U.S. Army Intelligence Center of Excellence, 10 August 2024), 2.

2. Ibid., 9.

3. Ibid.

4. Graphic adapted from Army Intelligence Center of Excellence, MI Pub 2-19.40 *Transforming Division Intelligence* (draft publication, 2025).

5. *How to Fight Army 2030*, 5.

6. Graphic derived from Colonel Rachel Sarles, Forces Command Deputy Chief of Staff G-2, email message to Ms. Beth Leeder, U.S. Army Intelligence Center of Excellence Director of Training and Doctrine, January 6, 2025. The email discusses LTG Anthony Hale's talking points to describe the role and benefits of an expeditionary-military intelligence brigade headquarters.

7. *Nomination Hearing of Lieutenant General Randall Reed, USAF, to be General and Commander, United States Transportation Command and Lieutenant General Xavier T. Brunson, USA, to Be General and Commander, United Nations Command/Combined Forces Command/United States Forces Korea, Before the Senate Committee on Armed Services*, 118th Cong. 53-54 (2024) (statement of Xavier T. Brunson, LTG, U.S. Army). https://www.armed-services.senate.gov/imo/media/doc/nomination_hearing.pdf.

8. Department of the Army, Field Manual (FM) 2-0, *Intelligence* (Washington, DC: Government Publishing Office [GPO], 01 October 2023), 7-16.

9. Department of the Army, Army Techniques Publication 2-19.3, *Corps and Division Intelligence Techniques* (Washington, DC: U.S. GPO, March 2023), 2-5; and *How to Fight Army 2030*, 9-10.

10. Office of the Chairman of the Joint Chiefs of Staff, Chairman of the Joint Chiefs of Staff Instruction 4310.01F, *Logistics Planning Guidance for Pre-Positioned War Reserve Materiel* (Washington, DC: The Joint Staff, 29 August 2022), B-8. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%204310.01E.pdf.

11. *How to Fight Army 2030*, 11.

12. Ibid., 10.

13. Ibid.

14. Graphic adapted from author's original.

15. "Gray Eagle Extended Range (GE-ER)," General Atomics Aeronautical, 2024, https://www.ga-asi.com/remotely-piloted-aircraft/gray-eagle-extended-range.

16. "Kraus Hamdani Aerospace Wins Contract to Provide the U.S. Navy with Its First Electric VTOL Unmanned Aerial System (UAS)," European Defence Review On-Line, April 04, 2024, https://www.edrmagazine.eu/kraus-hamdani-aerospace-wins-contract-to-provide-the-u-s-navy-with-its-first-electric-vtol-unmanned-aerial-system-uas.

17. Army Public Affairs, "Army Selects Sierra Nevada Corporation as Lead System Integrator for its High Accuracy Detection and Exploitation System," U.S. Army Website, August 22, 2024, https://www.army.mil/article/279124/.

18. *High Altitude (HA) Fact Sheet* (Huntsville, AL: U.S. Army Space and Missile Defense Command, 2023), https://www.smdc.army.mil/Portals/38/Documents/Publications/Fact_Sheets/HA.pdf.

19. *How to Fight Army 2030*, 3.

20. Ibid.

21. Ibid., 9.

22. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. GPO, 01 October 2022), 1-17, 2-2, 2-19, 4-19, 5-14, 6-38, 6-48.

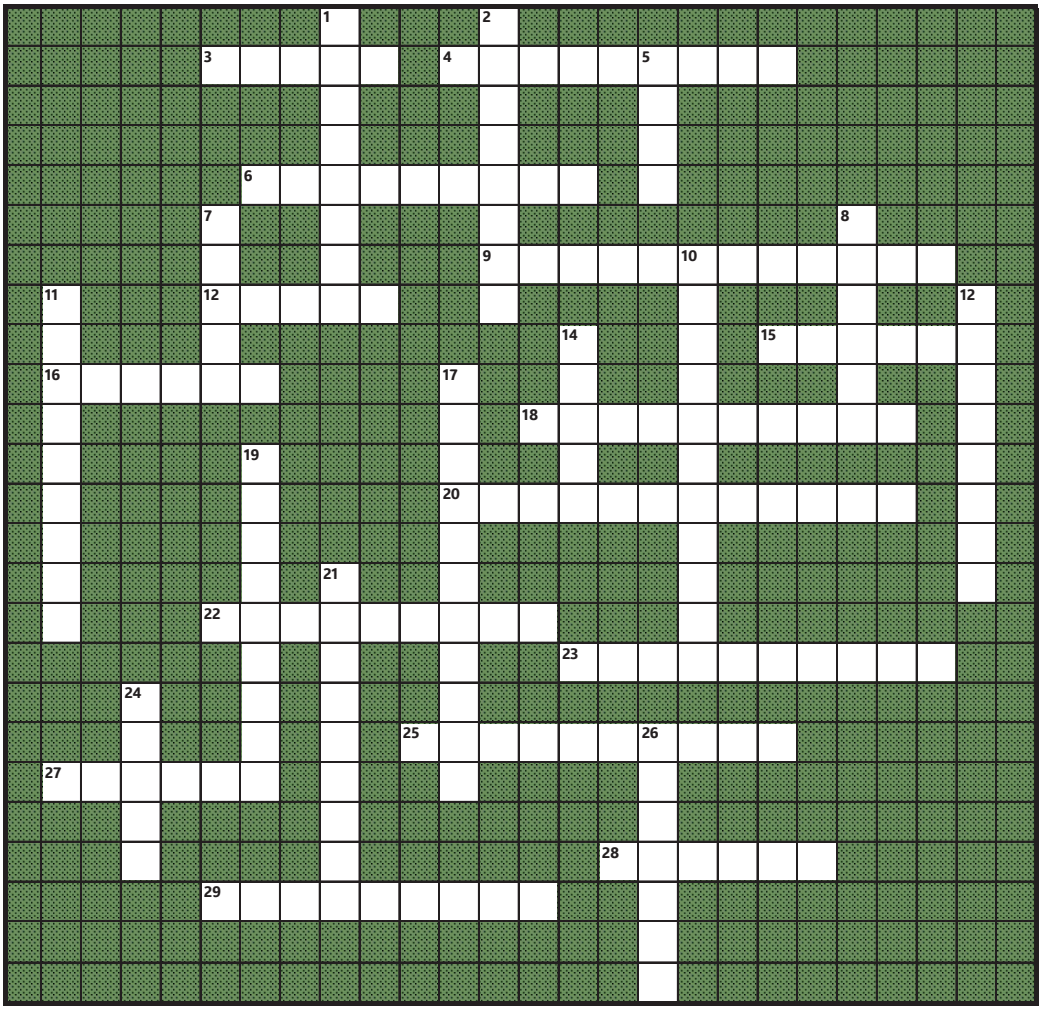
COL David C. Hazelton is the 201st Expeditionary-Military Intelligence Brigade (E-MIB) Commander. His earlier assignments include 403rd Military Intelligence (MI) Detachment Commander, 532nd MI Battalion Commander, Special Operations Command-Korea executive officer, 501st MI Brigade S-3, 8th Army ACE Chief, 4th Stryker Brigade S-2, and two years with NATO/SHAPE in the J-2. COL Hazelton deployed to Afghanistan in support of Operation Enduring Freedom. He holds a bachelor of arts in political science from the U.S. Military Academy, master's degrees from the University of Maryland, the National Intelligence University, the Command and General Staff College, and the Army War College, and a doctorate from North Central University.

MAJ Robert P. Rees II is the 201st E-MIB S-2 and collection operations manager. MAJ Rees's previous assignments include 201st E-MIB deputy operations officer, S-2 for 2nd Battalion, 2nd Infantry Regiment, 3rd Infantry Brigade Combat Team, 1st Infantry Division, 513th MI Brigade-Theater's Theater Ground Intelligence Center Company Commander, 311th MI Battalion assistant S-3, 2nd Battalion 35th Infantry Regiment, 3rd Infantry Brigade Combat Team, 25th Infantry Division battalion S-2, and 5th Battlefield Coordination Detachment Ground Liaison Officer. MAJ Rees holds a bachelor of arts in criminal justice from Eastern Kentucky University, a master of arts in intelligence studies from American Military University, and a master's degree in operational studies from Command and General Staff College.

MAJ Daniel R. Tuthill is the 502nd Intelligence and Electronic Warfare Battalion (Corps) S-3. He previously served as the I Corps collection manager. MAJ Tuthill's other assignments include Commander of the MI company at 1st Special Forces Group (A), 4th Battalion, 160th Special Operations Aviation Regiment (Airborne) S-2, and multiple jobs within 2nd Brigade Combat Team, 101st Airborne Division (Air Assault). He is an alum of the Junior Officer Cryptologic Career Program and has deployed numerous times in support of combat operations worldwide. MAJ Tuthill holds a bachelor of arts in supply chain management from Michigan State University, a master of professional studies in cybersecurity risk management from Georgetown University, and a master's in operational studies from the Command and General Staff College.

THE MI CROSSWORD

World War II Edition



ACROSS:

3. Acronym for the forces of the Australia-New Zealand Army Corps
4. The German Air Force
6. Nickname given to the A-bomb dropped over Hiroshima (two words)
9. The U.S. program to rebuild devastated countries post-war (two words)
12. To add territory to a state or country, often by threat or intimidation
15. Name of the machine used by Germany to encrypt comms
12. The provision of logistics and services necessary to maintain operations until successful completion of the mission
16. Site of the first major U.S. victory against Japan, universally considered the "turning point" in the war in the Pacific
18. Germany's code name for its invasion of the U.S.S.R. in 1941
20. Nickname for the insignia worn on Soldiers' uniforms designating them as recently separated from active service (two words)
22. A program of materiel assistance to allies that allowed the U.S. to remain neutral early in the war (two words)
23. A sudden, overwhelming attack, meaning "lightning war" in German
25. Hawaiian pidgin phrase that was the motto of the 442nd RCT (three words)
27. German word for a fast-moving armored tank
28. Meaning "to live 10,000 years," this was the Japanese battle cry
29. The Army of Germany

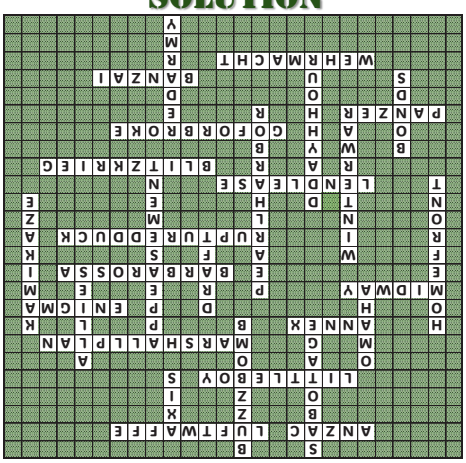
DOWN:

1. To deliberately destroy or damage something
2. British nickname for Germany's V-1 rocket (two words)
5. The "bad guy" alliance of Germany, Italy, and Japan
7. Code name for one of the Normandy beaches secured by the U.S. on D-Day
8. the "good guy" coalition, led by the U.S., Britain, and the U.S.S.R.

DOWN (cont.):

10. The policy of making concessions to an enemy to forestall violence
11. Americans of all ages contributing to the war effort in their local communities (two words)
13. Japanese for "divine wind," it was an aircraft on a suicide mission
14. The system used to select citizens for mandatory military service
19. The Russo-Finnish conflict that predicated Finland's entry into WWII as a German ally (two words)
21. The specific time the Normandy invasion began (four words)
24. Americans were encouraged to buy these to finance the war effort
26. The Soviet armed forces (two words)

SOLUTION



(Image created by DALL-E)

Harnessing SIGINT and EW for Tactical Dominance: A Guide for Combat Arms Leaders

Major General Rick Appelhans and Major General Ryan Janovic

Editor's Note: This article is reprinted with permission from* Infantry*, the professional journal of the U.S. Army Infantry School, Maneuver Center of Excellence, Fort Benning, Georgia. It appears in their Summer 2025 issue. The article has been modified to match MIPB's style and format.

Introduction

To the combat arms platoon leader and company commander: You are leading formations that will close with and destroy the enemy. Your ability to shoot, move, communicate, and then move again (see later section on countering enemy surveillance in the electromagnetic spectrum) is paramount to our success on the modern battlefield. The enemy is sophisticated, adaptive, and aggressively contesting your ability to maneuver in all domains, including the electromagnetic spectrum (EMS). You are not alone in this fight; the intelligence and cyber communities will enable you to dominate the EMS. These communities stand ready to provide you with actionable targets and the means to influence/dominate the EMS at echelon. This is not theory; this is the reality of combat against peer and near-peer adversaries, and we are bringing the full weight of the Department of Defense (DoD) and its combat support agencies to bear. Your S-2 section and Cyber Electromagnetic Warfare Activities (CEMA) cell will innovate at speed across the range of operations to ensure that you have the capabilities necessary to win.

SIGINT and EW: Your Tactical Edge

Signals intelligence (SIGINT) and electromagnetic warfare (EW) are distinct but complementary disciplines that must be integrated effectively to maximize battlefield effects. SIGINT identifies and characterizes enemy signals, providing critical intelligence that inform EW operations. EW teams can use that information to help locate enemy positions for destruction, or simply to disrupt, deceive, or deny the adversary's use of the electromagnetic spectrum. Proper coordination between SIGINT and EW enables deception operations, enhances precision targeting, and strengthens force protection measures, ensuring that friendly forces maintain dominance over the EMS while denying the enemy key capabilities.

Based on historical analysis of large-scale combat operations (LSCO), recent lessons learned from Ukraine, and predictive analysis of China's People's Liberation Army (PLA) capabilities, the teaming of SIGINT and EW can be a force multiplier across the warfighting functions. By integrating SIGINT-derived intelligence with EW's ability to deny and disrupt, we can significantly degrade an adversary's ability to maneuver and execute multidomain operations (MDO).

Understanding SIGINT in Your Fight. SIGINT is not just a tool for strategic planners in some far-off headquarters. It is a tactical enabler that allows you to detect, locate, and exploit enemy communications in real time. Whether you are setting up an ambush, planning a fire mission, or maneuvering to secure a key objective, SIGINT can provide the enemy's disposition, intent, and vulnerabilities. The Army's ability to identify and track enemy command nodes, air defense systems, and maneuver elements through SIGINT means you can strike at the right place and time with overwhelming force.

How EW Shapes the Battlefield. EW is your ability to seize control of the EMS. EW is the counterweight to enemy SIGINT and can greatly affect their ability to execute command and control (C2) while disrupting their ability to communicate, navigate, and coordinate. If the enemy cannot receive orders, they cannot react. If their targeting systems are blinded, they cannot fire effectively. Ultimately, if they can't navigate, they cannot effectively maneuver forces on the battlefield. EW, when employed effectively, can have significant battlefield effects, all without firing a shot.

EW's Three Essential Functions:

Electromagnetic Support (ES): Detecting and identifying enemy emitters to support targeting and situational awareness.

Electromagnetic Attack (EA): Jamming and deception operations that deny the enemy use of the spectrum.

Electromagnetic Protection (EP): Ensuring that friendly forces maintain reliable communications despite enemy jamming, to include employment of emission control measures (e.g., radio power, antenna placement, etc.) to defeat enemy attempts to surveil and target friendly forces.

The Critical Role of SIGINT and EW in Tactical Operations

The operational environment requires agility, synchronization, and unity of effort to converge all sensors and effects on a rapidly evolving threat. The ability to integrate SIGINT with EW at the tactical level allows commanders to enhance targeting fidelity (SIGINT and EW), disrupt adversary operations (EW), and provide real-time intelligence for maneuver forces (SIGINT).

To focus on C2 and counter-C2, expanded maneuver, and cross-domain fires, we must team SIGINT and EW across EA, ES, and EP to present multiple dilemmas to our enemy, enhance C2 protection, and increase lethality. Let's look at an example:

Kill Chain Analysis: A Counter-Unmanned Aerial System (C-UAS) Scenario. In an era where UAS play an increasingly critical role in modern warfare, understanding the full kill chain process for countering these threats is essential for operational success.

Phase 1: Detect and Identify. A brigade combat team (BCT) is executing a deliberate attack when SIGINT elements intercept and transcribe enemy communications emanating from an urban area associated with drone activity. Electromagnetic support reporting from sensors riding on a remote-controlled scouting vehicle confirms the presence of enemy UAS operating frequencies, geolocating multiple launch sites and relay nodes.

Phase 2: Target and Disrupt. Upon confirming the threat, the BCT's organic EW platoon, using Terrestrial Layer System (TLS) Manpacks, receives the locations of the threat signals of interest (SOI), and executes an electromagnetic attack to jam the drone's control frequencies, disrupting the operator's ability to maneuver the UAS effectively. Simultaneously, SIGINT analysts coordinating with higher-echelon intelligence teams pinpoint the drone operator's location for kinetic targeting.

Phase 3: Engage and Destroy. With the drone rendered ineffective, the fire support element coordinates an artillery strike on the enemy UAS ground control station, leveraging the precision geolocation refined by enhanced tools like the Electromagnetic Warfare Planning and Management Tool (EWPMT) and the Army Intelligence Data Platform (AIDP). Simultaneously, the EW platoon continues to jam the enemy's communications, preventing coordinated support or retrograde. Friendly forces neutralize the threat, allowing maneuver elements to proceed unimpeded.

Phase 4: Assess and Adapt. Post-strike analysis from SIGINT utilizing High Altitude Platform (HAP) sensors reveals ongoing enemy attempts to reestablish drone operations, underscoring the necessity for sustained EA efforts. In response, SIGINT teams disseminate updated threat reporting to the EW platoon, enabling them to adjust jamming frequencies and counter enemy adaptations. Concurrently, SIGINT elements refine their intelligence collection to anticipate and prepare for potential future enemy tactics, ensuring proactive EW measures.

This coordinated SIGINT and EW kill chain ensures the enemy's UAS capability is neutralized before it can affect friendly operations. This vignette effectively illustrates the critical synergy between intelligence-driven targeting and spectrum dominance.

How You Can Leverage SIGINT and EW at Your Level

To gain a decisive battlefield advantage, leaders must integrate SIGINT and EW capabilities to counter enemy threats in the EMS. The following approaches can help achieve this:

Incorporate SIGINT and EW into the DNA of Your Planning and Execution. From the outset, consider how to effectively integrate these capabilities into your operations to inform and shape your decision-making. Collaborate closely with

supporting staff elements, such as the BCT CEMA cell and S-2 section, to gain a deep understanding of the enemy's electromagnetic spectrum usage and identify opportunities to disrupt and exploit their vulnerabilities. By incorporating SIGINT and EW into your operational framework, you can create a more comprehensive and effective approach to achieving your mission objectives.

Train Your Leaders and Soldiers to Recognize and Exploit the EMS. Your Soldiers must understand that controlling the EMS is just as vital as controlling key terrain. Integrate SIGINT and EW considerations into your battle drills, mission rehearsals, and after-action reviews. Units that fail to account for enemy EW will put their formations at significant risk on the battlefields of the future. Training ensures you can adapt and maintain tempo under contested conditions.

SIGINT and EW teams can sense across the EMS with ES at the tactical edge. By developing new tactics, techniques, and procedures (TTPs), SIGINT support from higher echelons, such as from the division level, can be pushed down to BCTs, providing real-time EMS sensing without burdening them with protecting and maneuvering higher-echelon intelligence capabilities. Ultimately, this enables more agile and lethal maneuver forces.

Ensure Interoperability with Supporting SIGINT and EW Units. SIGINT and EW units are enablers, not afterthoughts. Integration of SIGINT and EW elements throughout the organic targeting process is key. Work with them to refine target identification and EA options. Develop unit standard operating procedures (SOPs) that detail how to request and synchronize their capabilities in real-time engagements and incorporate them in all rehearsals. Leaders must ensure that EW Soldiers are embedded within tactical formations to provide immediate effects that enhance maneuver and fires.

Adopt an Aggressive, Learning-Focused Mindset. The enemy is adapting. As such, we must do the same. Stay informed on the latest TTPs by leveraging resources such as the Center for Army Lessons Learned (CALL) and current doctrinal publications like Field Manual (FM) 2-0, *Intelligence*, and FM 3-12, *Cyberspace Operations and Electromagnetic Warfare*. We must continue to share lessons learned across our formations and with intelligence and EW enablers to continually refine our operational effectiveness.

Conclusion

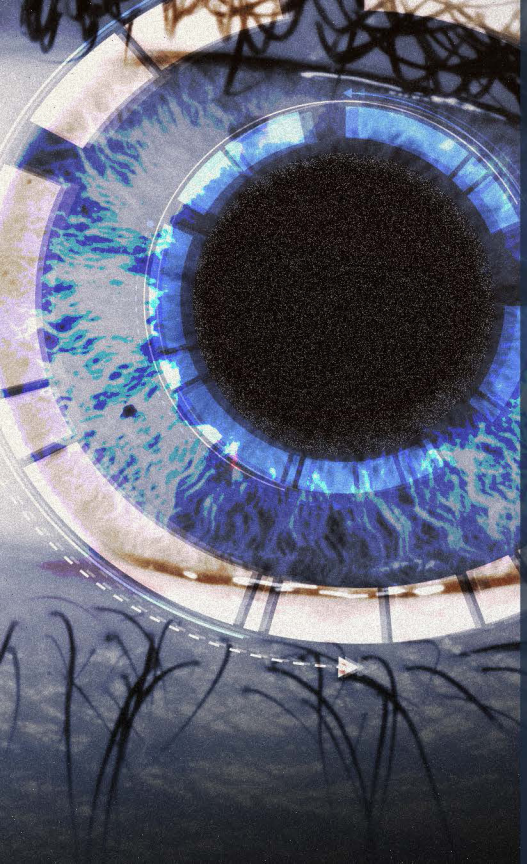
In an era where the electromagnetic spectrum is as contested as the physical battlespace, success demands leaders fully integrate SIGINT and EW into their tactical decision-making. These are not ancillary capabilities but core enablers of maneuver, fires, and protection. By treating SIGINT and EW as an integral piece of battlefield operations rather than separate support functions, we can outthink, outmaneuver, and overwhelm our adversaries before they can react.

The future fight will be won by those who master the integration of intelligence and electromagnetic warfare, seamlessly fusing these disciplines into their formations and operational planning. This requires continuous learning, rigorous training, and adaptive thinking to counter evolving enemy tactics. The intelligence and EW communities stand ready to support, provide counsel for our specialties, and execute through our commanders' intent.

Superiority in the EMS is not an option — it is a necessity. By embracing these capabilities and fostering interoperability, we ensure that our forces maintain a lethal edge on the battlefield. The challenge is clear, and the tools are at hand. Now is the time to educate our leaders and Soldiers and incorporate these capabilities into our training so we are prepared to fight and win our nation's wars.

MG Richard T. "Rick" Appelhans currently serves as the commanding general of the U.S. Army Intelligence Center of Excellence and Fort Huachuca, AZ. Prior to assuming this position, he served as the director of Intelligence, U.S. Forces Korea/deputy director of Intelligence, Combined Forces Command. MG Appelhans' overseas assignments and deployments include the Republic of Korea, Kuwait, Germany, the Netherlands, Afghanistan, Bosnia-Herzegovina, and Iraq. He began his military career as an Armor officer, serving as a tank platoon leader, company executive officer, and battalion S-4. Since transitioning to Military Intelligence in 1997, MG Appelhans has served in a variety of command and staff assignments to include detachment commander, battalion S-2, company commander, brigade combat team S-2, analysis and control element chief, region commander, division G-2, and group commander.

MG Ryan Janovic currently serves as the commanding general of the U.S. Army Cyber Center of Excellence and Fort Eisenhower, GA. A native of Akron, OH, he graduated from the U.S. Military Academy at West Point, NY, in 1993 and commissioned into the Military Intelligence Corps. He served with Multi-National Forces-Iraq, 1st Infantry Division in eastern Afghanistan, Military Intelligence in Korea, and later with Commander United Nations Command/Combined Forces Command/U.S. Forces Korea. His other assignments include various posts throughout the U.S. to include a tour as a White House Fellow. In 2019, MG Janovic joined the cyber ranks as the deputy commander of Joint Force Headquarters – Cyber (Army), leading the organization toward unit citations earned in support of U.S. Central Command.



Modernizing Intelligence Operations in Africa: Enhancing the Intelligence Process Through Data Science

by Colonel Chris Tomlinson,
Chief Warrant Officer 3 Felix Rodriguez Faica,
Chief Warrant Officer 2 Ryan Harvey,
and Mr. Keith Hickman

Introduction

The U.S. Army Intelligence and Security Enterprise and other members of the greater intelligence community are not immune from the often-repeated paradigm of rapidly increasing data and emerging technologies producing more information than can be accurately processed and understood. The Department of Defense Data Strategy recognizes the need for a systemic approach to attain analytic maturity to gain information superiority, highlighting the need for "data at speed and scale for operational advantage and increased efficiency."[1] The Army Africa Data Science Center's (ADSC's) application of data science methodologies and technologies has modernized the U.S. Army Southern European Task Force, Africa (SETAF-AF) G-2's ability to analyze and process vast amounts of data. By taking a deliberate, proactive approach to integrating artificial intelligence (AI) and machine learning (ML) and by incorporating data science and engineering (DS&E) to target this information explosion, ADSC provides a problem-solving approach focused on capturing efficiencies in the intelligence process. Using ADSC as a case study, this article illuminates the increasingly pivotal role DS&E plays in enhancing the intelligence warfighting function throughout the U.S. Africa Command (USAFRICOM) area of responsibility (AOR).

ADSC's mission is to provide customized AI and ML capabilities that enable intelligence analysts to answer SETAF-AF and USAFRICOM priority intelligence requirements (PIRs) more efficiently and effectively.[2] This is especially vital in a resource-constrained theater. ADSC accomplishes this in four ways:

- Focusing on improving data literacy across the force, which supports Army Data Plan 2022 and highlights the urgent need for a data-literate workforce.
- Leveraging the geographic expertise of theater-embedded engineers.
- Co-locating DS&E teams directly with intelligence analysts.
- Building modern analytical products and automation on government-furnished cloud technology.[3]

Through a combination of analysis and vignettes, this article highlights what four years of experiential learning have shown: that integrated DS&E teams can have a transformative impact on intelligence operations in the African theater and, by extension, other theaters. These efforts enable intelligence analysts to produce more comprehensive and timely intelligence products, ultimately increasing the commander's decision advantage.

A Foundation of Data Literacy

According to the U.S. Bureau of Labor Statistics, future demand for data-literate workers will increase in every sector of the economy, led by increasing adoption of complex data solutions and infrastructure in fields such as healthcare, finance, transportation, and utilities.[4] These civilian sectors seek to exploit the transformative potential of advanced analytic techniques to achieve better results, including improved patient outcomes, fraud detection, and traffic and safety optimization, while maximizing security to address growing cyber threats.[5] Ensuring a data-literate workforce is essential to achieving these benefits because these industries

will continue to evolve and become more overtly data-centric. Developing this skilled workforce requires an effort from the whole organization. Senior leaders must understand and leverage organizational data capabilities and requirements, analysts must ask more complex questions, and data teams must build solutions that support this model.

These same considerations apply equally in a military context. With the exponential growth of information accessible across all classification levels, military intelligence professionals find it increasingly difficult to triage vast amounts of data to respond promptly to PIRs. Concepts such as pattern recognition, anomaly detection, and predictive modeling are all viable approaches to solving these problems, and they all require a data-literate organization.[6] Nevertheless, there are many pitfalls along the path to organizational analytical maturity. According to the Army Data Plan of 2022:

> *The Army is increasing data literacy across Soldiers and civilians. . . . However, to increase change at scale, the Army needs to increase the basic data skills for generalists that benefit from greater accessibility to quality data to improve daily decisions, that is,* ***citizen analysts benefiting from our data democracy****.*[7]

Data literacy can be acquired in several ways, all entailing individual intellectual curiosity and perseverance. This can be encouraged across the Service through a combination of institutional, operational, and self-development opportunities following the Army training domain framework.[8] ADSC's efforts to improve data literacy within the SETAF-AF intelligence enterprise will fundamentally reshape how intelligence analysts think about the ways data supports the intelligence process. This evolution will improve the quality of intelligence products the intelligence warfighting function provides commanders and staffs to enhance situational awareness and maximize decision space for military operations.

ADSC leads and develops in-person courses and regularly works with analysts and leaders on complex data projects to rapidly improve unit, team, and individual data literacy. Incorporating the recommendations in this article will enable units to field data-centric teams at the appropriate echelon to meet their force data literacy goals.

Data Science and Engineering Structural Best Practices

Incorporating DS&E capabilities into an intelligence organization can increase the efficiency of processes that identify threats, assess risks, and inform decisions in real time while parsing quantities of information that would otherwise be insurmountable. However, achieving these lofty ambitions requires the adoption of specific principles to maximize efficiency and effectiveness, including co-locating developers with analysts and developing regional expertise. Experiential learning with ADSC has identified a "hub-and-spoke" model as the preferred structure to achieve these goals.

Co-location is vital to effective collaboration. A major advantage of the ADSC structure lies in the physical co-location of engineers with analysts. In the private sector, companies allocate billions of dollars annually toward market research to build a deeper understanding of consumer preferences and requirements, thereby maximizing their profit potential by accurately addressing their customers' needs. In software development, this often entails identifying a precise problem (i.e., the consumer requirement) and providing an effective solution that saves time or resources and improves workflow efficiency. Similarly, eliminating the divide between the intelligence analyst (i.e., the consumer) and the data scientist improves the ability to identify, refine, and prioritize requirements while shortening the time needed to develop and implement technical solutions. The Department of Defense and the intelligence community are uniquely situated to position DS&E teams alongside users.

Augmenting the nuanced depth of knowledge provided by intelligence professionals with a niche technical capability allows for quick prototyping of effective and efficient analytic solutions to meet a commander's evolving requirements while eliminating communication barriers. For this reason, DS&E teams need to be managed and staffed at the most tactical echelon possible, with support from and reachback to higher echelons.

Regional expertise generates effective analytic solutions. In addition to the efficiency benefits realized by co-locating DS&E teams with analysts and leaders, regional expertise is critical for effective data solutions. Every command faces a unique challenge presented by its distinctive geography and mission focus that requires time to develop domain understanding and expertise. For instance, some simplified examples of this complex problem include: USAFRICOM units often monitor instability ahead of potential crisis support operations, U.S. European Command and U.S. Indo-Pacific Command units narrowly focus on strategic competition, while U.S. Southern Command units tackle issues like human and drug trafficking. The datasets needed to answer questions based on these discrete missions are often very different, as are the applications built on those datasets. For instance, consider an analytical tool that gives insight into how a commander's PIRs are being answered. Nearly everything in this tool will be different from one command to the next, including the PIR, workflow, information presentation, etc. Additionally, intelligence enterprise datasets are tightly controlled, while operational domain information, such as human resources or logistics, may have different rules and applications.

ADSC acts as an intelligence multiplier by applying data engineering and automation techniques to quickly aggregate and identify valuable information,[9] in a meaningful way for SETAF-AF G-2 personnel. This capability is extremely valuable in a resource-limited and restricted collection environment.

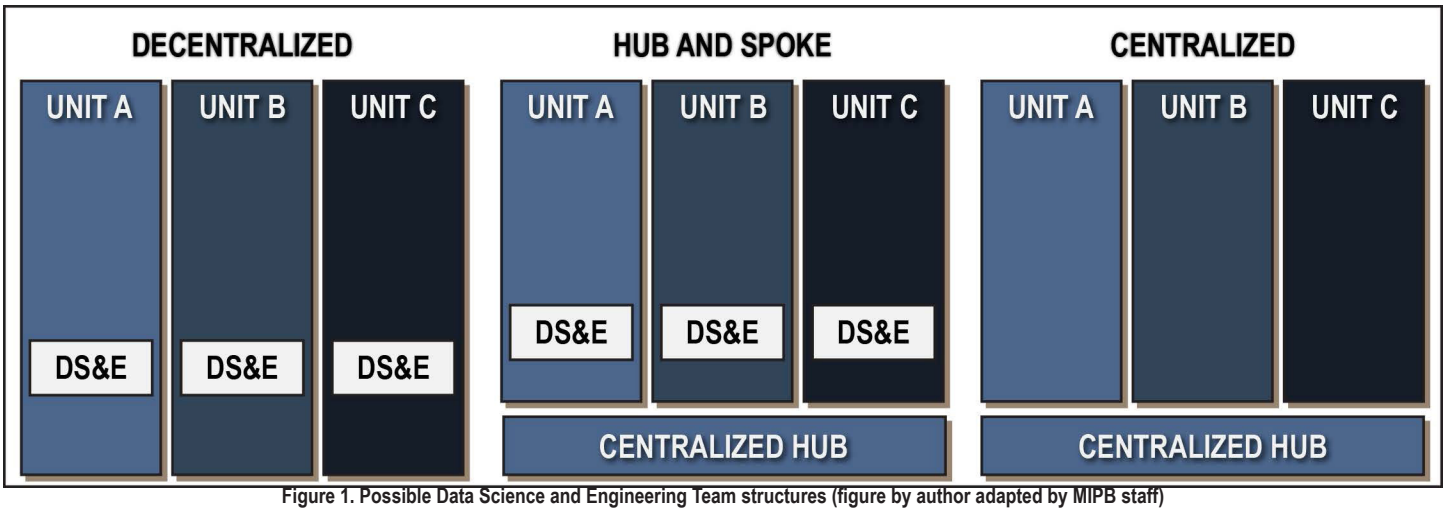


Figure 1. Possible Data Science and Engineering Team structures (figure by author adapted by MIPB staff)

Identified benefits support a hub-and-spoke model. Organizations scaling their data capabilities need technical reachback. Technical support provided at higher echelons substantially reduces the time spent on tasks common to all DS&E teams, including setting up infrastructure, finding development resources, streamlining collaborative projects, and implementing project management practices. This structure is often referred to as a hub-and-spoke model.[10] One hub may serve several embedded teams or "spokes." For instance, a central hub at a joint combatant command might support DS&E teams embedded in several service component commands. A hub might consist of a core group of data engineers and software developers, while a spoke refers to a supported theater-embedded data team such as the ADSC. A hub's primary concern is enabling embedded data teams by providing technical infrastructure and reachback, whereas a spoke directly answers RFIs from units. Compare this model with other configurations (see Figure 1). Centralized DS&E models might hold all data resources in a single space removed from users and, therefore, suffer from a lack of regional expertise. Further, the value proposition of a centralized DS&E team vanishes when considering the need to train, familiarize, and integrate with new commands instead of having organic teams in place. A decentralized model might be efficient but suffers from stovepiping and a lack of central support. ADSC has informally implemented a hub-and-spoke model by building relationships with other command DS&Es, U.S. Army Intelligence and Security Command, and various technical teams across the intelligence community.

The value of data science and engineering with applications and use case. Many companies seek the transformative power of advanced analytic techniques to optimize profits, service levels, and physical or digital products. Even cursory research finds myriad examples of DS&E applications and use cases across every industry sector. Use cases refer to specific data science techniques such as pattern recognition, anomaly detection, and predictive modeling.[11] Example applications include anomaly detection to improve cancer detection methods in healthcare, pattern recognition to detect fraud in finance, and traffic and safety optimization systems for government entities.[12] In addition to increasing efficiency and productivity, these initiatives must also maximize security to address growing cyber threats while incorporating ethical decision-making practices.[13] These and many other applications and use cases apply equally across the intelligence warfighting function. DS&E teams such as ADSC are experts in developing and deploying advanced applications.

Case Study One: Forecasting Violent Extremist Organization Activity in West Africa

One of the main concerns for the SETAF-AF G-2 analysis and control element (ACE) is providing indications and warnings of threats to U.S. forces and equities in Africa. Among the most persistent of these threats are violent extremist organizations (VEOs)—a significant issue across the USAFRICOM AOR, especially in West Africa. Until 2023, the prevailing methodology for conducting indications and warnings assessments was a manual, PowerPoint-based workflow, relying on analysts to interpret large clusters of dots on a map subjectively over long time horizons (see Figure 2 on the next page). Moreover, the inability to achieve the necessary granularity with the available data requires assessing areas prone to VEO presence or expansion at the country or regional level.

Due to the lack of objectivity and granularity within this antiquated methodology, the utility of these assessments was limited. For instance, the efficacy of security cooperation initiatives would noticeably increase if the supporting analysis were to more narrowly identify areas of greatest need, down to specific towns or checkpoints. Likewise, force protection measures can be tailored to a small area if clear trends and reliable forecasts exist for threats in that area.

Approach. In February 2023, senior analysts in the SETAF-AF ACE decided to implement a data-driven analysis of the VEO problem in West Africa. Relying on the unclassified armed conflict location and event data dataset as a suitable proxy for VEO events, ADSC and ACE analysts quantified VEO-related

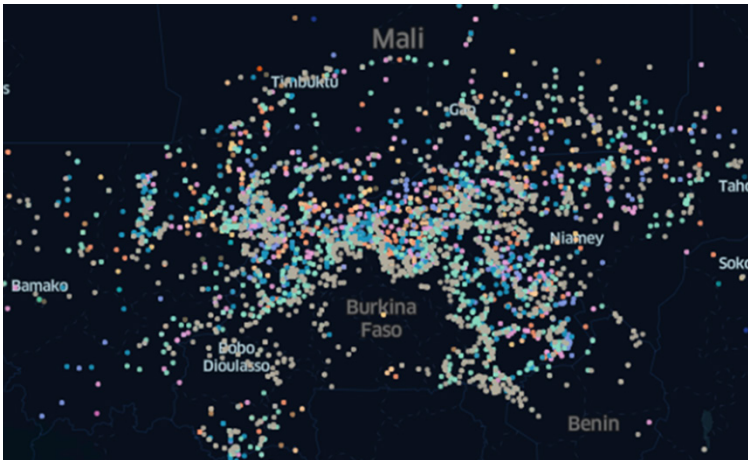


Figure 2. Armed conflict location and event data representation of violent extremist organization activity in West Africa (figure by author)

events to develop narrowly defined geographic forecasts by replicating scientific methods based on AI and ML techniques. Applying the strategies discussed by Andre Python et al. in their 2021 *Science Advances* article, ADSC developed a technique to forecast VEO weekly operational activity by location up to 16 weeks in the future.[14] The underlying location layers are represented by 50-kilometer by 50-kilometer squares published by the Peace Research Institute of Oslo, designed to capture demographic, environmental, and economic information about the squares.[15]

Result. SETAF-AF ACE analysts and ADSC produced a graphical product that forecasts VEO activity at a granular spatiotemporal level to an extent previously impossible with qualitative and subjective methods (see Figure 3). In addition to providing planning and operational support, this product is designed to support a commander's decision-making process for short- and long-term force protection and security cooperation activities. Notably, the product does not replace human-level judgment and only bolsters the qualitative understanding of a given threat assessment.

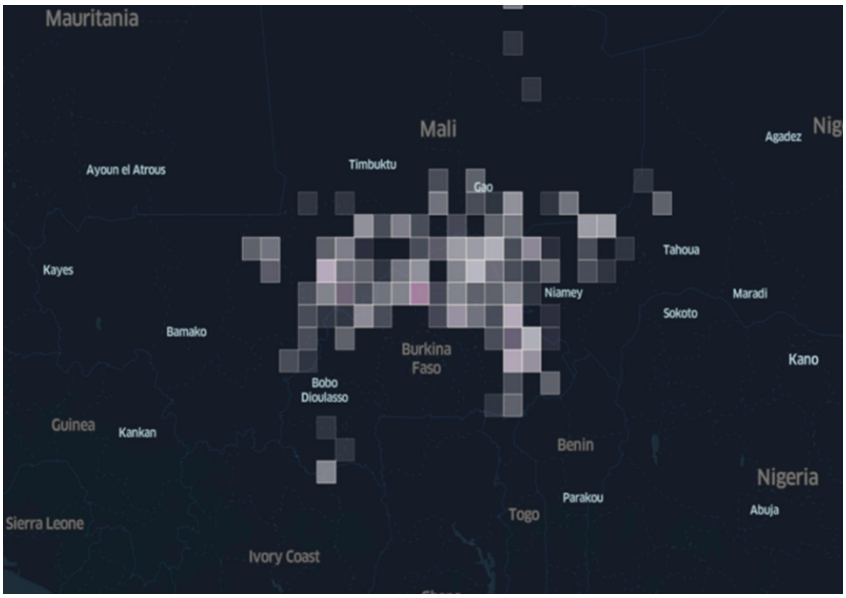


Figure 3. 16-week forecasted violent extremist organization activity on a Peace Research Institute of Oslo grid square (figure by author)

Lesson Learned:

- *Product integration is important.* Data analytics or AI and ML products must be intentionally integrated with existing processes and products, or they will have limited utility and reach. This is vital for new products, such as forecasts.
- *The analyst drives the process.* While the technical product is undoubtedly central to the effort, it can only reflect the analyst's understanding, input, and articulated requirements. Therefore, interaction between the DS&E team and the analyst must happen early and often, which is only possible through co-location, integration, and shared understanding of workflows. If products are intended to support multiple organizations or echelons, stakeholders from all parties should be involved early during requirements generation to maximize applicability.

Case Study Two: Multiple Intelligence Discipline Crisis Support Dashboard

During a recent crisis response operation, SETAF-AF geospatial intelligence analysts monitored hundreds of kilometers of road networks for potential evacuation disruption events, including checkpoints, mobility limitations, and VEO threats.

Approach. After observing several existing workflows, ADSC data scientists embedded with the SETAF-AF analysts identified potential automation projects. ADSC developed Python scripts that emulated keyword and geospatial queries across several intelligence data sources and automatically displayed relevant data in a dashboard. Analysts further requested that the tool provide customized email alerts for all pertinent activity observations. ADSC programmatically overlaid the road networks with a grid system filtering mechanism that displayed activity occurring within five kilometers of areas of interest and provided significant time savings compared to manual monitoring.

Results. This project ultimately achieved three results: cognitive burden shift, error reduction, and information gain. The product shifts the cognitive burden of rote and repetitive data tasks from analysts to computers. The ADSC can write programs that process very large datasets quickly in a meaningful way for ACE analysts, thereby allowing them to focus on critical analysis. Automated scripts like these have the built-in benefit of error reduction because machines process data precisely according to their instructions. Finally, the information gained from seeing many disparate datasets displayed together, such as merging data from multiple sensors or data from multiple intelligence disciplines, is invaluable, though difficult to measure.

Challenges to Adoption

While ADSC continues to demonstrate its value as a force multiplier for the SETAF-AF intelligence enterprise, several constraints have slowed the broader adoption of its technology-based approach and stymied some projects that ADSC has spearheaded.

The greatest challenge comes in educating members of any organization, including analysts and leadership, on the true capabilities that DS&E teams offer and how to use them most effectively. Without education to overcome this challenge, requirements will be either too simple, thus wasting their unique skillset, or too difficult to accomplish, resulting in hours wasted on projects that the team knew would likely never bear fruit. Ultimately, this is not a question of revolutionizing processes. Instead, it is a matter of developing systematic efficiencies that generate results within already adopted practices. Although there has been some resistance to adopting this approach, ADSC offers cutting-edge solutions that can help overcome generational data- and computer-literacy deficits. Within SETAF-AF, increased exposure to ADSC's capabilities across the staff, complemented by a thorough requirements management process, has already started alleviating some of the problems posed by this challenge. Participation in capabilities briefs and support to projects outside the G-2 are good starting points, though support and investment across the command will ultimately be necessary.

Another challenge DS&E entities operating within a Department of Defense construct face is the difficulty of integrating traditional data science tools and platforms into programs of record. These are often specialized commercial off-the-shelf programs with outdated custom modifications and scripting, including security parameters preventing linkages to many external repositories. While acknowledging the legitimate security concerns that inform many of these roadblocks, a commitment to adaptability and modernization through the iterative implementation of DS&E best practices is essential to ensuring the Army retains an advantage over strategic competitors.

Finally, the limited period of analysts' assignment creates an inherent inability to train large numbers of Servicemembers to execute data science tasks proficiently at the unit level. We must therefore rely on contract mechanisms with high costs and uncertain long-term program funding. While this has been a challenge to expanding the ADSC, some benefits will emerge as data scientists continue to deepen their understanding of the problems unique to the USAFRICOM AOR and leverage their depth of knowledge and established automations to present a degree of continuity.

Conclusion

In recent years, incorporating DS&E teams has fundamentally transformed Army intelligence. DS&E encompasses diverse methodologies and technologies to extract valuable insights from vast and varied datasets. Data science has revolutionized how we collect, analyze, and process information by harnessing techniques such as ML, predictive analytics, and geospatial intelligence analysis.

Overall, DS&E teams play a vital role in enhancing intelligence analysis for U.S. Army Soldiers by leveraging advanced analytics, predictive modeling, visualization tools, and automation. By integrating these capabilities into intelligence operations, Soldiers can gain a deeper understanding of the operational environment to produce timely intelligence products that better inform decision makers to achieve mission success.

As the U.S. Army navigates the constantly evolving security landscape of the USAFRICOM AOR, it is imperative to capitalize on the opportunities presented by integrating data science into our established intelligence procedures to stay ahead of emerging threats and challenges. This approach enhances operational effectiveness and increases the efficiency of intelligence procedures. Robust intelligence capabilities remain vitally important in the dynamic and complex operating environment of the USAFRICOM AOR. From countering terrorism and insurgency to addressing regional conflicts and strategic competitors, effective intelligence is paramount for mission success in the USAFRICOM AOR.

Endnotes

1. Department of Defense, *DoD Data Strategy*, October 8, 2020, 2, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

2. Efficiency refers to how quickly a task can be achieved. Effectiveness refers to impact—how much information was gained, how many people were affected, etc.

3. Department of the Army, Office of the Chief Information Officer, *Army Data Plan*, October 11, 2022, https://www.army.mil/e2/downloads/rv7/about/2022_army_data_plan.pdf.

4. "Occupational Outlook Handbook–Data Scientists," U.S. Bureau of Labor Statistics, April 17, 2024, https://www.bls.gov/ooh/math/data-scientists.htm; and Aleksandra Yosifova, "The Best Industries for Data Science Specialists in 2024,"*Career Advice, 365 Data Science* (blog), 11 April 2024, https://365datascience.com/career-advice/the-best-industries-for-data-science-specialists/.

5. Zaid Obermeyer and Ezekiel J. Emanual, "Predicting the Future–Big Data, Machine Learning, and Clinical Medicine," *The New England Journal of Medicine* 375, no. 13 (September 29, 2016): 1216-1219, https://www.nejm.org/doi/full/10.1056/NEJMp1606181; and Xinhu Zheng et al., "Big Data for Social Transportation," *IEEE Transactions on Intelligence Transportation Systems* 17, no. 3 (March 2016):620-630, https://doi.org/10.1109/TITS.2015.2480157.

6. Hsinchun Chen et al., "Crime Data Mining: A General Framework and Some Examples," *Computer* 37, no. 4 (April 2004):50-56, https://doi.org/10.1109/MC.2004.1297301.

7. Department of the Army, Office of the Chief Information Officer, *Army Data Plan*, 3.

8. Department of the Army, Army Regulation 350-1, *Army Training and Leader Development* (Washington, DC: U.S. Government Publishing Office, 1 June 2025), 5.

9. Automation can refer to everything from basic scripting to machine learning applications.

10. Norman Krueger, Tim Gabriel, and Cezar Adam, "The Hub-and-Spoke IT Operating Model: Increasing Innovation and Continuous Improvement," ISG (Information Services Group), n.d., https://isg-one.com/articles/the-hub-and-spoke-it-operating-model.

11. Chen et al., "Crime Data Mining."

12. Obermeyer and Emanual, "Predicting the Future."

13. Zheng et al., "Big Data for Social Transportation."

14. Andre Python et al., "Predicting Non-State Terrorism Worldwide," *Science Advances* 7, no. 31 (July 2021), https://www.science.org/doi/10.1126/sciadv.abg4778.

15. The Peace Research Institute Oslo, https://www.prio.org/.

References

Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 26 May 2022). Change 1 was issued on 5 July 2024.

"Market Research Industry–Statistics and Facts," Statista, May 16, 2024, https://www.statista.com/topics/1293/market-research/#topicOverview.

COL Chris Tomlinson is the Director of Intelligence, G-2, for the Southern European Task Force, Africa (SETAF-AF) and is operational director of the Africa Data Science Center (ADSC) for SETAF-AF. His prior intelligence assignments include Director of Intelligence, J-2, for the Special Operations Joint Task Force–Operation Inherent Resolve, Deputy Director of Intelligence, J-2, and theater analysis and control element chief U.S. Army Europe. He holds a master's degree in strategic studies from the Marine Corps War College and a bachelor of arts in political science at Texas Tech University.

CW3 Felix Rodriguez Faica is an intelligence planner and common intelligence picture/Army Intelligence Data Platform lead integrator in the intelligence operations division of the SETAF-AF G-2. His previous assignments were at various unit echelons including brigade combat team and military intelligence brigade-theater. He received a bachelor of arts in intelligence studies from American Military University and completed the Digital Intelligence Systems Master Gunner Course.

CW2 Ryan Harvey is an all-source intelligence technician serving as an intelligence planner and performance manager for the ADSC in the intelligence operations division of the SETAF-AF G-2. His previous assignments were at various unit echelons, including brigade combat team and military intelligence brigade-theater. He holds a master's degree in intelligence management from Henley-Putnam University and a bachelor of arts in political science from the University of California, Santa Barbara.

Mr. Keith Hickman is a senior data scientist for the ADSC of the SETAF-AF G-2. He previously served as an Army intelligence officer at a brigade combat team. He holds a juris doctor from Pennsylvania State University and a master's degree in computer science from Indiana University.

Contact & 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 1,000 and 3,000 words, double-spaced with normal margins without embedded graphics.
- We cannot guarantee we will publish all submitted articles.
- Please do not send overly large and complicated or small print graphics/PowerPoint slides. What looks good as a PowerPoint presentation doesnt always translate well to an 8 1/2" x 11" article format.
- 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 memorandum is available from the MIPB Staff. Contact us at the email address at the bottom of the page.
- **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297) 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@army.mil. For any questions, email us at the above address or call 520-533-7836/DSN 821-7836.

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

PIN: 221283-000