

MI PROFESSIONAL BULLETIN



2025
PB 34-25-2

A close-up, high-contrast photograph of a soldier wearing a helmet with various attachments, including a night vision device and a microphone. The soldier is wearing camouflage gear. The background is a clear blue sky with the rotor blades of a helicopter visible.

**CONTINUOUS
TRANSFORMATION:
ECHELONS CORPS
AND BELOW**



PLANNING AND EXECUTING DIVISION INTELLIGENCE REACH CELL OPERATIONS

by Major Franklin Peachey, Captain William Lairson,
and Chief Warrant Officer 2 Erik Wickham

U.S. Army Soldiers assigned to 3rd Infantry Division move equipment into a building during Austere Challenge 2024 at Forward Operating Site Bolesławiec, Poland. (U.S. Army photo)

Recognizing the Requirement

The problem of meeting mission requirements with limited organizational capabilities is an inherent leadership challenge that spans services, branches, and echelons. Conducting intelligence operations in an active theater is no different. Meeting mission requirements entails the routine and collaborative efforts of intelligence personnel across echelons and, potentially, over significant geographic distances. During the 3rd Infantry Division's (ID's) recent deployment to Victory North, V Corps' area of operations (AO) in Poland and the Baltics, the division G-2 met this leadership challenge by establishing a federated intelligence reach relationship with its direct support intelligence and electronic warfare (IEW) battalion (BN), the 103rd, in Fort Stewart, Georgia. Establishing this type of relationship falls doctrinally within the task of conducting intelligence reach and its various subtasks as outlined in Appendix B of Field Manual 2-0, *Intelligence*.¹ By going one step further and federating the intelligence reach cell, 3rd ID G-2 established a command and support relationship with the cell that ensured some capabilities remained dedicated to the mission for the duration of the deployment. The success of this approach required identifying intelligence requirements and allocating capabilities, deliberately leveraging the operations process, and actively involving leaders across organizations.

Intelligence Reach

Intelligence reach is "the activity by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command."²

Identifying the various mission requirements and the necessary capabilities was a crucial component of the 3rd ID G-2's mission analysis more than three months before deployment. To ensure proper identification, the G-2 team completed a

pre-deployment site survey and conducted routine working groups with the outgoing 4th ID G-2. From this mission analysis, the 3rd ID G-2 analysis and control element (ACE) identified the following mission requirements:

- ◆ Partner nation intelligence support through the Security Assistance Group-Ukraine.
- ◆ Exercise support leading up to and during European Command's Austere Challenge 2024.
- ◆ Intelligence support to NATO regional defense planning.
- ◆ Intelligence security cooperation activities.
- ◆ Steady-state intelligence production to include maintenance of a common intelligence picture for an assigned area of responsibility from the V Corps G-2.
- ◆ Maintenance of a G-2 home-station mission command presence to provide intelligence support to one remaining brigade combat team.

Once the G-2 team assessed the capabilities necessary to meet these requirements, it determined that staffing for the division ACE, supplemented by augmenting capabilities from across the brigade military intelligence companies, was insufficient to meet all requirements.

The inability of a division ACE to meet its expected intelligence requirements in an active theater is a known capability gap for the Army; consequently, the Army allocates a direct support IEW BN to divisions. However, the 3rd ID's request for the 103rd IEW BN to deploy in support of the mission in Europe was not granted because of other operational requirements. To meet the division's mission needs the 3rd ID G-2 team developed a course of action employing part of the 103rd IEW BN through intelligence reach to support the division G-2's forward deployment to Poland. Developing this course of action required determining whether the intelligence requirements could be executed through intelligence reach and, if so, whether the resulting intelligence products would be suitable

for the mission. Because most intelligence requirements necessitated proximity to the source, intelligence reach support from the 103rd IEW BN would be limited primarily to significant augmentation of steady-state intelligence production, with only minor support for other requirements. With this assessment, the 3rd ID G-2 ACE developed a detailed analysis of steady-state production requirements and the capabilities necessary to support them.

Establishing the Intelligence Reach Cell

To answer the 3rd ID Commanding General’s priority intelligence requirements, the 3rd ID G-2 ACE developed a weekly production cycle. The 103rd IEW BN then completed a feasibility assessment based on this production requirement to determine the specific military occupational specialty roles, equipment, and facilities required to support the schedule. The assessment results indicated that the battalion could provide the necessary support with a cross-intelligence discipline reach cell comprising approximately 19 to 21 individuals while still maintaining their other operational requirements (Figure 1).

Based on the assessment, the 3rd ID G-2 ACE determined that by leveraging the intelligence reach cell to complete most of its steady-state production requirements, the ACE could then surge to meet its other intelligence requirements in theater. As these requirements would persist throughout the division’s deployment, it was necessary to formalize this direct support relationship to allow portions of the division ACE to remain fully dedicated to other mission requirements.

The 3rd ID G-2 and the 103rd IEW BN collaborated on a fit-for-purpose request for support that enabled the 103rd IEW BN to keep its necessary capabilities. The request was submitted through G-3 channels to the XVIII Airborne Corps for tasking the 525th Expeditionary Military Intelligence Brigade (E-MIB) with the requirement to support. The 103rd IEW BN, a subordinate headquarters of the 525th E-MIB, was then formally tasked with directly supporting the 3rd ID G-2 for the duration of its deployment using an intelligence reach cell with the capabilities to facilitate the weekly intelligence production. By leveraging this operations process, the 3rd ID G-2 employed federated support from an intelligence reach cell and met its mission requirements.

As the 103rd IEW BN assembled the intelligence reach cell to support the 3rd ID G-2, leaders from both organizations began positioning the cell to enable its long-term support. The battalion determined which personnel and equipment would provide the support. At the same time, the 3rd ID G-2 ACE identified space adjacent to its home-station mission command personnel from which the intelligence reach cell would operate. Once established, the intelligence reach cell leadership developed a battle rhythm nested with that of the 3rd ID G-2 ACE, training their personnel and gathering the necessary tools to begin production. Approximately one month before the 3rd ID G-2 advance elements deployed, the intelligence reach cell acquired the necessary equipment and trained personnel to achieve initial operating capacity

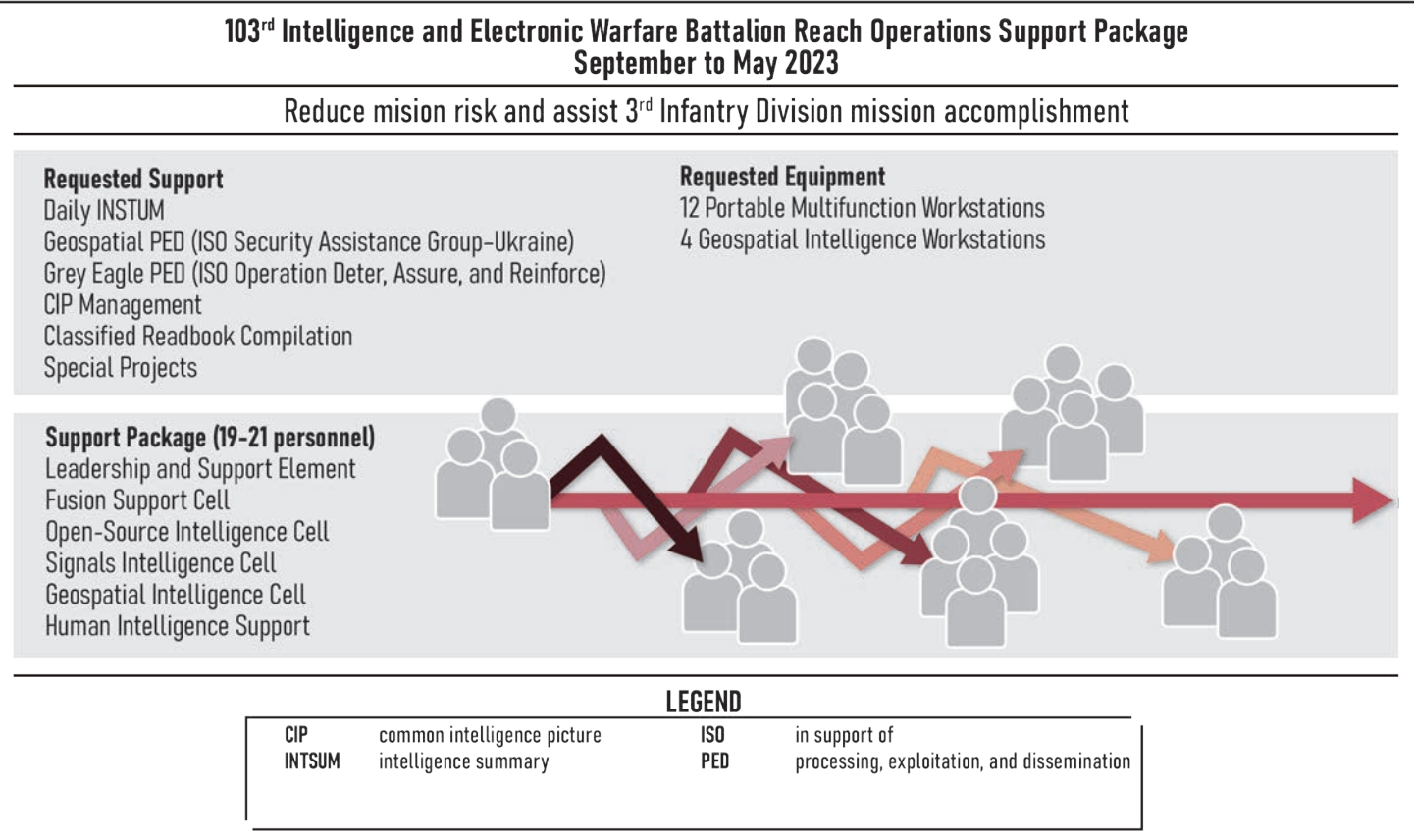


Figure 1. 103rd Intelligence and Electronic Warfare Battalion Support³

and began executing its mission. As the 3rd ID G-2 advance elements transitioned with the 4th ID G-2 in theater, the intelligence reach cell became fully operational and published its first weekly production requirement of three open-source summaries, two intelligence summaries, and one graphical intelligence summary.

Operating an Intelligence Reach Mission Team

Continued leadership engagement and routine production of after action reviews proved crucial to developing the final intelligence reach cell’s structure in a way that used talent most efficiently to meet all mission requirements (Figure 2). Throughout the intelligence reach cell’s support mission, the 3rd ID G-2 ACE’s leadership and the intelligence reach cell’s officer in charge maintained an open dialogue about production requirements and refinements, which included a weekly synchronization meeting. Additionally, both the IEW BN commander and the intelligence reach cell officer in charge briefly joined the G-2 team at the forward-deployed location to assess the effectiveness of their support and make necessary adjustments.

The G-2 leadership provided guidance and implemented weekly production requirements for the intelligence reach cell. The schedule developed around these requirements had the team working Sundays through Thursdays. The daily battle rhythm of the intelligence reach cell included completing and sending products by 1700 on the day prior to the “required by” date because of the 6-hour time difference between their

location in Fort Stewart, Georgia, and the forward-deployed G-2 in Europe. This allowed the 3rd ID G-2 ACE to review and refine the products the following morning before publishing them. Once the forward team published the products, the intelligence reach cell reviewed any changes and used them to inform the development of subsequent products. The intelligence reach cell’s product schedule remained flexible to account for forward training exercises and leadership requests for information that required the intelligence reach cell to develop deep-dive products.

Lessons Learned

During the mission, several lessons and best practices contributed to the evolution of better processes, management, and structure of the intelligence reach cell.

Planning. Implementing an in-depth road-to-war discussion focused on the AO’s political, military, economic, and civil considerations will enable analysts to understand the context in which the forward team operates and help determine the best way to support it. To maintain contextual understanding, the intelligence reach cell analysts must remain synchronized with the division’s weekly operations through attendance at commander updates and routine review of the situation reports, the long-range training calendar, and the commanding general’s executive calendar. This synchronization enables a responsive intelligence reach cell to be more proactive in its production.

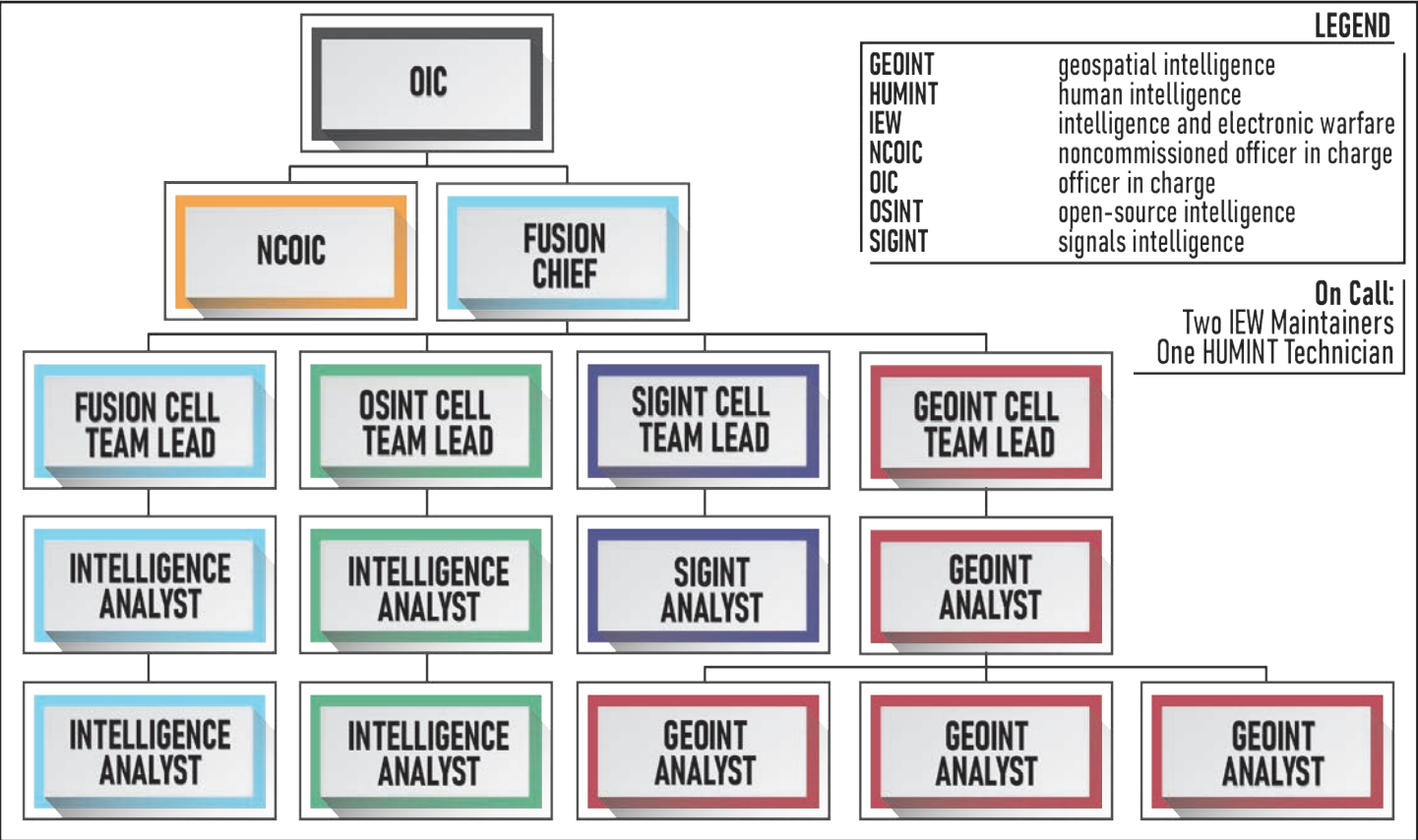


Figure 2. Intelligence Reach Cell Structure⁴

Staffing. Assigning a warrant officer or fusion noncommissioned officer to the team provides the experience and expertise necessary to orient and drive production.

Training. Planning should include courses on report writing, analytical research, product classification, command post computing environment, and specific courses for individual intelligence disciplines. This training enables intelligence reach cell analysts to work more efficiently with their division G-2 counterparts.

Equipping. Maintaining active accounts across the SECRET Internet Protocol Router Network (SIPRNET), the tactical SIPRNET, the mission partner environment, and the battlefield information collection and exploitation system will ensure that all necessary systems are available.

Division Focused Open-Source Intelligence

Open-source intelligence (OSINT) has taken many forms throughout its employment in the Army, changing through litigation, nascent capability, and organizational redesign. Employment at the division level can quickly become redundant with theater (66th Military Intelligence Brigade-Theater) and forward-deployed theater-servicing (519th IEW BN/525th E-MIB) OSINT. The 103rd OSINT team, however, operated under U.S. Army Forces Command (FORSCOM) and XVIII Airborne Corps authorities, solely supporting the 3rd ID. To deconflict reporting and provide the best service to the division, the 3rd ID G-2 provided AO-oriented geographic focus areas from which the 103rd OSINT team provided reports. By focusing on open-source reporting in Poland and the Baltics, the OSINT team directly supported 3rd ID's priorities and operations, filling intelligence gaps where other intelligence disciplines lacked authority or international permissions to collect.

OSINT Stand-Up. In tandem with the stand-up of the intelligence reach capability, the 103rd IEW BN established an OSINT program in support of and under the authorities of the 3rd ID. The preconditions for conducting OSINT activities included:

- ◆ OSINT standard operating procedures (signed by the division G-2).
- ◆ OSINT collection plan (signed by the division G-2).
- ◆ OSINT risk assessment (signed by the division G-2).
- ◆ Authority to collect (FORSCOM and XVIII Airborne Corps memorandum signed by the respective G-2s).

- ◆ OSINT Basic Course mandated for all collectors.
- ◆ Army OSINT office memorandum with collection identification numbers for each collector.
- ◆ Compliance with Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities*; Department of Defense Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*; and Executive Order 12333, *United States Intelligence Activities* (as amended by Executive Orders 13284 [2003], 13355 [2004], and 13470 [2008]).
- ◆ Responsibility to publish to the entire intelligence community.

“This experience exemplifies leveraging external intelligence elements remotely while ensuring maximum collaboration to meet mission requirements.”

OSINT Outputs. OSINT production consisted of three weekly open-source summaries and infrequent OSINT reports driven by requests for information. As a fluid, rapidly changing intelligence discipline, OSINT has unique educational requirements for staff that may be unfamiliar or no longer keep abreast of emerging OSINT tools, limitations, and regulations. OSINT leaders have a responsibility to actively seek opportunities to inform leaders and commanders about the updated regulations and current suite of available tools that will satisfy requirements most effectively. The 103rd

OSINT products were among the most well-received products provided by the intelligence reach cell because of their timeliness and value in understanding public perceptions and the atmospherics within a given focus area.

Maximizing Collaborative Intelligence

The 3rd ID G-2 met its mission requirements by developing a fit-for-purpose, federated intelligence reach cell in coordination with the 103rd IEW BN. This federated intelligence reach cell resulted from a collaborative mission analysis with numerous stakeholders to identify mission requirements and allocate the appropriate capabilities. The formalization of this team through the operations process ensured its support to the 3rd ID G-2 and enabled the massing of organic intelligence resources elsewhere within the division. Finally, the routine involvement of leaders from both organizations throughout the planning and operating of the intelligence reach cell ensured that it not only met mission requirements but continued to improve throughout its direct support to the division. This experience exemplifies leveraging external intelligence elements remotely while ensuring maximum collaboration to meet mission requirements. 🌟

Endnotes

1. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: Government Publishing Office [GPO], 01 October 2023), B-9.
2. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: GPO, 31 July 2019), 3-5.
3. Figure adapted from original by CW2 Wickham.
4. Figure adapted from original by CW2 Wickham.

MAJ Franklin G. Peachey is the brigade intelligence observer, coach, and trainer at the Joint Multinational Readiness Center in Hohenfels, Germany. He previously served as the analysis and control element chief for 3rd Infantry Division's (ID's) deployment in support of U.S. Army Europe and Africa's Operation Assure, Deter, and Reinforce. He holds a master of arts in diplomacy from Norwich University, along with master degrees from the Art of War Scholars Program and the School of Advanced Military Studies.

CPT William "Bill" Lairson most recently served as the multidomain officer for the 103rd Intelligence and Electronic Warfare Battalion (IEW BN), 525th Expeditionary Military Intelligence Brigade located in Fort Stewart, GA. He served as an infantry platoon leader, mortar platoon leader, and company commander for the 1st ID in Fort Riley, KS while deploying to Germany and Poland. He holds a bachelor of science in education from the University of Akron.

CW2 Erik Wickham is an Army operations and integration technician who manages all-source intelligence training requirements and synchronizes 103rd IEW BN operational requirements in support of 3rd ID. His previous assignments include open-source Intelligence team chief for the 103rd IEW BN; intelligence sergeant, 10th Army Air and Missile Defense Command; South America noncommissioned officer in charge, 470th Military Intelligence Brigade; and intelligence sergeant, 2nd Squadron, 2nd Cavalry Regiment.

U.S. Army Soldiers assigned to the 103rd Intelligence and Electronic Warfare Battalion begin a convoy movement to the Mission Training Complex at Fort Stewart, Georgia. (U.S. Army photo)



INTELLIGENCE AND FIRES CAPABILITIES INTEGRATION

by Major General Christopher Norrie, Colonel Shawn Bault,
Colonel Marcus O'Neal, Major John Hornecker,
and Captain Xavier Ehresman

Introduction

The Army is transitioning and adapting to the multidomain threat and requires updated processes and procedures to maintain an edge over future adversaries. The current conflict in Ukraine demonstrates that successful operations and survivability in a deliberate and dynamic fight depend on an army's ability to target expeditiously. The 3rd Infantry Division (ID) tested this concept using a strike cell within its division artillery (DIVARTY) to determine if the strike cell could focus the DIVARTY on a portion of the division's targeting requirements. This would enable the division's joint air-ground integration cell (JAGIC) to maintain focus on deep shaping operations. This strike cell concept proved its value during a recent command post exercise (CPX), where the Army's first DIVARTY strike cell enhanced division effects.

Testing the Strike Cell Concept

While deployed in the European theater, Soldiers from the 3rd Infantry Division Artillery (3DIVARTY) and the 103rd Intelligence and Electronic Warfare (IEW) Battalion (BN), in coordination with the 3rd ID Headquarters, conducted CPX III in preparation for Austere Challenge 24 (March 2024), a multinational exercise for the V Corps, with support from the 3rd ID and 3DIVARTY.

CPX III simulated the complexities of conducting command and control, maneuver, fires, and intelligence operations in a large-scale combat operations environment. It also tested both the division and subordinate commands' ability to conduct command and control of assigned formations and the 3DIVARTY's ability to synchronize fires and deliver lethal effects. The 103rd IEW BN Soldiers were integrated into the 3DIVARTY intelligence section to enhance the unit's target acquisition capabilities and reduce the time from sensor to shooter.

"The Strike Cell integration into 3DIVARTY is a force multiplier that enables effects continuity throughout the division battlespace from the division forward boundary to brigades' front-line trace."—COL Shawn Bault, 3DIVARTY Commander.

The 3DIVARTY received the following capabilities for CPX III: a processing, exploitation, and dissemination (PED) element; a battle damage assessment team; an intelligence, surveillance, and reconnaissance assessment team; and mission manager support to assume responsibility for current collection operations management, freeing the 3DIVARTY intelligence section's officer in charge to focus on providing intelligence analysis and situational awareness.

The 3DIVARTY strike cell comprised a geospatial intelligence imagery analyst to monitor full-motion video and ground movement target indicator feeds and a signals intelligence analyst to monitor and analyze signal and communications data.¹ A mission manager² and a field artillery intelligence officer³ led strike cell operations. This combined effort facilitated a consistent focus on deliberate and dynamic targeting within the DIVARTY.

The 3rd ID uses target focus areas (TFAs)⁴ to support targeting operations. Each TFA is a 15-kilometer by 15-kilometer square comprising a geographic grouping of target areas of interest and named areas of interest, which are anticipated to contain many high-payoff targets. The division actively targets the deepest TFAs beyond the coordinated fire line (CFL) and assigns the TFA nearest to the CFL to 3DIVARTY. Each TFA is assigned to a strike cell in the division's deep area, approximately 25 to 45 kilometers beyond the CFL, pending firing assets and munitions available. This practice was validated during CPX III and will be applied in future operations.

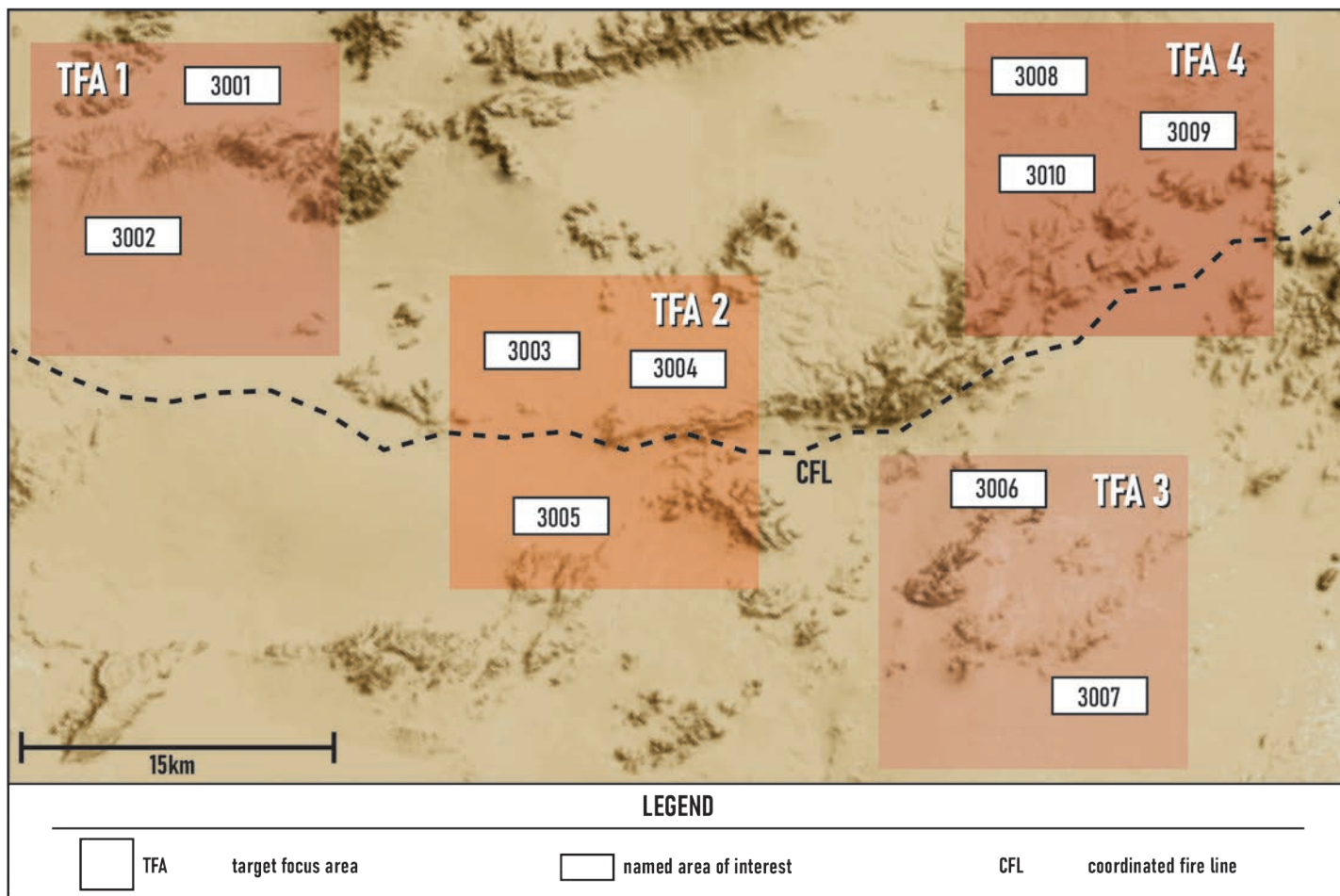


Figure. Example Target Focus Area

The 3DIVARTY, in close coordination with the division fires, the division G-2, and the 103rd IEW BN, used DIVARTY capabilities to detect, deliver, and assess targets. This enabled the rapid employment of surface-to-surface fires, decreased target decay times, and ultimately allowed the JAGIC, the strike cell, and the G-2 analysis and control element to maintain focus on deep area shaping operations. The 3DIVARTY passed objectives to the brigade combat teams to maintain constant pressure on simulated enemy formations. The 3DIVARTY then focused on TFAs with their strike cell to enable prioritizing the division's TFA nearest to the CFL. This maximized division effects and permitted the JAGIC to focus on the division's deep fight with long-range and joint fires capabilities.

The 3DIVARTY strike cell provided effective PED support to the field artillery intelligence officer and the fire support element's targeting efforts. The synchronization between the DIVARTY fire support element and the JAGIC was paramount in clearing airspace to ensure timely and accurate fires. The DIVARTY air defense airspace management/brigade aviation element assisted the JAGIC in expeditiously clearing airspace for fires after the division allocated a TFA to DIVARTY. In turn, the JAGIC supported DIVARTY in deconflicting airspace above the coordinated altitude by using airspace control measures to rapidly execute fires.

"The IEW Battalion provides the Division's Artillery element with an expeditionary intelligence capability that bolsters the intelligence capacity of the S-2 staff, allowing for targeting efforts independent of the Division's JAGIC."—COL Marcus O'Neal, 103rd IEW BN.

Conclusion

The 3DIVARTY strike cell proved to be a critical capability, directly impacting division shaping operations and enabling division transitions across the battlefield. Through CPX III, the 3DIVARTY validated the strike cell concept. The 3DIVARTY strike cell, along with existing 3DIVARTY systems and the 103rd IEW BN, was central to the success of targeting operations. The strike cell led the fight when the division main and tactical command posts jumped, enabling a smooth transition and maintaining division effects. Additionally, the 103rd IEW BN accomplished its mission of providing additional intelligence analysis and collection capabilities to a division—the Army's unit of action in a large-scale combat operation scenario—enhancing the overall capability of the division's intelligence elements and ensuring lethality for maneuver elements. ✨

"Our DIVARTY Strike Cell is critical to maintaining lethal contact to keep the *combine*⁵ churning up ground as we transition contact to maneuver brigades." said MG Christopher Norrie, 3rd ID Commanding General.

Endnotes

1. Joint Chiefs of Staff, Joint Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 26 May 2022), GL-22. Change 1 was issued on 5 July 2024. Signals intelligence is intelligence derived from communications, electronic, and foreign instrumentation signals.
2. The mission manager ensured the geospatial intelligence imagery analyst and signals intelligence analyst cued each other, tasked the unmanned aircraft system operator with dynamic movements, and communicated with the division for updated nonlethal effects and theater support. The mission manager also managed the collection plan focused on the high-payoff target list assigned by the division fire support element.
3. Department of the Army, Field Manual 3-09, *Fire Support and Field Artillery Operations* (Washington, DC: GPO, 12 Aug 2024), 2-3, 2-7–2-8. The field artillery intelligence officer communicated with the division artillery fires support element fire control officer by sending validated targets for the fire control officer to engage. Additionally, with support from the strike cell, the field artillery intelligence officer contributed to target assessment (battle damage, munitions effectiveness, and re-attack recommendations).
4. *Target focus areas* are a non-doctrinal concept and term used by the 3rd Infantry Division to support its targeting operations.
5. The term *combine* describes how the 3rd ID places numerous effects on the enemy, simultaneously or sequentially, forcing a commander to make a choice between multiple unappealing options.

MG Christopher Norrie is the Commanding General, 3rd Infantry Division (ID), Fort Stewart, GA. He previously served as the Director, People First Task Force, Office of the Deputy Chief of Staff, G-1. He has held multiple command and other assignments within 1st Cavalry Division, 1st Armored Division, 1st ID, 4th ID, the Training and Doctrine Command, and Headquarters, Department of the Army staff. His operational deployments and combat tours include Operation Joint Forge, Operation Iraqi Freedom, Operation Spartan Shield, and Operation Atlantic Resolve. His military education includes the U.S. Army Armor Officers Basic Course, Infantry Officer Advanced Course, and the Command and General Staff College. MG Norrie is a distinguished military graduate of Bucknell University in Lewisburg, PA, and holds master's degrees in business administration from Embry-Riddle University and in national security strategy from the National War College.

COL Shawn Bault is the Commander, 3rd ID Artillery, Fort Stewart, GA. He previously served in the Pentagon as Chief of Staff for the Chief of Army Public Affairs. He deployed multiple times in support of Operations Enduring Freedom, Iraqi Freedom, Spartan Shield, Inherent Resolve, and European Assure, Deter, and Reinforce. COL Bault's military education includes the National War College, the School of Advanced Military Studies, the Command and General Staff College, Joint Firepower Control Course, Air Assault School, and Advanced Airborne School. He holds a bachelor's degree in history from the U.S. Military Academy and a master's degree in kinesiology from Texas A&M University.

COL Marcus O'Neal is the Director (J-2) Special Operations Command South, Homestead Air Reserve Base, FL. He previously served as the Commander, 103rd Intelligence and Electronic Warfare (IEW) Battalion, Fort Stewart, GA. COL O'Neal deployed several times throughout his career. He deployed to Iraq as both an armor and intelligence officer and to Afghanistan as an intelligence officer. COL O'Neal graduated as a distinguished military graduate from Southern University, Baton Rouge, LA. He holds a master of science of strategic intelligence from the National Intelligence University.

MAJ John Hornecker is the 3rd ID Deputy G-2, Fort Stewart, GA. He previously served as the 3rd ID Collection Manager and 3rd ID Artillery Brigade S-2 in support of Operation European Assure, Deter, and Reinforce (Latvia). MAJ Hornecker previously deployed in support of Operation Spartan Shield from June 2012–March 2013. His professional accomplishments include completion of the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance program. MAJ Hornecker is a graduate of Saint Louis University.

CPT Xavier Ehresman is the 3rd ID G-2 Targeting Officer. He previously served as the Commander, Bravo Detachment, 103rd IEW Battalion, Fort Stewart, GA. Prior to company command, he served as an infantry platoon leader and battalion assistant S-2 at Fort Drum, NY, and as a battalion S-2 for the 103rd IEW Battalion. He holds a bachelor's degree in forensic psychology with a focus in psychology from the University of New Haven. He is currently pursuing a master's degree in human performance and nutrition from Liberty University.

A U.S. Army officer confers with Polish officers over a map during Avenger Triad 24 on 12 Sep 24 in Boleslawiec, Poland. (U.S. Army photo by PFC Hector Blanco)



INTEGRATING TACTICAL

AND OPERATIONAL

COLLECTION: V CORPS

G-2 LESSONS FROM

AVENGER TRIAD 24

BY MAJOR BRIAN CANIANO

During large-scale combat operations (LSCO), corps headquarters operate at the transition between the operational and tactical levels of warfare. Corps commanders must understand the operational context of the battlefield to ensure their tactical operations achieve operational objectives.¹ Intelligence collection provides the information required for commanders to achieve this visualization. The corps G-2 must understand both its own tactical intelligence requirements and the operational level intelligence requirements of its higher headquarters to develop and execute a collection plan that encapsulates both levels of warfare.

U.S. Army doctrine provides a minimal description of efficient methods for corps headquarters to execute this process during LSCO. During the Avenger Triad 24 exercise in September 2024, V Corps refined techniques to integrate tactical collection requirements into a North Atlantic Treaty Organization (NATO) Multi-Corps Land Combatant Command (MCLCC) collection plan and to conduct intelligence collection in a contested LSCO environment. The G-2 collection management and dissemination (CMD) section prioritized corps and division requests for the limited available collection from its higher headquarters while integrating nonintelligence capabilities to maximize collection opportunities. This required V Corps to learn and adapt to intelligence handover and collection differences between the operational and tactical levels.

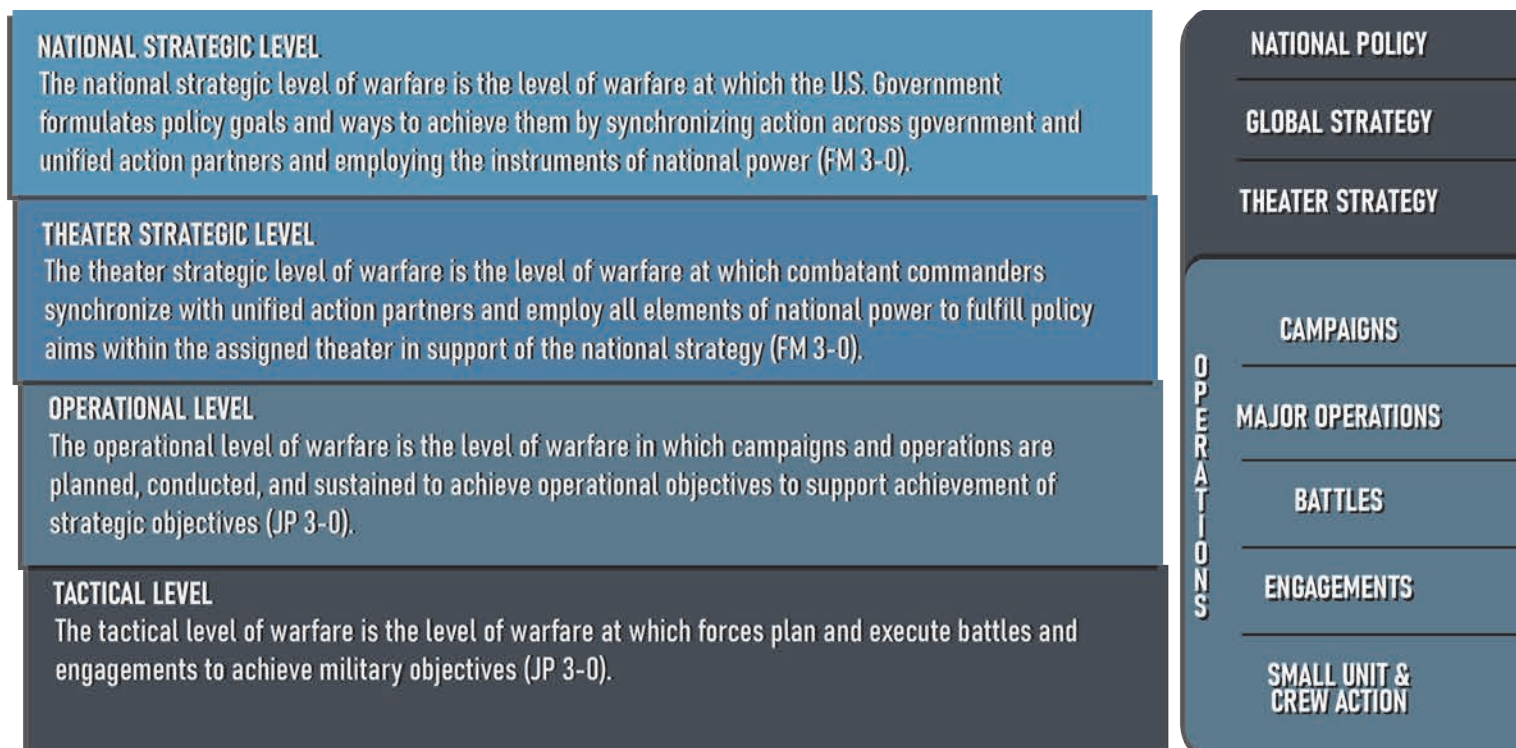


Figure 1. Levels of Warfare²

Exercise Background

During Avenger Triad 24, V Corps executed LSCO in a contested operational environment against a near-peer enemy. U.S. Army Europe-Africa served as the NATO MCLCC, commanding six corps of U.S., NATO, and allied units across several countries. The MCLCC G-2 CMD required subordinate units to submit requests for collection from the MCLCC and theater capabilities 96 hours in advance of execution to facilitate review and submission into the air operations center's air tasking orders, with ad hoc and dynamic re-tasking within 96 hours also available through proper coordination. V Corps commanded three U.S. Army divisions, an expeditionary sustainment command, a fires brigade, a combat aviation brigade, and additional corps enabler formations. The 336th Expeditionary Military Intelligence Brigade provided V Corps G-2 with additional collection, targeting, and analytical support normally provided by an intelligence and electronic warfare battalion (corps). V Corps conducted both offensive and defensive operations during the exercise in support of the MCLCC.

Concept of Intelligence Collection

The V Corps collection strategy in entering Avenger Triad was to mix complementary geospatial intelligence and signals intelligence collection from higher echelon assets to cue V Corps full-motion video capabilities to detect high-payoff targets in real time for lethal targeting. Higher echelon assets provided the operational reach and detection capabilities to collect in the V Corps deep area and cue its assets. Organic full-motion video assets provided V Corps with a flexible, real-time capability that could be controlled internally on

the battlefield to expedite the targeting of enemy high-payoff targets. Theater asset availability and corps asset freedom of movement on the battlefield were critical to the success of the V Corps collection strategy.

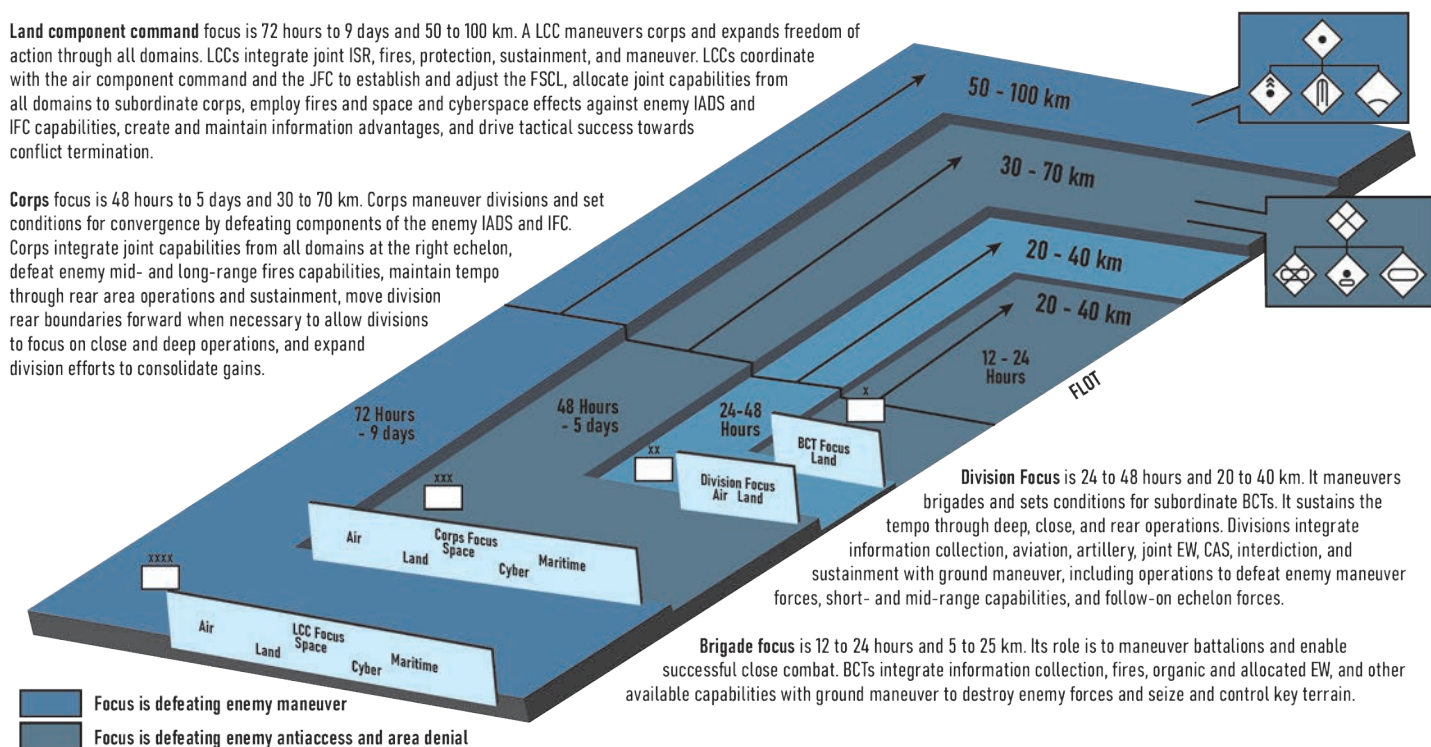
Corps, divisions, and brigades execute intelligence handover at the tactical level using established graphic control measures known as intelligence handover lines that regularly correspond with the unit's fire support coordination measures. This relationship aligns collection with unit fire support plans to enable sensor-to-shooter operations at echelons in the corps and division deep areas. During Avenger Triad 24, corps and division intelligence handover lines and fire support coordination measures were within operational ranges of their aerial intelligence collection sensors. These lines shift as the battle progresses, with the higher headquarters conducting an intelligence handover of their former areas to their subordinate units to facilitate intelligence operations and targeting continuity.³

Lessons Learned During Execution

V Corps encountered several obstacles to executing its collection strategy during Avenger Triad 24. Enemy integrated air defense systems (IADS) at the brigade and above echelons significantly restricted freedom of movement for corps aerial collection platforms. These enemy assets protected the enemy's command posts, electronic warfare systems, and long-range artillery, constituting most of the V Corps high-payoff target list. The enemy's advanced electronic warfare capabilities also prevented V Corps sensors from transmitting their collection feeds for processing, exploitation, and dissemination by intelligence analysts. In addition to the enemy,

Land component command focus is 72 hours to 9 days and 50 to 100 km. A LCC maneuvers corps and expands freedom of action through all domains. LCCs integrate joint ISR, fires, protection, sustainment, and maneuver. LCCs coordinate with the air component command and the JFC to establish and adjust the FSCL, allocate joint capabilities from all domains to subordinate corps, employ fires and space and cyberspace effects against enemy IADS and IFC capabilities, create and maintain information advantages, and drive tactical success towards conflict termination.

Corps focus is 48 hours to 5 days and 30 to 70 km. Corps maneuver divisions and set conditions for convergence by defeating components of the enemy IADS and IFC. Corps integrate joint capabilities from all domains at the right echelon, defeat enemy mid- and long-range fires capabilities, maintain tempo through rear area operations and sustainment, move division rear boundaries forward when necessary to allow divisions to focus on close and deep operations, and expand division efforts to consolidate gains.



Note 1. Distances are from the FLOT toward the enemy

Note 2. Time and distances are illustrative and vary depending on the situation

BCT	brigade combat team	FSCL	fire support coordination line	JFC	join force commander
CAS	close air support	IADS	integrated air defense system	km	kilometers
EW	electromagnetic warfare	IFC	integrated fires command	LCC	land component command
FLOT	forward line of own troops	ISR	intelligence, surveillance, and reconnaissance		

Figure 2. Notional Roles/Responsibilities in Time, Space, and Purpose at Different Echelons⁴

weather conditions also restricted the ability of V Corps to utilize real-time full-motion video for targeting. These same restrictions also degraded the ability of the three subordinate V Corps divisions to conduct collection in their deep areas.

The transition from operational to tactical level intelligence operations entails a fog of war as the level of detail that corps and division G-2 sections must anticipate and plan against intensifies. Intelligence handover between the operational and tactical levels of warfare is not as linear as the handover process internal to corps and division. The MCLCC's collection focused on its high-payoff targets and the locations of enemy operational and strategic reserve forces. However, MCLCC and theater collection and targeting priorities were noncontiguous and did not directly align with territory beyond the V Corps deep area. The MCLCC and theater high-payoff targets were often located inside the V Corps intelligence handover line boundaries. Concurrently, there were areas of the battlefield beyond the V Corps deep area that were not a collection or targeting priority for the MCLCC but contained enemy units that would later be relevant to V Corps tactical operations.

V Corps encountered all of these problems simultaneously during Avenger Triad 24. Corps and divisions could not collect across the breadth of their deep areas with organic assets due to the enemy IADS and electromagnetic warfare threats. The

MCLCC had limited collection on terrain and enemy forces beyond the corps deep area that V Corps would later have to detect and target. The operational environment did not support a detailed intelligence handover that could correspond to the pace of combat operations due to the sheer size and tempo of the battlefield. The V Corps G-2 collaborated with its higher, lower, and adjacent intelligence sections to develop solutions to fill these collection gaps.

Reimagining Intelligence Handover

The V Corps G-2 needed to develop a new element of its collection strategy to account for how the LSCO environment's complexity and tempo influenced the application of intelligence collection at the operational and tactical levels of warfare. This necessitated a realization at the corps level that it could not plan collection operations with the expectation of receiving a detailed intelligence handover for all areas beyond the current corps deep area from the MCLCC. The V Corps G-2 assumed responsibility for requesting collection through the MCLCC to fulfill tactical-level information requirements regardless of their position on the battlefield. The focus of corps intelligence collection should dictate the forward boundary based on its relevance to future planning, rather than being limited by the range of corps collection and fires assets. This would enable V Corps to correctly forecast feasible

The General Atomics Aeronautical Systems' MQ-1C Gray Eagle is a medium altitude, long endurance unmanned aircraft system that provides intelligence, surveillance, and reconnaissance collection support.



collection allotments for future operations and develop additional methods to supplement projected gaps in collection without disrupting operations.

These two activities were paramount to V Corps and the MCLCC's success during Avenger Triad 24.

V Corps was constantly competing for intelligence collection asset allocation with its adjacent corps and the MCLCC due to the sheer size of the enemy on the battlefield. During planning and targeting meetings, V Corps identified intelligence requirements against enemy units that would not be within range of V Corps collection or fires capabilities for at least 48 to 72 hours. V Corps simultaneously recognized that many corps and division collection requirements within V Corps boundaries related to current and future operations would likely go unfulfilled due to the enemy's protection and electronic warfare capabilities. These two factors prompted V Corps to develop a comprehensive and efficient method to holistically assess and prioritize corps and division collection requirements that required support from MCLCC and theater assets.

V Corps G-2 CMD realized it could not assess the fulfillment of these tactical intelligence requirements simply by reviewing the MCLCC and theater collection plans to verify if sensors were allocated to a specific area or unit. The mere presence of collection over an area does not indicate that such collection completes the processing, exploitation, and dissemination process to generate actionable intelligence. To assess the intelligence it could expect to receive from the operational headquarters and the existing gaps, V Corps needed an adequate understanding of the MCLCC collection plan and its overall priorities for intelligence collection. V Corps also required an understanding of the collection plans and priorities of its adjacent multinational and allied corps headquarters to determine whether they were competing similar requirements. V Corps determined that listing both priority intelligence requirements and priority units for targeting best described the relevance of operational-level collection to the tactical level. This collective information enabled V Corps to identify collection gaps against enemy second-echelon divisions and brigades beyond the V Corps deep area that were not enemy operational or strategic reserves. Identifying these gaps early enabled V Corps to request collection against these

forces and empowered V Corps leaders to place their command emphasis on the need for resources to support collection and targeting during scheduled battle rhythm events

with the MCLCC.

V Corps G-2 CMD leveraged their daily corps collection management working group to address collection gap concerns within the established battle rhythm and to keep pace with the tempo of LSCO. During Avenger Triad 24, the collection management working group agenda expanded from a review of collection plans between V Corps and subordinate units to include an assessment and review of prioritized collection requests to the MCLCC for the next 96 hours. The V Corps G-2 CMD section developed a list and graphic overlay of proposed collection requests incorporating division and corps requirements for each air tasking order cycle. V Corps G-2 CMD invited adjacent corps collection managers to the collection management working group to facilitate collection plan sharing and discussion. This collaboration was equally relevant to the corps and division CMD sections, as adjacent unit collection activities overlapped both echelons' deep areas. The collection management working group's output was a finalized list of prioritized requests for collection to the MCLCC. These processes resulted in an improved method of establishing collection priorities and identifying collection gaps, creating a shared understanding of collection requirements across echelons.

Integrating Nonintelligence Assets for Collection

Near-peer adversaries in LSCO have great depth in their air defense and electronic warfare capabilities to block the United States from detecting targets using aerial collection platforms. This prevents U.S. units from detecting and shaping high-payoff targets in the deep fight intended to enable successful future ground combat operations in the close fight. Due to the limited availability of theater and national collection assets during LSCO, corps and divisions must develop new strategies to collect intelligence in the face of vast enemy air defense and electronic warfare assets. V Corps developed two approaches to this problem. First, V Corps integrated allied territorial defense force elements into its collection plan to conduct ground reconnaissance against collection requirements. This gave V Corps a deep sensing capability that was not vulnerable to enemy IADS. Second, V Corps massed cyberspace and electromagnetic activities (CEMA) effects to neutralize enemy IADS at pre-planned intervals to support collection for follow-on deep attacks from the V Corps combat aviation brigade.

V Corps had no assigned or attached territorial defense forces. Still, elements of the Polish Territorial Defense Forces and the Lithuanian Land Forces operated within the V Corps area of operations under their respective national chains of command.⁵ The V Corps G-2 shared the collection plan for the next 96 hours with its corresponding Territorial Defense Forces liaison officers (LNOs) at the corps command post. The LNOs provided responses from their units on whether they could deliver supplementary collection on identified named areas of interest. The two Territorial Defense Forces communicated collection on targets using spot reports through their LNOs to the V Corps G-2 operations cell. This method greatly facilitated timely intelligence reporting on enemy areas that V Corps aerial intelligence, surveillance, and reconnaissance assets could not access due to the air defense threat.

V Corps also deployed CEMA effects from theater and national assets to temporarily neutralize the enemy air defense systems and enable V Corps full-motion video collection. Like the MCLCC and theater intelligence, surveillance, and reconnaissance assets, these CEMA effects were limited in their availability across the battlespace. V Corps utilization of these effects supported corps out-of-contact attacks from the combat aviation brigade against enemy high-payoff targets. V Corps G-2 CMD integrated with V Corps planning operations for these deep attacks to allocate and request appropriate collection assets. V Corps adjusted its overall collection plan to account for these windows of CEMA effects to greatly enhance the survivability of assets and collection effectiveness.

Conclusion

The scale and tempo of the LSCO battlefield will continue to increase through technological innovation and expanded military investment from U.S. adversaries. We must recognize our processing and data transmission limitations as the U.S. Army and our allies adapt to these challenges. Tactical command posts must innovate new methods to process and prioritize intelligence requirements on the battlefield to leverage the vast capabilities of theater and national assets. Collaboration between the tactical- and operational-level CMD sections across the battlefield enables the efficient prioritization of collection requests to ensure that tactical units achieve victory in the close fight.



Endnotes

1. Department of the Army, Field Manual (FM) 3-94, *Armies, Corps, and Division Operations* (Washington DC: U.S. Government Publishing Office [GPO], 23 July 2021), 1-4-1-5.
2. Figure adapted from Figure 1-1, Department of the Army, Army Techniques Publication 2-19.3, *Corps and Division Intelligence Techniques* (Washington DC: U.S. GPO, 08 March 2023), 1-4.
3. Department of the Army, FM 2-0, *Intelligence* (Washington, DC: U.S. GPO, 01 October 2023) 8-28-8-29.
4. Figure adapted from Figure 7-2, Department of the Army, FM 2-0, *Intelligence*, 7-7.
5. For additional Information on Polish and Lithuanian territorial defense capabilities see Waldermar Skrzypczak, "Poland's Territorial Defense Force—Its Role, Significance and Tasks," (Pulaski Policy Papers Series, Casimir Pulaski Foundation, Warsaw, 2017), <https://pulaski.pl/en/polands-territorial-defence-force-its-role-significance-and-tasks/>; and "Land Force," Structure, Lithuanian Armed Forces, <https://kariuomene.lt/en/structure/land-force/23583>.

MAJ Brian Caniano serves as the V Corps G-2 collection manager in Fort Knox, KY. He holds a master of arts in North American history from Arizona State University.

U.S. Army Soldiers, assigned to the 6th Squadron, 8th Cavalry Regiment, and the Artificial Intelligence Integration Center, conduct drone test flights and software troubleshooting during Allied Spirit 24 at the Hohenfels Training Area, Joint Multinational Readiness Center, Germany, March 6, 2024. (U.S. Army photo by Micah Wilson)



ADDING ARTIFICIAL INTELLIGENCE TO THE TEAM

by Major Wesley Wood
and Sergeant Derrion Robinson

The Origin of the Idea

"We've got some work to do and not a lot of time to do it," the Collection Manager said, hustling back to our workspace from the division targeting coordination board. The division's plan for the combat aviation brigade's deep attack had just changed based on recent intelligence we had collected concerning a particular threat formation's strength. As the G-2 collection management team, we needed to adjust our information collection synchronization matrix (ICSM)—the scheduling and tasking tool for all division collection assets—to align with the new maneuver plan.

"It's not a significant change," the Collection Manager continued, handing over his notes. "We just need the second Gray Eagle line to focus on the named areas of interest five kilometers south of our original plan."

The Collection Manager and I exchanged glances. We both knew that any change to the ICSM was a big deal. Shifting even one collection asset would create redundant collection, gaps in coverage, and a lack of mixed assets—a scheduling nightmare that would require a fine-tooth comb review of our whole collection plan for that 24-hour period. This "not significant" change was going to take hours of rewriting the plan, and we didn't have hours. We had minutes.

We needed a more efficient way to process these changes without sacrificing our level of analysis. That's where the Non-classified Internet Protocol Router Generative Pre-Training Transformer, or NIPRGPT, came in.¹ This artificial intelligence (AI) tool enabled us to streamline our collection management, making quick adjustments possible without the usual headaches and providing a new level of collection plan analysis that we hadn't considered previously.

The Problem

In this article, we will discuss how to access a large language model (LLM), like NIPRGPT, and share basic knowledge about using one, asking it the right questions, and how a problem-solving AI assistant can catalyze your team.

We did not initially think of using AI when faced with the problem of adjusting our ICSM. We have used AI before on our smartphones and for personal projects. We have heard predictions from senior leaders like Andrew Evans, the Director of the Army's Intelligence, Surveillance, and Reconnaissance Task Force, who said, "We must learn to leverage AI to organize the world's information, reduce manpower requirements, make it useful, and position our people for speed and accuracy and delivering information to the commander for decision dominance."² Still, in our work we never really saw a current, practical application for AI. The idea of asking a LLM to "generate an information collection plan" seemed far-fetched. We doubted it would produce anything coherent or usable. However, we were out of viable options when we ran into the ICSM problem.

Our unit, the 11th Airborne Division, is the Army's newest division; consequently, we had a fraction of the manning of other Army divisions. At any given time, only three collection management Soldiers were working at our command post. We could not realistically collaborate and synchronize our efforts, whether internally with the team or externally with the rest of the staff, quickly enough to re-create and refine a quality product in the available time. The ICSM often incorporates over 670 data points, with tens of thousands of options for how and when to collect the information needed. Given the small staff and limited time available, the plan was sure to have inefficiencies and errors where we missed certain named areas of interest (NAIs), enemy formations, or targeting priorities requiring a collection focus. Although we applied an A-plus effort, by the end of our rushed edits, it felt like we were stuck with a C-minus product.

As we brainstormed, we found more issues. How could we ensure that our changes did not create redundant collection or gaps in coverage? How could we mix collection assets effectively without spending hours on manual adjustments? We knew that AI could provide some text-based solutions if we needed help writing Annex L (Information Collection), but the ICSM is a product that often needs to be communicated in a format best represented by a spreadsheet. LLMs can't produce spreadsheets. We needed a solution that could manage the complexity of our data and the urgency of our situation.

The Solution

We started asking basic questions on commercially available Generative Pre-training Transformer (GPT) services using prompts like, "Can you make a schedule for three people who cannot be in the same place at the same time?" "Can

you coordinate for each of those three people to visit ten different parks during a 24-hour period?" "Can you make sure that each of those people is at those parks for multiple hours?" And, finally, "Have the first person focus on parks 1 through 3." We reasoned that this generic situation could represent the problems we faced with the ICSM's development. Surprisingly, these prompts generated text-based answers that were very promising. We realized, though, that while a commercial GPT service could be helpful, its results were not useable. Since we were working with collection assets and operational planning, we needed to find a tool already familiar with Army doctrine and operations available on both controlled unclassified and classified systems.

We began researching Department of Defense LLMs that fit our requirements and identified several options. The most helpful and easiest to use on unclassified systems were NIPRGPT and CamoGPT³, but NIPRGPT, specifically, was more suited to our purpose and became our preferred app for testing the integration of AI into our team.

Through trial and error, we could make the LLM work for us rather than the other way around. Our desired end product was a copy-and-paste-worthy ICSM publishable as a division fighting product during a warfighter exercise. By using an AI assistant, we turned an error-prone process that cost us hours of time and included some emotional strain into a process that took minutes, had minimal errors, and allowed us to think about "big picture" problems instead of grinding out updated schedules for a dozen or more collection assets.

Ours was a niche problem set; however, the practical ways we applied AI may also apply to a variety of similar work issues. Accessing NIPRGPT is simple; after that, it is just a matter of asking the right questions.

Creating a NIPRGPT Account

Using your NIPR government email and user certification to authenticate your identity via the Department of Defense Global Directory, you can create a NIPRGPT account and access the platform. The NIPRGPT chat function, which provides the greatest familiarity to most users, allows users to engage in a conversation with the AI platform. The platform's developed algorithm answers users' questions based on a text database that is current as of December 2023. Responses to inquiries are "generated answers," meaning that the platform creates new information from its database. The platform also has a "Workspace" function that enables users to conduct queries of text-based uploaded documents such as articles, doctrine, or white papers. Additionally, the platform offers multiple help options for users who are unfamiliar with AI applications.

Our team's accounts were created within five minutes of applying, and we began testing the LLM. Our requests did not require approval by supervisors or other security managers—unlike many Army programs, access to NIPRGPT needed no

other credentialing. Finally, unlike commercial LLM subscriptions, there is zero cost to the unit.

Asking the Right Questions

The turnaround time for producing an AI-assisted product depends on asking the right questions. As we experimented with our inputs, key phrases and words like “text-based representation” and “spreadsheet” helped the AI tool understand the baseline product we wanted to create. Specifying numbered rows and lettered columns also helped communicate adjustments to the product’s layout.

The AI tool excels in its ability to ingest rules and requirements and make on-the-spot adjustments. For example, if a user inputs a rule like, “no information collection asset can collect on an area for more than 2 hours,” the AI tool will immediately change pre-coordinated collection timelines to comply with the new conditions. Setting up your rules and requirements at the beginning of product creation shortens the refinement process while minimizing the chances of human error that could result in coverage gaps and redundant collection.

Unfortunately, the chat function cannot retain rules and conditions from previous conversations. This is a known issue that NIPRGPT creators are working to address. Until the issue is resolved, users must re-enter the rules and questions at the beginning of each new chat to return to the desired baseline product.

The chat is also very literal, sometimes requiring users to refine their questions or requests. For example, if a user asks

the chat to make an Excel sheet or a spreadsheet, it will reply that it cannot do so—but it will give you step-by-step instructions on how to use Microsoft “Excel” to create a spreadsheet on your own. However, rewording the request to ask for a “text-based representation” of a spreadsheet will result in a spreadsheet that can be copied and pasted into an Excel workbook. Working through these minor issues is a simple learning process that is more than worth the minutes of effort.

After some trial and error with setting rules and asking the right questions, we had a working set of instructions on how to start a conversation with the LLM to produce the AI-adjusted products we needed within seconds. The LLM even produced a written summary of the adjustments we made to the instructions, which was a great help for understanding the fine-tuning process and rapidly created shared understanding across the collection management team on effectively using this tool.

A Practical Example

Building the rules and asking the right questions is an iterative process. In this example, we prompted NIPRGPT to help us refine our ICSM. We began by stating the product’s intent and providing some basic information. The initial interaction (Figure 1) was a request to build a synchronization spreadsheet for a 24-hour period with four assets.

Figure 2 reflects a request to adjust the spreadsheet’s layout to swap the information between the columns and rows, reassigning the time as column headers with the assets naming each row.

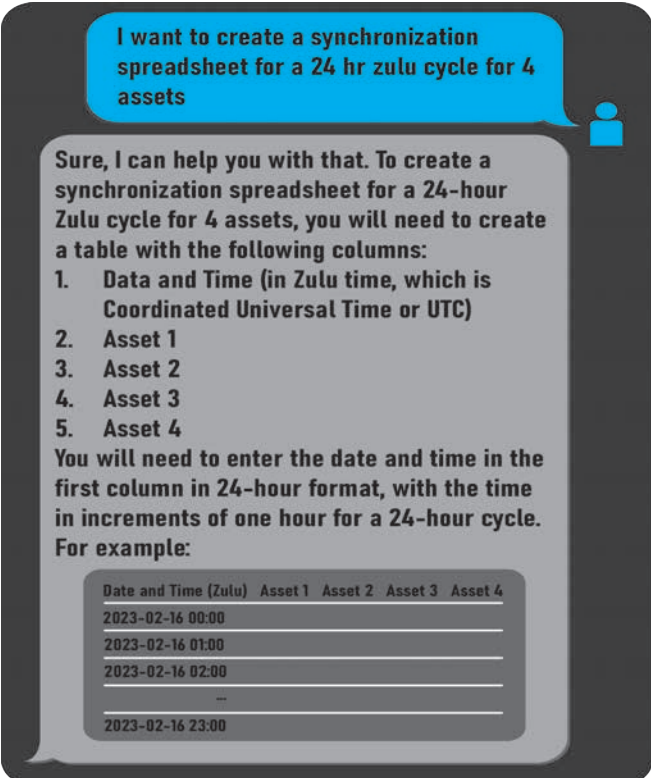


Figure 1. Initial Interaction with NIPRGPT (adapted from author original)

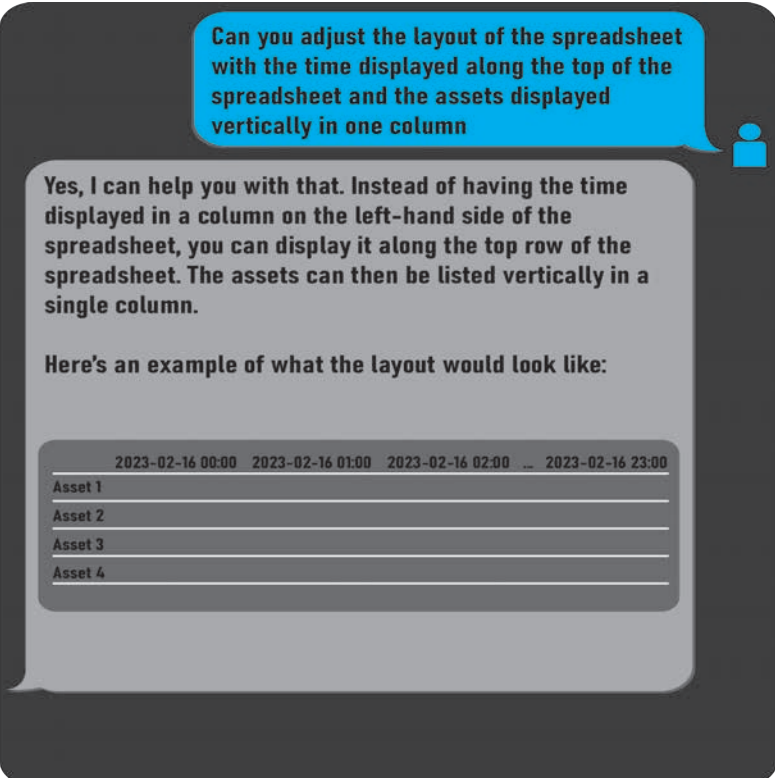


Figure 2. Request for Adjustment Interaction with NIPRGPT (adapted from author original)

After establishing the product layout, we provided the NAIs that needed to be built into the collection plan (Figure 3). These were numbered T-001 through T-020. Each asset was assigned specific NAIs for collection. We placed rules and conditions on the assets' collection scheme. The LLM then created a prioritized ICSM based on the information we provided.

Once the ICSM was created, we set specific collection requirements. At that point, we could also request a summary of each asset and NAI by total collection time to provide a holistic understanding and assessment of the collection plan. Figure 4 (on the next page) illustrates this end product, which we copied and pasted into an Excel spreadsheet without adjustments, requiring minimal user labor.

Other Potential Uses for Large Language Models

As our team continues to grow in understanding of how LLMs work, we can recognize many other potential applications. Examples include brainstorming priority intelligence requirements (PIRs), providing generalized indicators of enemy intent for the information collection matrix, and assisting with generating Annex Ls that are easier to digest for our subordinate units.

LLMs can be helpful when writing PIRs for different division operations. Instead of asking, "Can you write PIRs for our division operation?" we begin by describing some of the operation's mission variables—for example, "We are a division in the offense that is planning to use an air assault in a forested environment with rolling hills while facing a threat the size of a brigade that is set in an established defense.

What are the recommended PIRs?" Typically, this will result in a list of some example PIRs with a doctrinal breakdown by mission variables:

- ◆ Enemy.
 - ◆ Determine the location, range, and effectiveness of the air defense.
 - ◆ Locate and assess vulnerabilities of the threat's command and control.
 - ◆ Determine where the threat's reserve is and how it will be committed.
- ◆ Terrain.
 - ◆ Determine the weather patterns that will affect air assault operations.
 - ◆ Locate key terrain for landing areas around the objectives.
- ◆ Time.
 - ◆ Determine key moments of vulnerability in the threat's air defense, such as maintenance times or cloud cover, for a defense that isn't radar-assisted.
- ◆ Civil Considerations.
 - ◆ Determine how civilians will interfere with movement or how they will attempt to leave the conflict area.

Although the PIRs are broad and require additional work to tailor them before publishing, they are an excellent starting point. The LLM allows users to rapidly structure their own questions and form the recommended PIRs for the division commander.

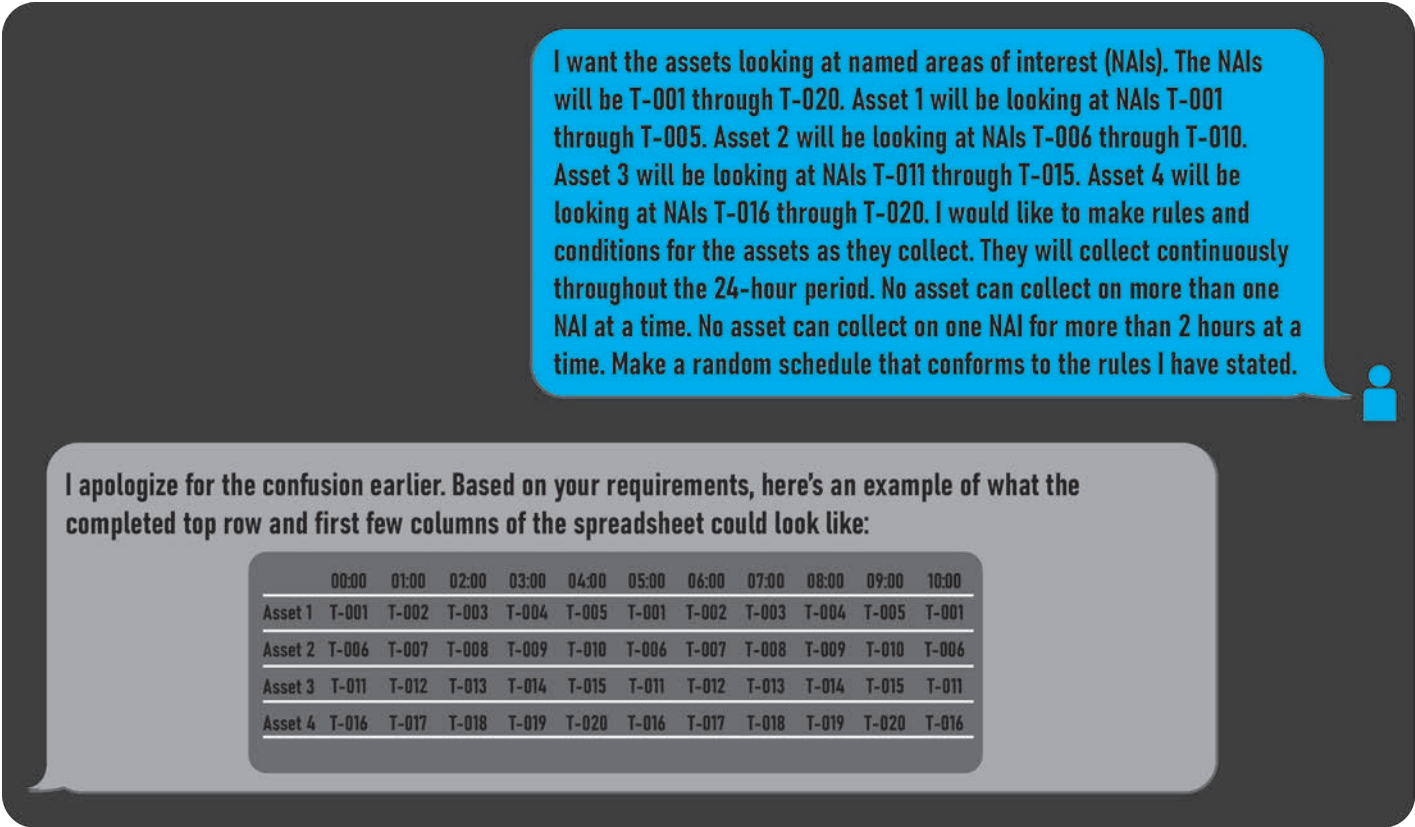


Figure 3. Named Areas of Interest Interaction with NIPRGPT (adapted from author original)

	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00
Asset 1	T-001	T-002	T-003	T-004	T-005	T-001	T-002	T-003	T-004	T-005	T-001	T-002	T-003
Asset 2	T-006	T-007	T-008	T-009	T-010	T-006	T-007	T-008	T-009	T-010	T-006	T-007	T-008
Asset 3	T-011	T-012	T-013	T-014	T-015	T-011	T-012	T-013	T-014	T-015	T-011	T-012	T-013
Asset 4	T-016	T-017	T-018	T-019	T-020	T-016	T-017	T-018	T-019	T-020	T-016	T-017	T-018

	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
Asset 1	T-004	T-005	T-001	T-002	T-003	T-004	T-005	T-001	T-002	T-003	T-004
Asset 2	T-009	T-010	T-006	T-007	T-008	T-009	T-010	T-006	T-007	T-008	T-009
Asset 3	T-014	T-015	T-011	T-012	T-013	T-014	T-015	T-011	T-012	T-013	T-014
Asset 4	T-019	T-020	T-016	T-017	T-018	T-019	T-020	T-016	T-017	T-018	T-019

Figure 4. End Product Spreadsheet (adapted from author original)

When humans create an information collection matrix, they often run out of ideas or fail to consider all warfighting functions when assessing indicators of enemy intent. LLMs can provide valuable assistance in thinking through different factors, and they can offer example indicators that we can sort through for our specific operation. For example, consider the following LLM query: “What are some indicators of a threat rotary wing attack battalion planning a long-range assault into an American division’s area of operations? Account for American tactical air defense and threat strategic enablers.” The LLM will produce a list of indicators that includes increased reconnaissance activity, forward deployment of forces, increased logistical support, preparations for suppressing enemy air defenses, enhanced communications, electronic warfare and cyber operations, use of strategic assets, pre-assault reconnaissance, simulation and training, and civilian information operations.

These are only a few examples of AI’s potential applications on the battlefield. Our only limits are our creativity and willingness to experiment with finding the right questions to ask.

Not the Tool for Every Task

While an LLM can help make tasks more efficient, it is not a suitable tool for every task. It is important to understand the limitations and weaknesses of LLMs in the field. For example, an LLM is a poor tool choice when sourcing direct quotes or gathering specifications on equipment, and although it is a powerful assistant it cannot do our jobs for us.

LLMs are not designed to pull direct quotes from doctrine or other published material. The NIPRGPT model is not intended to reference specific sources or documents directly; instead, it generates responses based on a broad survey of resources. This means that the LLM generates a response that a source *could* say or extrapolates what that source *would* say rather than directly referencing what that source *did* say. First Lieutenant Nicholas Brooks, one of the designers of NIPRGPT, recommends finding direct quotes using internet search functions. The NIPRGPT model is not connected to current internet content, so it may not reflect the exact wording or context of a specific quote or doctrinal reference.⁴

Likewise, LLMs are not well-suited for gathering equipment capabilities. The models’ responses are based on a wide range of sources and may not always reflect the most accurate or up-to-date information. For this type of information, it is always best to refer to official documentation, internal running estimates, and technical manuals. Once that information is in hand, it can be included in the LLM rules. This will result in more accurate assessments when the model is asked to help with understanding the best uses for specific capabilities.


AI can be a valuable teammate when generating ideas or providing information, but it cannot replace thorough planning or team collaboration. In his October 2024 appearance on The Convergence Podcast, Lieutenant Colonel Blaire Wilcox noted that “[AI] makes professionals better. It doesn’t necessarily make amateurs or the inexperienced [into] professionals.”⁵ There are no shortcuts to good professional

military staff work—but there are catalysts. While AI models cannot understand the nuances of a specific situation or develop a plan independently, they can help generate ideas and prevent the kind of human errors that can be created when processing substantial amounts of data, as was our situation with the ICSM.

By treating AI like any Soldier, we can trust it to provide the best information it has. As with any team member, though, it is important to conduct regular inspections and reviews to ensure that the information it provides is accurate and relevant while continuing to coach it to improve its performance continuously.

Conclusion

Integrating AI into staff processes, specifically a LLM like NIPRGPT, has proven to be a valuable tool for streamlining tasks and providing a new level of analysis in the 11th Airborne Division. We used it to adjust our ICSM quickly and continue to find other uses for it as we develop our standard operating procedures. The practical applications across all staff processes in a G-2 section, the staff sections of the other warfighting functions, and beyond into other echelons of command are limitless.

We cannot allow ourselves to perceive AI as a tool that needs to be perfect and provide independent answers without human input and analysis. It must be employed practically. As our experience demonstrates, the practical application of AI has the potential to improve the quality and efficiency of any team's performance. How can you add AI to your team? 

Endnotes

1. Mikayla Easley, "Army Implements Generative AI Platform to cArmy Cloud Environment," DefenseScoop, September 10, 2024, <https://defensescoop.com/2024/09/10/army-generative-ai-capability-carmy-cloud/>.
2. Mark Pomerleau, "Army's ISR Task Force Looking to Apply AI to Intel Data Sets," DefenseScoop, October 17, 2024, <https://defensescoop.com/2024/10/17/army-isr-task-force-apply-ai-intel-data-sets/>.
3. Lori McFate, "Operationalizing Science at JMC with Artificial Intelligence and Machine Learning," U.S. Army Worldwide News, October 29, 2024, https://www.army.mil/article/280941/operationalizing_science_at_jmc_with_artificial_intelligence_and_machine_learning.
4. First Lieutenant Nicholas Brooks, telephone discussion with authors, n.d.
5. Luke Shabro and Matt Santaspirit, "107: Hybrid Intelligence: Sustaining Adversary Overmatch with Dr. Billy Barry, LTC Blair Wilcox, & TIM," October 25, 2024, in The Convergence, produced by The Army Mad Scientists, podcast, 58:52, <https://theconvergence.castos.com/episodes/107-hybrid-intelligence-sustaining-adversary-overmatch-with-dr-billy-barry-ltc-blair-wilcox-tim>.

MAJ Wesley Wood currently serves as the collection manager for the 11th Airborne Division. He previously served as the Deputy G-2 for the 11th Airborne Division, as the Airborne Task Force Observer, Controller, Trainer at the National Training Center, and as the Commander, Military Intelligence Company, 1st Stryker Brigade Combat Team, 25th Infantry Division, Fort Wainwright, AK.

SGT Derrion Robinson currently serves as a collection management noncommissioned officer for the 11th Airborne Division. He previously served as a fusion analyst in the 4th Infantry Division G-2, as a security manager in the 4th Infantry Division G-2, and as a S-2 analyst at the 1st Battalion, 41st Infantry Regiment, Fort Carson, CO.



INTELLIGENCE AT THE SPEED OF MODERN WARFARE: XVIII AIRBORNE CORPS EXPERIMENTATION WITH THE ARMY INTELLIGENCE DATA PLATFORM

BY CHIEF WARRANT OFFICER 3 JOHN BARTLETT

On a future battlefield a U.S. Army corps executes a joint forcible entry operation into terrain currently occupied and defended by an adversary nation state. This fictional enemy enjoys numerical superiority and a dense antiaccess, area-denial system of systems, including formidable sensing capabilities, integrated air defenses, and an integrated surface-to-surface fires complex employing tube artillery, rockets, and longer-range missiles. The corps must rapidly gain an information advantage—gains realized from a comprehensive understanding of the battlefield while denying the threat any ability to achieve its information goals—to defeat this bristling, lethal, and entrenched enemy force. To accomplish this, the future corps must leverage the latest available technology to obtain, aggregate, interpret, and disseminate large amounts of data at speed to enable the commander's desired approach. Gaining and maintaining this data advantage enables the corps to converge the right effects at the right time in order to address key adversary capabilities and create opportunities for maneuver forces to close with and destroy the enemy.

Introduction

XVIII Airborne Corps G-2 leveraged an emerging data management technology, the Army Intelligence Data Platform (AIDP),¹ to fight and win in a scenario much like the preceding vignette during a recent corps warfighter exercise. In such an environment, the intelligence enterprise must employ technology to maintain pace with the increasing speed of war. The Army must progress beyond 12- or 24-hour reporting cycles, PDF files attached to emails, reviewed and published intelligence information reports, and significant activity storyboards. The intelligence community is a data-centric, data-driven profession responsible for informing decision makers by providing the latest and most accurate information at the speed of now. Having an information advantage supports situational understanding and enables decision advantage. To achieve that information advantage, XVIII Airborne Corps employed AIDP during Warfighter Exercise 24-05 (WFX 24-05) as the primary intelligence warfighting system to execute the following key G-2 tasks:

- ◆ Federate AIDP across echelons.
- ◆ Achieve shared understanding.
- ◆ Execute intelligence support to targeting.
- ◆ Perform battle damage assessments (BDAs).
- ◆ Conduct collection management.

The foundational framework of AIDP forms a collaborative platform providing the capability to conduct intelligence preparation of the operational environment in support of mission analysis at the corps level and below. The tools in AIDP provide an intelligence-specific, discipline-agnostic collaborative environment in which tactical echelons communicate in near real time. AIDP can depict the common intelligence picture (CIP) graphically, in conjunction with other staff overlays and estimates. WFX 24-05 provided an environment of speed and complexity, challenging the XVIII Airborne Corps G-2 to adapt while in contact and to meet planning and operational requirements. While AIDP's framework and user interface enabled the G-2 to achieve shared understanding across echelons in near real time, three key areas presented challenges: knowledge management, intelligence support to targeting execution, and single-source intelligence integration.

Working within AIDP's cloud environment presented both advantages and disadvantages. The collaborative tool suite in AIDP provided the primary advantage by enabling synchronization and integration both internally and externally across the battlefield in near real time. This feature was a critical factor to achieving shared understanding across echelons. During WFX 24-05, the XVIII Airborne Corps intelligence process centered around the G-2's "Big 5" production: the CIP, intelligence running estimate, event template, intelligence collection synchronization matrix, and BDA. The G-2 planned to develop and maintain these production outputs within AIDP using live data. AIDP's design enabled "the integration of intelligence and information from all relevant sources in order to analyze situations or conditions that impact operations."² AIDP's foundational toolsets, Gaia and Dossier,³ enabled the XVIII Airborne Corps G-2 to maintain these products in real time while simultaneously sharing data and analysis across the formation; however, there were still technological, capability, and knowledge management limitations.

When using AIDP as the primary production toolsuite, analysis did not stop for production; instead, analysis *became* production. Within AIDP, real-time analysis and the ability to modify battlespace geometry rapidly proved remarkably successful. Analysts could modify tactical graphics, manipulate visual analytical tools (e.g., range rings/fans, modified combined obstacle overlays), and rapidly share data, which outpaced the previous production cycles utilizing legacy systems. Creating shared understanding at the pace of operations

facilitated flexible commander prioritization. It truncated the decision-making cycle, relying on orders or dedicated battle rhythm events to publish enemy situation and graphic overlays through the Defense Digital Service.

The XVIII Airborne Corps G-2 created links and data feeds, constantly pushing and pulling data, to ensure the CIP remained current and shared with the common operational picture within the Maven Smart System (MSS).⁴ MSS is the XVIII Airborne Corps primary mission command system, supporting plans, operations, and fires. This deviation from historical production cycles enabled the G-2 to support deep operations by maintaining a CIP of enemy forces throughout the area of interest.⁵ It also enabled the G-2 to provide accurate and timely input into the friendly decision support matrix. While these benefits are clear game changers, the current architecture and interoperability between AIDP and MSS are imperfect. However, AIDP is consistently improving. To address technical issues related to interoperability between MSS and AIDP, field service representatives are working directly with units through Soldier touchpoints to capture and resolve problems, build data link connections, and assist in developing software tools to support the analyst.

Knowledge Management

Developing a knowledge management plan, utilizing the primary, alternate, contingency, and emergency (known as PACE) communications plan, and reinforcing digital discipline is key when working in a live data cloud environment. Prior to XVIII Airborne Corps G-2 implementing a knowledge management plan, analysts found knowledge management cumbersome because AIDP allows real-time access and information flow with constant inputs, edits, and refinements from 100-plus users. The XVIII Airborne Corps G-2 quickly identified maintaining quality assurance, quality control, and version control as critical to ensuring the continued accuracy of the G-2's "Big 5" production. The G-2 discovered that the absence of permissions, quality assurance, and quality control capabilities to manage AIDP objects at echelon significantly affected current operations, future operations, and fusion workflows. Subordinate echelons could not refine objects from the bottom-up without impacting the corps picture, and any update to an object in the system impacted every unit and user utilizing AIDP. Leveraging AIDP's chat service enabled the quick dissemination of guidance across the formation to reinforce digital discipline, establish new tactics, techniques, and procedures (TTPs), and confirm acknowledgment from subordinates. Knowledge management is naturally difficult, especially when dealing with live data. AIDP enabled the rapid identification of solutions and dissemination of TTPs all within the platform, showcasing the system's flexibility and allowing the G-2 to transform in contact.

Intelligence Support to Targeting

Regarding systems and their interoperability, passing objects between AIDP and MSS, specifically within the Target Workbench tool,⁶ was significantly limited during WFX 24-05. The bifurcation of observation and object-based production created a significant time gap (typically 10 minutes) before the data populated into Gaia. This time gap caused a cascading effect that restricted the XVIII Airborne Corps ability to conduct dynamic targeting, especially in the fast-paced large-scale combat operations environment.

Conducting deliberate targeting using objects created in AIDP also had its limits. The XVIII Airborne Corps G-2 produced the enemy order of battle using AIDP's Graph tool, creating objects and associating key pieces of equipment for each unit. There were two reasons for this: first, these objects would feed BDA, and second, this would allow analysts and targeteers to gain efficiencies by associating information and intelligence to the objects to build the "target packet" in AIDP instead of the previously used PowerPoint slide deck.

Unfortunately, the target information could not be passed to MSS. This limitation forced XVIII Airborne Corps G-2's targeting team to operate on MSS almost exclusively to support fires and to use the Target Workbench residing on MSS. Once targets were actioned and the collection had confirmed or denied effects on the target, AIDP ingested the observation reports. Analysts in the BDA cell then manually sorted and filtered those reports to associate them with the specific target. This is an instance where XVIII Airborne Corps identified slow, inefficient processes but could not implement a quick-fix solution during WFX 24-05. Nevertheless, it provided a key opportunity for the G-2 to provide feedback on the issue and work directly with AIDP representatives to begin investigating a solution—a practical demonstration of how AIDP supports transformation in the intelligence enterprise, allowing it to fight at the speed of data in conflict.

Obstacles to Single-Source Integration

Integrating single-source intelligence analysis into AIDP is crucial for intelligence to support both targeting and situational awareness during large-scale combat operations. Intelligence professionals work from the assumption that the enemy utilizes fast emplacement, engagement, and displacement of systems to bolster survivability. As a rule, a well-trained crew

Analyzing and disseminating a near real-time indication of target activity is essential for enabling the intelligence warfighting function to feed the targeting process.

can displace within 10 to 15 minutes, making targeting timelines exceptionally tight. Analyzing and disseminating a near real-time indication of target activity is essential for enabling the intelligence warfighting function to feed the targeting process. Moreover, intelligence analysts must provide as much time as possible for the targeting and fires cells to do their jobs, meaning that intelligence should be disseminated no more than 10 minutes from discovery. Integrating single-source analysis tools into AIDP would shorten production timelines and (assuming AIDP will be able to communicate directly with systems used

by the fires cell) could allow for targeting and engagement of enemy systems before their displacement.

Before continuing, it is important to note that AIDP was initially designed for military intelligence brigades-theater to "set the theater" and conduct intelligence preparation of the operational environment. It is a tool still under development. AIDP does not currently host organic capabilities or tools to support single-source disciplines. Because of this, single-source analysts encountered many challenges using AIDP to its full potential in command post exercises before and during WFX 24-05, primarily because the tools were still in development or otherwise not yet released. The next evolution of AIDP will include All Source II/Intel Apps, which will address some of the gaps.

Nevertheless, despite unavailable capabilities and toolsets, single-source analysts worked with field service representatives during the exercise to develop workarounds. This allowed the quick development of data paths, building tools for data correlation, and ingesting analysis from other platforms into AIDP. Additionally, the coding foundation in AIDP allows units to innovate and develop their own tools to aid in analysis, something previous military intelligence programs of record did not allow. This transformation in contact enabled all-source intelligence to provide a timely and accurate CIP.

From a single-source perspective, the first challenge for the signals intelligence (SIGINT) section centered around training. Single-source intelligence analysts did not participate in AIDP's fielding training because the system was released as an all-source-specific suite of tools. XVIII Airborne Corps SIGINT analysts first utilized AIDP during the command post exercise immediately preceding WFX 24-05. This lack of training and experience meant SIGINT analysts learned the

capabilities and limitations of AIDP in real time while participating in the exercise. SIGINT analysts overcame the initial knowledge gap and achieved basic proficiency with AIDP by the end of the command post exercise before the beginning of the warfighter exercise.

A second issue is that AIDP does not possess a SIGINT analysis toolset. SIGINT analysts must accomplish very specific information processing tasks. Although SIGINT reports ingested into AIDP constitute “finished” reporting, SIGINT analysts need certain second-order analysis tools to provide value to the all-source CIP. These tools are not yet present in AIDP. XVIII Airborne Corps SIGINT analysts could not convolve multiple ellipses to provide better targets for deliberate and dynamic targeting efforts. They could not process geolocational lines of bearing to pinpoint signals of interest. Additionally, AIDP could not determine how a signal would propagate across varying terrain or environmental conditions.

For SIGINT analysts to process and analyze the sheer volume of data expected during large-scale combat operations, manipulating the metadata of reports quickly and efficiently to provide greater situational understanding is necessary. AIDP can parse, filter, and cross-reference data and metadata from reports reasonably well; however, the learning curve for achieving this function used time SIGINT analysts could not easily spare during the exercise. To address this, the SIGINT analysts adjusted their TTPs, exporting the datasets from AIDP and importing them into FADE/MIST, a National Reconnaissance Office-sponsored toolset capable of processing metadata in a useful way.⁷ Efforts to reintegrate this data into AIDP to support situational understanding and all-source analytics were unsuccessful.

Finally, the timeliness of data integration also created issues. The exercise data path created significant latency between the time of intercept and the time of analysis. As the exercise progressed, AIDP programmers attempted to address that latency but could not mitigate it enough for SIGINT analysts to use the collection to support the dynamic targeting process. As a result, SIGINT analysts supporting the dynamic targeting process moved “upstream” to the U.S. Army Intelligence and Security Command Cloud Initiative instance, which allowed them to submit targets fast enough for the fires section to prosecute them.

Implementing a suite of SIGINT-specific analysis tools in AIDP could address many of the issues experienced by the XVIII Airborne Corps SIGINT section. This suite could include an ellipse convolving tool, a line-of-bearing generator, and a line-of-sight/radio horizon tool. Improving the metadata analysis capability in AIDP to accommodate the types of analysis used by SIGINT analysts or enabling data exported from AIDP for analysis using another tool to reintegrate after analysis could greatly enhance situational understanding.

Enabling AIDP to interface as directly with exercise dataflows as with its real-world counterparts would allow intelligence analysts to train more effectively and operate as they would in real-world situations.

Conclusion

If the intelligence enterprise is to innovate, adapt, and transform in contact, intelligence professionals must understand both the doctrine and the coding foundation upon which AIDP is built. AIDP’s foundational tools, Gaia and Dossier, enabled the XVIII Airborne Corps G-2 to maintain necessary products in real time while simultaneously sharing data and analysis across the formation. This sharing is essential to gain and sustain decision advantage over our adversaries on the modern battlefield. Throughout WFX 24-05, XVIII Airborne Corps encountered and overcame significant technological, capability, and knowledge management limitations. The end user is key to identifying AIDP’s limitations, and recognizing this allows intelligence professionals to demonstrate creativity and exploration in developing new tools and tradecrafts. Given this autonomy, intelligence professionals, collaborating with expert coders and software engineers, can quickly adjust, modify, enhance, and improve AIDP. The current iteration of AIDP does not service all requirements for each intelligence discipline, does not include intuitive workflows to create doctrinal products for which the intelligence enterprise is responsible, and does not ingest all required data feeds. Nevertheless, AIDP does provide a solid foundation, enabling the Army intelligence community to transform at speed to overcome the increasing national security challenges of today, as well as those of tomorrow and beyond. 🌟

Endnotes

1. Shawn Nesaw, “Cloud-Based Intel Tool AIDP Rolls Out to Army Units Globally,” News, Program Executive Office–Intelligence, Electronic Warfare and Sensors, October 9, 2024, <https://peoews.army.mil/2024/10/09/277811/>; and “Army Intelligence Data Platform (“AIDP”),” Palantir Technologies Inc., 2003, https://www.palantir.com/assets/xrfr7uokpv1b/7JAWiSA6yA5MLDAD1AsX7I/c256437b1c29bad5747633123957b4b7/AIDP_AUSA_2_updated2.pdf.
2. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 4-1.
3. “Platform Capabilities,” Secure Collaboration, Palantir Technologies Inc., 2024, <https://www.palantir.com/offers/defense/secure-collaboration/capabilities/>. Gaia is a battlefield visualization tool that integrates intelligence and operations data into a single GUI. Dossier is a tool that assists users in building orders, mission plans, and intelligence reports; it restricts data appropriately based on security clearances and produces a detailed audit trail of all activity.
4. “Maven Smart System,” Missile Defense Advocacy Alliance, 2004, <https://missiledefenseadvocacy.org/maven-smart-system/>.
5. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. GPO, 01 October 2022), 6-37.
6. “Target Workbench,” Palantir Technologies Inc., 2023, https://www.palantir.com/assets/xrfr7uokpv1b/1lqzwzpmemtBSm98TNCczao/49bbc30cb-ec4d2d4d189ab27bd07376c/Palantir_Target_Workbench_1_.pdf. Target

Workbench is a target management tool that assists intelligence and operations users to collaborate throughout the targeting process.

7. “Fusion Analysis & Development Effort,” (slicksheet, National Conference Services, Columbia, MD, April 2021), https://www.ncsi.com/wp-content/uploads/2021/04/FADE_Slicksheet_Releasable.pdf; and “Multi-INT Spatial Temporal (MIST) Toolsuite: Discover Hidden Patterns Within Complex Data,” (factsheet, CACI, Arlington, VA, 2020), https://www.caci.com/sites/default/files/2020-02/F367_2002_MIST.pdf.

CW3 John Bartlett currently serves as the XVIII Airborne Corps G-2 Analysis and Control Element Production Chief where he is developing tactics, techniques, and procedures for employing the Army Intelligence Data Platform in training and real-world missions. Throughout his 17-plus years in the military, Mr. Bartlett has served at multiple echelons in the conventional and special operations communities, to include 4 years forward deployed to the U.S. Central Command area of responsibility.

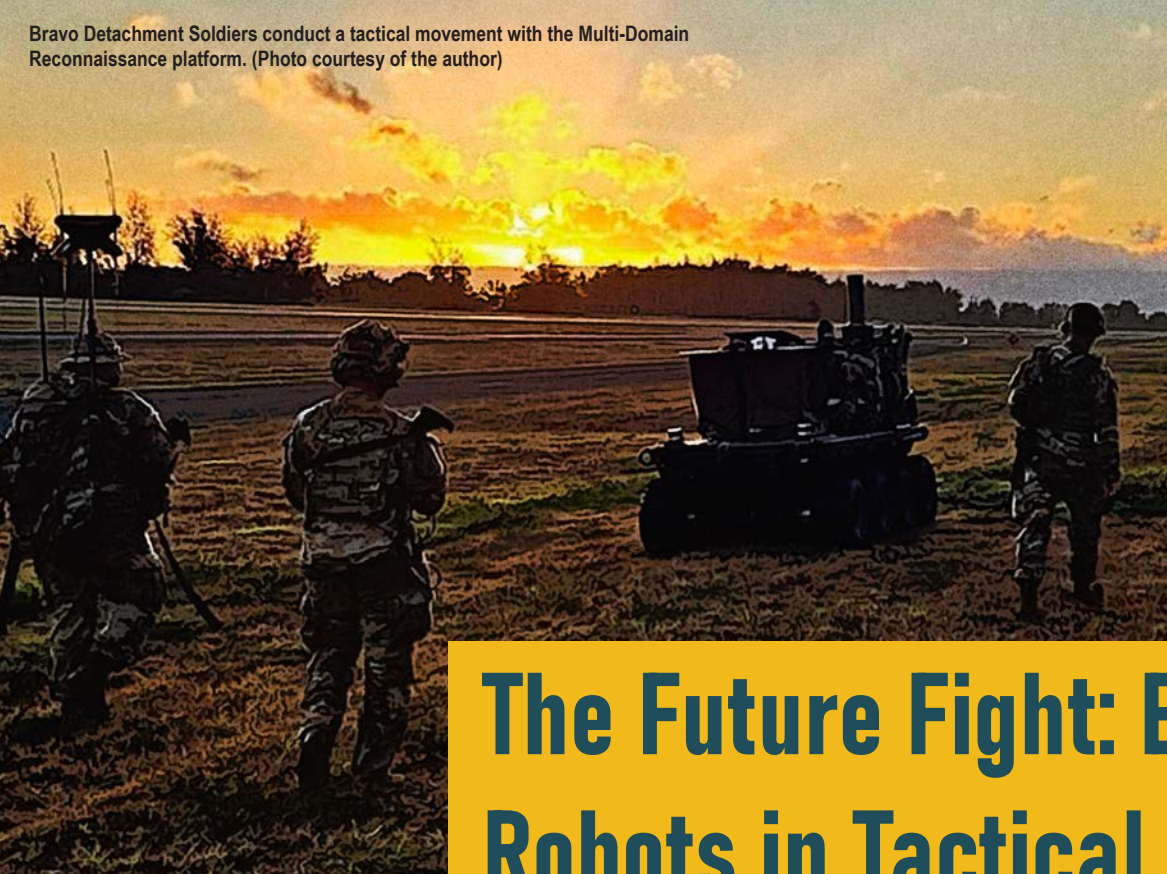
Contributors:

LTC Evan Westgate is the XVIII Airborne Corps G-2 Analysis and Control Element Chief.

CW4 Farley Covington is the XVIII Airborne Corps G-2 Senior Signals Intelligence Technician.

CW4 Brandon Mesa is the XVIII Airborne Corps G-2 Senior Intelligence Technician.

CW3 Michael Francisco is the XVIII Airborne Corps G-2 Fusion Intelligence Technician.



The Future Fight: Employing Robots in Tactical Formations

by Captain Leland Lancaster

Introduction: Project Context

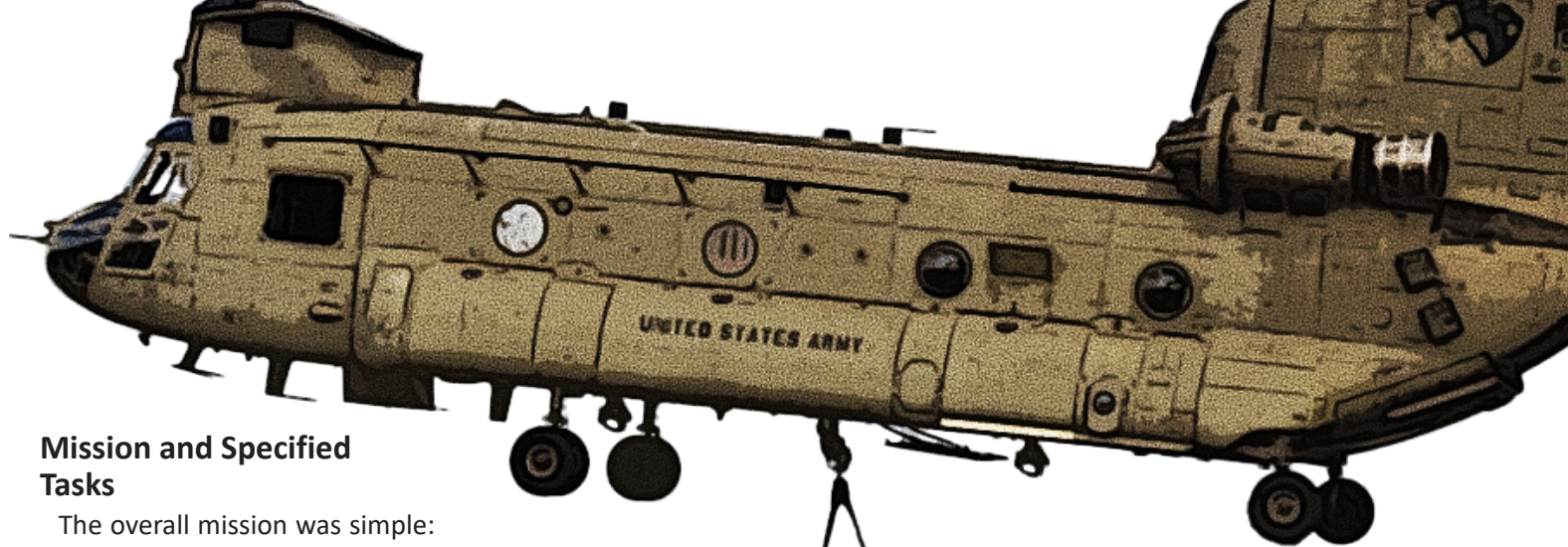
Military intelligence (MI) formations require collection assets capable of finding the enemy and supplying target data in a timely manner. Refining the sensor-to-shooter process is critical to enabling freedom of maneuver on the ground, and this refinement is primarily contingent on technological advances. The Rapid Defense Experimentation Reserve is one of the U.S. Department of Defense's (DOD's) primary means of quickly modernizing the force, and equipping Soldiers with robotic combat vehicles (RCVs) is one of their current lines of effort.¹ After the DOD allocated funds toward developing autonomous RCVs, leaders from the U.S. Army Combat Capabilities Development Command (DEVCOM) contacted tactical intelligence units within the U.S. Indo-Pacific Command to coordinate testing.

In August 2024, as part of this larger DOD initiative, the 125th Intelligence and Electronic Warfare Battalion (IEW BN) at Schofield Barracks, Hawaii, fielded and experimented with four fully autonomous Small Multipurpose Equipment Transports, or S-METs,² RCVs provided by the DEVCOM Ground Vehicle Systems Center. One was equipped with a Common Remotely Operated Weapon Station (CROWS) lethality system,³ capable of mounting and autonomously firing crew-served weapons; this unit would provide direct-fire support. The remaining three robots came equipped with a tethered unmanned aerial system (TeUAS) on top of each platform

capable of direction finding and full-motion video; these would provide deep sensing in support of targeting.

After agreeing to the project, the 125th IEW BN tasked its Bravo Detachment to conduct the experiment. Bravo Detachment serves as the battalion's expeditionary element, and experimenting with RCVs gave the detachment additional equipment to support its signals intelligence (SIGINT) and processing, exploitation, and dissemination mission. Of note, none of the equipment used during this experiment is organic to the 125th IEW BN. Bravo Detachment primarily employs man-packable SIGINT systems in conjunction with small unmanned aircraft systems (UASs) to enable targeting, and they are the first unit in the Army to field this experimental equipment package.

The Ground Vehicle Systems Center provided three weeks of new equipment training; then, during the experimentation phase, the battalion tested these systems in the field during a brigade training exercise. For context, equipping infantry units with RCVs is not uncommon, but units typically use these robots to transport equipment. Employing RCVs as a collection platform gave Soldiers in the 125th IEW BN an additional tool capable of providing timely and accurate intelligence. Ultimately, this experiment provided valuable feedback on what worked, what didn't, and how to utilize the platform effectively in the future to enable Soldiers on the ground.



Mission and Specified Tasks

The overall mission was simple: remotely maneuver multiple unmanned autonomous RCVs ahead of the forward line of own troops to achieve a sensing capability. The goal was to get RCVs into the hands of Soldiers to employ in a tactical scenario. Within that scenario, project developers planned to test the command and control of multiple vehicles, payloads, and sensors. Ideally, system operators would direct each autonomous RCV to its hide site, remotely launch the TeUAS, and populate target data on the end user's common intelligence picture. Executing this project required an extensive equipment list, primarily four RCVs and one workstation (known as the Global Expeditionary Miniature Mission Interface, or GEMMI⁴) designed to control all four platforms simultaneously.

Three Multi-Domain Reconnaissance (MDR) RCVs. These platforms were the primary focus of the battalion's testing, and each platform consisted of the following:

- ◆ Eight-wheeled robotic S-MET capable of obstacle avoidance.
- ◆ TeUAS equipped with a full-motion video and direction-finding payload (300-foot tether).
- ◆ Extended range tactical communications.
- ◆ Beyond line-of-sight (BLOS) sensing and targeting capability via Starlink.
- ◆ Line-of-sight (LOS) sensing ahead of human maneuver.
- ◆ Electro-optical/infrared sensing to detect and identify targets.
- ◆ Counter UAS sensing; capable of small UAS detection and defeat.
- ◆ Handheld remote capable of LOS driving.
- ◆ Operator control unit tablet capable of route mission planning, LOS driving, and TeUAS flight operations control.

One Direct-Fire Lethality RCV. Soldiers from the 125th IEW BN and the 25th Infantry Division's 2nd Light Brigade Combat

Team (2LBCT) received new equipment training on this system but did not employ it in a tactical scenario. This platform consisted of the following:

- ◆ Eight-wheeled robotic S-MET capable of obstacle avoidance.
- ◆ Lethality Platform—M152 CROWS capable of mounting most crew-served weapons.
- ◆ 15-foot mast capable of providing Soldiers with an added visual tool (i.e., sight over tall obstacles).
- ◆ Extended range tactical communications.
- ◆ BLOS sensing and targeting capability via Starlink.
- ◆ LOS sensing ahead of human maneuver.
- ◆ Handheld remote capable of LOS driving.
- ◆ Operator control unit tablet capable of route mission planning, LOS driving, and TeUAS flight operations control.

Global Expeditionary Miniature Mission Interface (GEMMI).

This is an open, high-performance, low-footprint ground control workstation with the following capabilities:

- ◆ Computer display kits allowing Soldiers to operate the RCVs' BLOS via Starlink.
- ◆ Autonomous RCV control.
- ◆ Autonomous TeUAS launch, flight, and landing.
- ◆ Ability to receive full-motion video from the three MDR RCVs.
- ◆ Ability to receive lines of bearing from the direction-finding sensor.
- ◆ Ability to fire crew-served weapons BLOS (not evaluated during this iteration).

Execution

The 125th IEW BN experimented over six weeks in three phases: new equipment training, tactical employment, and a distinguished visitor demonstration.

Phase One—New Equipment Training (three weeks). After nearly a year of planning and preparation, new equipment training began in mid-July with the arrival of civilian personnel and all experimental equipment at Schofield Barracks. Approximately 30 contractors and DOD civilians flew to Oahu from all over the continental United States to help facilitate this fielding. Over three weeks, project leads assembled the robots, and Bravo Detachment Soldiers received four sequential blocks of instruction. The training progression covered RCV mobility, TeUAS flight, lethality employment, and GEMMI BLOS autonomous operations. Each Soldier in Bravo Detachment's signals collection teams (SCTs) certified on driving the RCVs, flying the TeUAS with handheld remotes, and passing control of the system to GEMMI operators. The detachment's SIGINT operations cell (SOC) additionally certified on GEMMI BLOS operations, which included passing target data to end users via tactical communications. New equipment training also covered maintenance, initial equipment inventories, and S-MET towing operations with military vehicles. It took longer than initially expected to get the equipment assembled and online, so operations started slowly. Despite these initial hiccups, the detachment's SCTs deployed to the field in time for the exercise kickoff.

Phase Two—Exercise Execution (two weeks). Bravo Detachment integrated its SOC and three SCTs into two weeks of 2LBCT's company situational training exercise lanes in early August. The project's civilians also spent time in the field observing testing and providing maintenance and technological support. Bravo Detachment trained and operated at the same location as 2LBCT during the exercise. However, it did not truly embed with a maneuver unit simply because the project was still in its initial stages. Despite some system limitations, testing the equipment in a live environment gave project managers valuable feedback.

The exercise began with the detachment's SOC postured at 2LBCT's headquarters at Schofield Barracks and the SCTs established in hide sites positioned in training areas across the island. The SCTs in the field received onsite assistance from both civilian contractors providing system support and Pacific Foundry supplying Stratomist emitters that allowed sensors on the TeUASs to obtain lines of bearing. For the duration of the exercise, Bravo Detachment Soldiers utilized the three MDR RCVs to provide force protection support to 2LBCT elements.


During tactical employment, SCT Soldiers on the ground maintained primary control of the system. Operators used the operator control units to move the RCVs during mounted and dismounted operations, and the SCTs conducted handovers

with SOC operators manning the GEMMI in the rear while halted. Once at a standstill, the operator, either on the ground or using the GEMMI, flew the TeUAS to its desired altitude. At altitude, operators processed the full-motion video feed, controlled the electro-optical/infrared payload, and tasked the direction-finding payload to receive lines of bearing. By the end of the exercise, all three systems functioned as one unit to geolocate targets up to five kilometers away and pass data back to the SOC in the rear.

Initial feedback from the detachment's Soldiers was primarily positive, but there was concern about the RCV's lack of mobility. Testing revealed that the system has difficulty navigating jungle terrain and cannot be driven with the TeUAS mounted on top. Despite these limitations, our Soldiers found value in fielding the equipment to an MI formation. The platforms allowed the SCTs to position themselves in the brigade's rear area while simultaneously collecting on targets ahead of the forward line of own troops. Once RCV mobility improves and project engineers correct technological bugs in the GEMMI and TeUAS, the system will certainly enhance an MI formation's ability to collect and pass targetable data.

Phase Three—Distinguished Visitor Demonstration (one week). Experimentation concluded with a distinguished visitor demonstration to two Senate Appropriations Committee Defense Staff members and a senior leader delegation from the U.S. Army Pacific. Bravo Detachment Soldiers rehearsed for one week before execution, and the briefing concluded with a live demonstration during which Soldiers highlighted the capabilities, limitations, and real-world implementation of each system. The distinguished visitors were particularly interested in how the GEMMI passed information to fires elements, whether there is a plan to have a direct-link connection to a direct fire system, and whether there are plans to improve RCV mobility moving forward. There are plans to address all three of these issues, and project leads have taken the distinguished visitors' feedback for action.

Conclusion

The Army's first iteration of RCV testing at the tactical level was a resounding success. The system is not deployable in its current form; improvements are needed to make the platform more mobile, durable, and technologically dependable. Nevertheless, the 125th IEW BN's experimentation allowed program developers to assess the system's performance during live training in a harsh jungle environment. Feedback from maneuver commanders, senior intelligence professionals, and Bravo Detachment's Soldiers will allow project leads to make improvements, and the detachment will continue experimenting with this equipment. Adding SIGINT equipment to the top of the platform's mast, conducting sling load operations with the RCVs, and improving the system's BLOS communications are just a few ideas for improvement moving forward. 

Author's Note: After this article was written, Bravo Detachment, 125th IEW BN, and 25th Infantry Division's Combat Aviation Brigade conducted sling load testing on the MDR platform. Testing consisted of a CH-47 Chinook air assaulting the MDR platform and an SCT hide site at two landing zones on Schofield Barracks, Hawaii. This training was the first time the Army conducted sling load operations with the robotic MDR platform, and it was one of the first external sling load operations for the S-MET. Testing confirmed that sling loading the MDR platform is an efficient and realistic method of maneuvering this system across the battlefield. Bravo Detachment's SCTs rigged the load at hide sites in under 15 minutes; subsequent internal and external load operations with a CH-47 took under 5 minutes.

Overall, these RCVs enhance a tactical MI formation's ability to sense deep while reducing risk to the force. It's encouraging that the 125th IEW BN could field these robots, receive training from subject matter experts, and implement the equipment in an exercise over a few short weeks. The system

needs upgrades; nevertheless, this project enabled transformational innovation at the tactical level and could potentially add intelligence value to maneuver units in the near future.

Endnotes

1. Department of Defense, Office of the Under Secretary of Defense for Research and Engineering, Assistant Secretary of Defense for Mission Capabilities, "Rapid Defense Experimentation Reserve," <https://ac.cto.mil/pe/rder/>.
2. Robin Porter and James Jahnke, "General Dynamics Land Systems Delivers S-MET, the U.S. Army's First Robotic Infantry Support Vehicle," News, General Dynamics Land Systems, November 2, 2022, <https://www.gdls.com/gdls-smet22/>.
3. "Common Remotely-Operated Weapon Station (CROWS)," Pioneering Decisive Solutions, 2016, <https://pideso.com/common-remotely-operated-weapon-station-crows/>.
4. "StratFac Digital Engineering Environment," Solutions, Parry Labs, 2023, <https://parrylabs.com/stratfac/>.

CPT Leland Lancaster is the Bravo Detachment Commander for the 125th Intelligence and Electronic Warfare Battalion, 25th Infantry Division, Schofield Barracks, HI.

U.S. Army V Corps liaison officer assigned to the 2nd Polish Corps, Polish Land Forces, stands with Polish soldiers for a group photo during Avenger Triad 24 in Kielce, Poland, September 17, 2024. (Photo courtesy of 2nd Polish Corps)



ANONYMOUS NO MORE: COUNTERING THE GRAY ZONE THREAT

by Lieutenant Colonel
H. Eric Perez-Rivera and
Captain Wade Allen

Introduction

Adversary state actors successfully leverage gray zone activities and exploit their relative anonymity at the unclassified level to counter the conventional advantages of the United States and our allies. Our current agreements, policies, and procedures are inadequate to oppose the gray zone activities in competition; however, our current doctrine and tactics are more than sufficient to defeat these gray zone activities in crisis and conflict. During two recent North Atlantic Treaty Organization (NATO) exercises, the V Corps G-2 successfully used identity intelligence to remove adversary intelligence operatives' anonymity and defeat the gray zone network in the rear area.

The National Intelligence Council describes gray zone activities as "coercion and subversion . . . below what constitutes armed conflict but outside the bounds of historically legitimate statecraft."¹ Writing in 2023, Major Ryan Barkholder described the gray zone as "an operational environment in which actors use multiple instruments of power to pursue political-security objectives through graduated activities that are more fervent than steady-state competition, exploit ambiguity, and fall below the threshold of conventional warfare."² Deniability is critical to the success of this strategy; attribution risks escalation and effective response by the United States and her allies.³

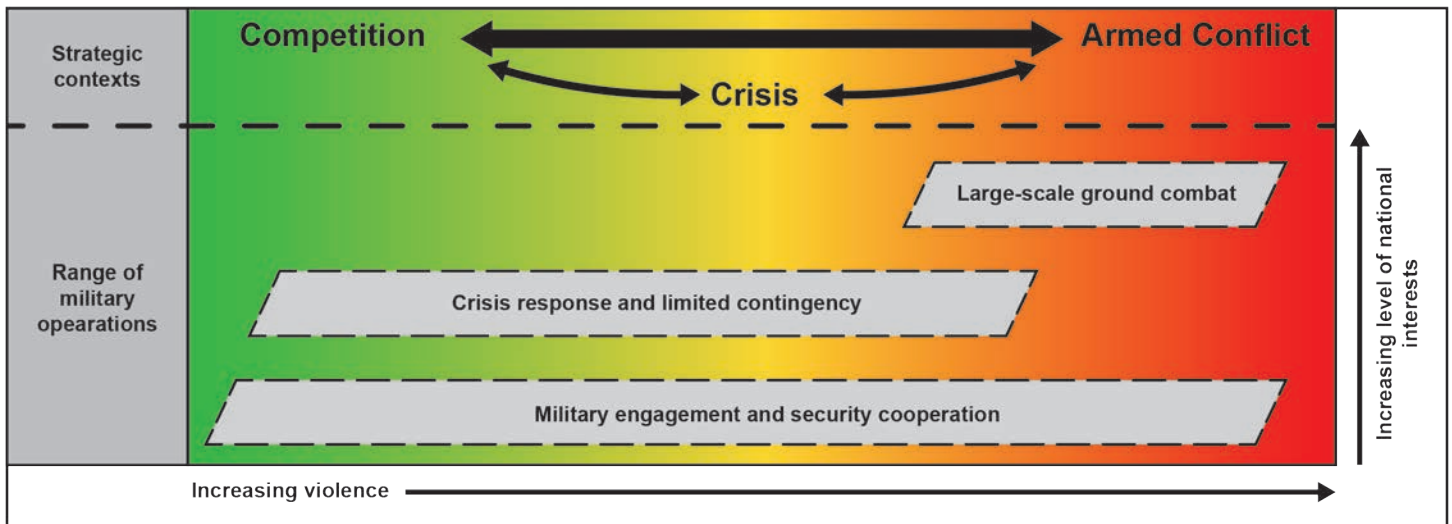


Figure 1. Army strategic context and operational categories⁴

Specific gray zone tactics vary depending on their strategic context. In competition, sustained information operations and using proxy political organizations to counter U.S. access to the targeted region define gray zone threats.⁵ In crisis, gray zone tactics elevate to include covert support to organized criminal gangs, sabotage, and increased cyberspace attacks.⁶ In conflict, gray zone activities shift to a hybrid threat model operating in the tactical, operational, and strategic rear areas, seeking to undercut the legitimacy of U.S. forces, disaggregate our alliances, remove our will to fight, and disrupt our momentum.⁷

Recently, Russia has expanded its gray zone campaign in Europe. Within the last year, Russia has been accused of—

- ◆ Infiltrating water treatment plants in Finland, Sweden, and Germany.
- ◆ Detonating arson devices on DHL facilities and aircraft in Germany and the United Kingdom.
- ◆ Sponsoring arson attacks in Lithuania and Latvia.
- ◆ Conducting small unmanned aircraft system (sUAS) overflights of critical infrastructure in Sweden and Germany.
- ◆ Attempting to assassinate the Chief Executive Officer of German arms manufacturer Rheinmetall.⁸

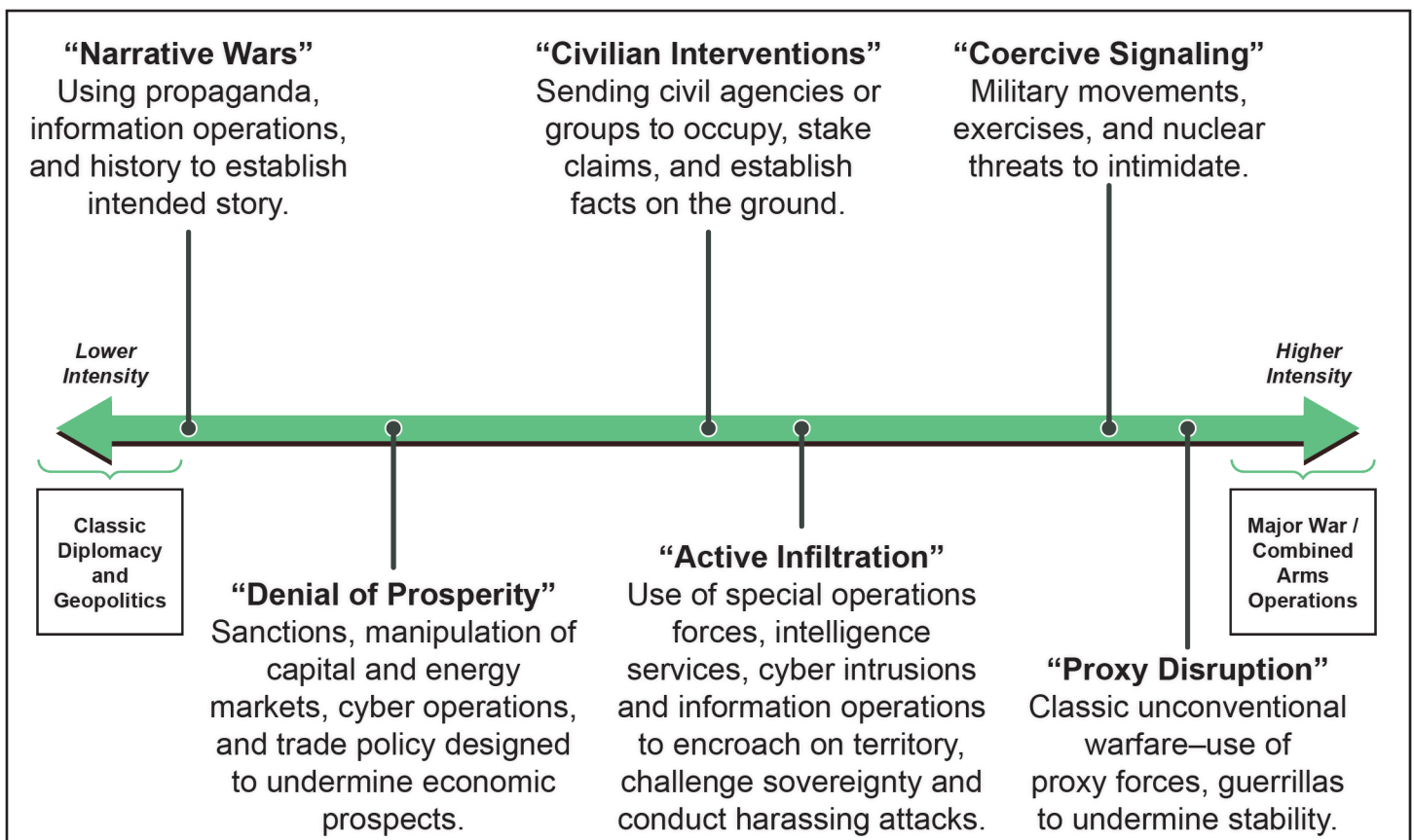


Figure 2. A Spectrum of Gray Zone Techniques⁹

U.S. Army V Corps Soldier studies simulated enemy activity reports as an intelligence analyst during Avenger Triad 24, in Fort Knox, Kentucky, September 16, 2024. (U.S. Army photo by SGT Devin Klecan)



Polish authorities closed the Russian Consulate in Poznan as a result of several incidents in Poland.¹⁰ Countless other events across Europe remain un-attributed, preventing an effective, unified allied response.

When faced with a similar attribution gap in the late 1990s, the U.S. Army developed the concept of *identity intelligence*. Used successfully during the Global War on Terrorism, identity intelligence is defined by Joint Publication 2-0, *Joint Intelligence*, as “the intelligence resulting from the processing of identity attributes” and is used to deny adversaries anonymity.¹¹ Identity intelligence that leverages biometrics-enabled intelligence (BEI) can remove Russia’s anonymity in gray zone sabotage efforts and enable the United States and our allies to defeat adversarial actors. BEI uses the measurable anatomical, physiological, biographical, and behavioral characteristics of an individual (i.e., their biometrics) in combination with other information to connect an individual to a significant activity.¹²

In two recent NATO exercises, the V Corps G-2 used two separate elements of BEI to identify, counter, and defeat gray zone actors in crisis and conflict. During Avenger Triad 24, V Corps used behavioral and biographical characteristics to find, fix, and defeat a state-sponsored threat cell operating in the V Corps rear area. During Northern Spirit 24, V Corps worked alongside NATO allies using anatomical characteristics to identify gray zone actors—including threat actor proxies and transnational criminal organizations—and establish NATO’s first international biometric-enabled watchlist (BEWL).

Biometric-Enabled Watchlist

A biometrically enabled watchlist is a Department of Defense capability that aids screening for persons of interest based primarily on their biometrics (mainly fingerprints but may also include iris and facial matching). The persons of interest are identified by intelligence analysis, usually for screening, vetting, persistent targeting, or population management by Department of Defense ground forces.¹³

Avenger Triad 24: Identity Intelligence to Secure the Corps Rear Area

Avenger Triad 24 was a multinational, multicomponent, multi-corps NATO exercise based on a 2025 large-scale combat scenario in the European theater. V Corps was one of six corps, participating alongside the Multinational Corps Northeast, the 1st German-Netherlands Corps, the 2nd Polish Corps, the NATO Rapid Deployable Corps-Spain, and the Allied Rapid Reaction Corps. The authors led a small team, including an

embedded French officer, in the intelligence section of the V Corps rear command post.

The corps rear command post is responsible for planning and directing sustainment, terrain management, movement control, and security of the corps rear area.¹⁴ During Avenger Triad, the primary threats to these responsibilities were divided between traditional special purpose forces (SPF) conducting reconnaissance and enabling long-range precision fires and gray zone actors employing cyberspace attacks, crowd-sourced intelligence, improvised explosive devices (IEDs) on critical national infrastructure, and protests to halt each corps momentum.

Using conventional intelligence preparation of the operational environment and intelligence analysis techniques, the V Corps G-2, along with the expeditionary sustainment command G-2, the maneuver enhancement brigade S-2, and the military police brigade S-2, was able to identify potential staging locations for the SPF battalion operating in the V Corps area. Employing collateral collection on assets returning to base in conjunction with exploiting downed tactical unmanned aircraft systems and captured tactical unmanned aircraft system waypoints and routine military police patrols, V Corps could find, fix, and finish the SPF battalion within 48 hours. After sharing these tactics, techniques, and procedures (TTPs) with the Multinational Corps Northeast and the 2nd Polish Corps, V Corps identified a second SPF battalion moving from the Multinational Corps Northeast’s area of operations into the V Corps area of operations. Close coordination with the assigned maneuver enhancement brigade S-2 and combat aviation brigade S-2 enabled V Corps to ambush this massed SPF formation as they entered the V Corps area of operations and neutralized the SPF threat.

Countering the gray zone cell proved more difficult, especially at a releasable level. While the 2nd Polish Corps did provide some releasable human intelligence reporting on the gray zone cell, it was often delayed and incomplete. Instead,



U.S. Army Soldiers walk to the V Corps main command post in the early morning fog. (U.S. Army photo by CPT Wade Allen)

V Corps utilized behavioral characteristics to identify several gray zone social media entities, enabling V Corps to use its organic open-source intelligence cell to develop a fully releasable network diagram for tracking the gray zone cell in near-real time. As a result of this TTP, V Corps successfully disrupted an attempted crowd-sourced intelligence collection scheme across the theater and rapidly dispatched maneuver enhancement brigade and military police patrols to gray zone threat locations. These actions ultimately denied the adversary an opportunity to target critical national infrastructure and helped tailor the V Corps messaging campaign. Being able to attribute seemingly mundane events like train derailments, criminal distributed denial of service attacks, and organized protests to this gray zone cell denied the enemy freedom of maneuver and rendered their gray zone efforts insignificant.

Critical to the defeat of this gray zone cell was the ability to share threat information with adjacent multinational corps and host nation agencies. During Avenger Triad, the gray zone cell consistently moved between the corps' rear areas to avoid detection and exploited the seams between the corps' areas of operations. Sharing the updated threat assessments and TTPs between adjacent corps enabled an accurate common intelligence picture, preventing the gray zone cell from taking advantage of corps seams. Additionally, having publicly releasable intelligence enabled V Corps to work alongside the Polish Territorial Defense Forces (and, by proxy, host nation law enforcement) to attribute gray zone actions to the enemy. This attribution and subsequent publication of the threat to the general public increased the sensors V Corps had on the gray zone cell. They directly defeated the crowd-sourced intelligence collection attempt and undercut gray zone actor anti-NATO messaging.

Northern Spirit 24

Northern Spirit is an annual NATO BEI exercise. In 2024, Northern Spirit was nested with Ardent Defender, an annual

NATO explosive ordnance disposal (EOD) exercise, to assess new NATO identity intelligence doctrine. The common exercise scenario simulated a NATO task force assisting a nation in crisis attempting to counter a state-sponsored gray zone actor. EOD personnel and enhanced field exploitation teams responded to and exploited incidents, sending captured exploitable material to a Canadian lab. Biometric samples collected by the lab were processed through the NATO Automated Biometric Identification System (ABIS) and six additional national ABISs. Once an individual was identified, the biometric match report was sent to the identity intelligence cell for fusion with all-source reporting and BEWL nomination. During the exercise, a separate legal advisor cell worked through potential issues with NATO, national, and international laws, policies, and procedures. Northern Spirit was the first NATO exercise to simulate a NATO-led BEWL. Both Northern Spirit and Ardent Defender assumed a biometric sharing agreement between the NATO countries and the host nation government.

V Corps provided four personnel to Northern Spirit/Ardent Defender 24: one EOD officer (enhanced field exploitation team observer), one human intelligence warrant officer (ABIS observer), one lawyer (legal advisor participant), and one intelligence officer (identity intelligence participant).

The now obsolete Army Techniques Publication 2-22.82, *Biometrics-Enabled Intelligence*, dated November 2015, heavily influenced the NATO doctrine for BEI and identity intelligence, laid out in NATO Standardization Agreement (STANAG) 6515, *Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence*. In contrast to U.S. doctrine, NATO does not retain any biometric data; instead, data collected during NATO operations remains with the member or partner country that originally collected the data.¹⁵ The NATO ABIS serves as a transaction manager, temporarily transmitting the search to the federated national ABIS, screening the results against national release limits, and transmitting the screened results back to the original requestor. While this doctrine preserves national equities, it results in a fragmented picture of the adversary.¹⁶ NATO identity intelligence doctrine does not recognize behavioral attributes as part of identification.¹⁷ Until this exercise, NATO also opted not to maintain a BEWL, relying instead on member nations to establish bilateral BEWL sharing agreements. During Northern Spirit, NATO used a BEWL for the first time as a test, starting with two enrollment categories: Person of Interest and Terrorist/Insurgent. There is currently no published NATO STANAG on BEWLs.

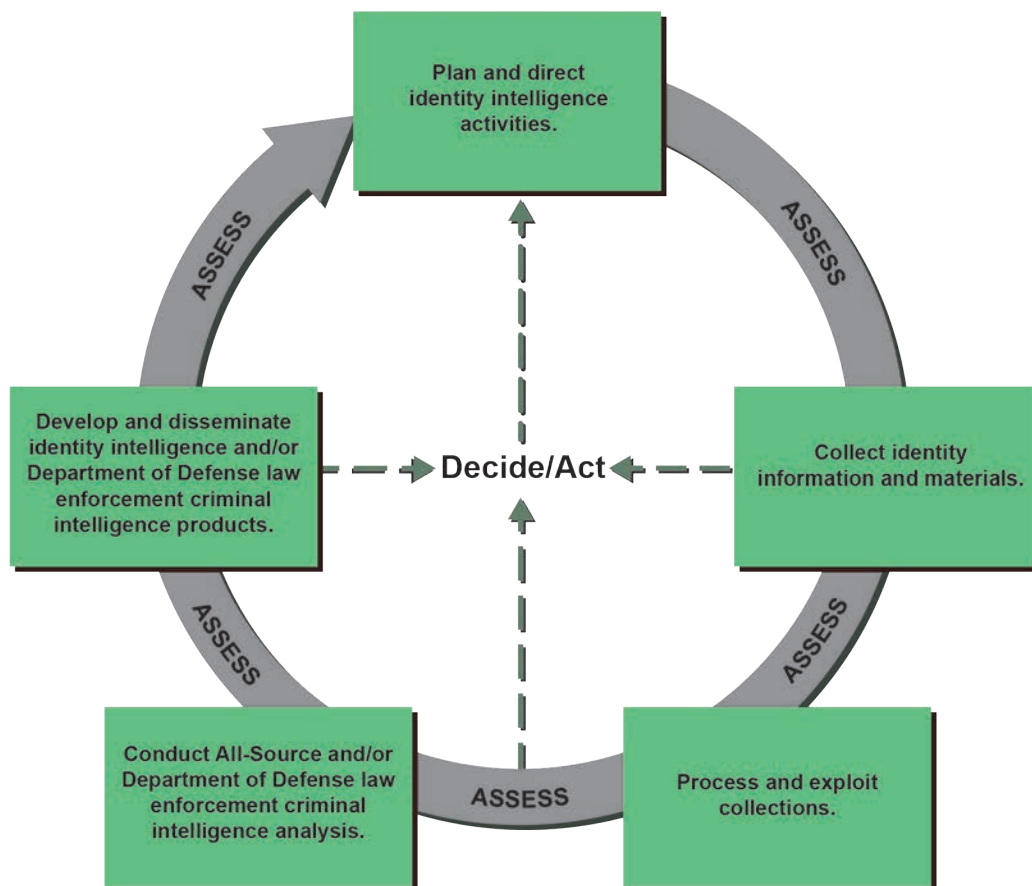


Figure 3. Identity Intelligence Activities Operational Cycle¹⁸

The Northern Spirit threat consisted of a state-sponsored ethnic separatist movement and a transnational criminal organization serving as a state proxy. Both threat organizations sought to undermine the legitimacy of a Western-aligned host nation government and received training, lethal support, and amplified information operations from their state sponsor, a neighbor of the targeted government. Among the threat tactics observed were one-way attack UASs, complex IEDs, vehicle-borne IEDs, disinformation campaigns, commercial sUAS reconnaissance of NATO facilities, criminal vandalism, and modified commercial drones to deploy lethal munitions.

Through Northern Spirit, the international identity intelligence cell successfully used BEI derived from captured exploitable material collected by the Ardent Defender enhanced field exploitation teams, exploited through a Canadian-led multinational lab, and evaluated through six national ABIS databases to build out threat networks and to nominate several threat personas, insider threats, and persons of interest to the NATO BEWL. The current NATO BEWL doctrine, including the nomination process and BEWL categories, has proved insufficient. During the exercise, the identity intelligence and legal advisor cells collaborated on defining additional watch list categories (including force protection categories). Still, national limitations prevented NATO from adopting all of the 33 current U.S. watch categories.


The current NATO exploitation doctrine and TTPs have proved sufficient for collecting biometrics during the exercise. However, especially with sUAS, BEI failed to remove the anonymity of threat actors on a first-time encounter; only with routine patrols, host nation security force engagement, and field biometric enrollment was the identity intelligence cell able to identify the sUAS reconnaissance cell. Other gray zone TTPs (e.g., arson, IEDs, sabotage) were easier to attribute after the NATO task force and host nation law enforcement established an agreement to share biometric data.

Left unaddressed in Northern Spirit was the application of BEI to the targeting process and how to integrate that targeting process with host nation law enforcement for a judicial solution to gray zone activity. Future doctrine and exercises integrating national and international law enforcement organizations should be developed.

Conclusion: An Imperfect Defense

The experiences of V Corps at Avenger Triad and Northern Spirit highlight successful identity intelligence TTPs to remove the anonymity of adversarial gray zone actions in crisis and conflict. Open-source intelligence enabled V Corps to produce publicly available reports, which inoculated the population against gray zone messaging and disrupted gray zone actors. Cross-corps communication and integrating host nation law enforcement denied the adversary physical, procedural, and

policy-based seams for exploitation. Northern Spirit highlighted a way forward for a combined NATO BEWL that balances national caveats while enabling a better understanding of common threats.

While these TTPs proved successful in crisis and conflict, they are not currently deployable in competition. Historically, the U.S. treats gray zone actions in competition as a law enforcement matter, collected and supported primarily by U.S. special operations forces. Like the terrorism threat in the early 1990s, this policy gap remains exploitable by adversarial actors as V Corps and regional NATO allies regularly witness along the eastern flank. Continued simulation of gray zone threats in exercises, which add to the complexity of current steady-state conventional threats, will help build a shared understanding between allied formations and interagency partners. Additionally, continued U.S. and NATO exercises incorporating identity intelligence will help identify, test, and work through potential policy differences, international agreement gaps, and procedural interoperability to narrow the adversary's window of anonymity. 

Endnotes

1. Office of the Director of National Intelligence, National Intelligence Council, *Conflict in the Gray Zone: A Prevailing Geopolitical Dynamic Through 2030*, July 2024, <https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Conflict-In-The-Gray-Zone-July2024.pdf>.
2. Ryan Barkholder, "Tackling Russian Gray Zone Approaches in the Post-Cold War Era," *Journal of Advanced Military Studies* 14, no. 2 (2023): 158, <https://doi.org/10.21140/mcu.20231402008>.
3. Department of the Army, Army Techniques Publication (ATP) 7-100.1, *Russian Tactics* (Washington, DC: U.S. Government Publishing Office [GPO], 29 February 2024), 1-4. Change 1 was issued on 23 April 2024.
4. Figure adapted from Figure 1-3, Department of the Army, Field Manual 3-0 *Operations* (Washington, DC: U.S. GPO, 01 October 2022), 1-14.
5. Department of the Army, ATP 7-100.1, *Russian Tactics*, 2-7.
6. Ibid.

7. Ibid., 2-1 and 2-7.

8. Peter Apps, "Russia's Suspected Sabotage Campaign Steps Up in Europe," *Reuters*, October 20, 2024, www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/.

9. Figure 5-2 from Michael J. Mazarr, "Understanding Gray Zone Conflict," in *Mastering the Gray Zone: Understanding A Changing Era of Conflict* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 2015), 60. <http://www.jstor.org/stable/resrep12018.9>.

10. Natalia Ojewski, "Poland to Close Russian Consulate Over Sabotage Claims," *Bloomberg*, October 22, 2024, <https://www.bloomberg.com/news/articles/2024-10-22/poland-to-close-russian-consulate-in-poznan-over-sabotage-claims>.

11. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 26 May 2022), GL 14. Change 1 was issued 05 July 2024.

12. Ibid., D-5.

13. Ibid., D-8-D-9.

14. Department of the Army, ATP 2-19.3, *Corps and Division Intelligence Techniques* (Washington, DC: U.S. GPO, 08 March 2023), 2-3.

15. North Atlantic Treaty Organization (NATO), Standardization Agreement 6515, *Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence* (Brussels, Belgium: NATO Standardization Office, 23 February 2016), 3-1.

16. Ibid., 2-5.

17. Ibid., 5-9.

18. Figure adapted from Figure D-2., Joint Chiefs of Staff, JP 2-0, *Joint Intelligence*, D-7.

LTC H. Eric Perez-Rivera is the V Corps G-2 Chief of Operations. He previously served in the North Atlantic Treaty Organization Supreme Headquarters Allied Powers Europe J-2X and in multiple intelligence positions at the tactical, operational, and strategic levels over the last 28 years.

CPT Wade Allen serves as a G-2 Operations Officer for V Corps at Fort Knox, KY. He previously served as a company commander for two separate headquarters companies as well as serving as a Patriot Battalion S-2.



Introduction

During 2024, V Corps participated in two major exercises: Warfighter (WFX) 24-03 and Avenger Triad 24. WFX 24-03 was nested with theater exercise Austere Challenge 24 and led by U.S. European Command; Avenger Triad 24 was a multinational exercise led by U.S. Army Europe and Africa Command (USAREUR–AF) that involved six different North Atlantic Treaty Organization (NATO) and United States corps headquarters. Both exercises offered unique training opportunities that allowed V Corps to advance the Army’s understanding of multidomain operations while integrating host-nation, allied, and national capabilities. During Avenger Triad 24, V Corps validated its ability to achieve interoperability with NATO and USAREUR–AF using federated communications systems across all echelons of command with clearly defined common operational pictures (COPs) and mission command information systems (MCIS) by warfighting function.

WFX 24-03 and Avenger Triad 24 both presented challenges, but the V Corps G-2 came away with lessons learned and best practices to share with the greater intelligence community. Through the framework of the three interoperability dimensions (technical, procedural, and human), this article will describe how the V Corps G-2 integrated the Army’s MCIS with NATO allies to create a combined theater common intelligence picture (CIP), established intelligence synchronization procedures across the intelligence warfighting function, and leveraged the trust and rapport built through numerous previous engagements with multinational partners to overcome interoperability challenges.

Technical Interoperability and Architecture

Although the most difficult of the three interoperability dimensions to achieve, technical interoperability is critical to enabling the procedural and human dimensions to create shared understanding across multinational forces. Coordination with

allied nations well ahead of an operation or exercise is crucial to achieving technical interoperability to accommodate U.S. forces and allies’ different systems and processes.

Before WFX 24-03, V Corps G-2 exercise planners scheduled frequent touchpoints with allies from Estonia and the United Kingdom, which resulted in an initial level of technical interoperability.¹ V Corps elements conducting distributed operations from Estonia, the United Kingdom, Poland, Romania, and Germany communicated effectively through email, chat, and distributed collaboration tools such as Cisco Media Server and Command Post Computing Environment. Additionally, V Corps and the multinational divisions could access each other’s sharing portals, enabling redundancy for sharing products if other communication platforms were degraded or disrupted.

From a technical interoperability standpoint, the WFX 24-03 intelligence architecture initially relied on the Warfighter Simulation Intelligence Module (WIM) to generate intelligence for the multinational exercise. However, due to network concerns, the WIM generated U.S. Message Text Format intelligence messages at the collateral Secret level, which precluded sharing with allied partners during the exercise. To overcome the issue, the Joint Multinational Simulation Center and Mission Command Training Program instituted the use of the Intelligence Electronic Warfare Tactical Proficiency Trainer (IEWTPT) on the lower-enclave Mission Partner Environment (MPE) network to generate U.S. Message Text Format intelligence messages with the Releasable to NATO Forces (REL NATO) dissemination marking.

Using the IEWTPT as the intelligence warfighting function simulator increased intelligence generated at the REL NATO level, which enabled a vast increase in intelligence sharing ability among allies. It also expanded the intelligence support to targeting supplied by U.S. personnel using the Intelligence

Fusion Server and by both U.S. and allied forces using the U.S. Army Intelligence and Security Command (INSCOM) Cloud Initiative. Intelligence messages generated from IEWTPT on the MPE network enabled timely high-payoff target list equipment targeting, as targeting information did not have to be transferred from the secured internet protocol router network (SIPRNET) to the MPE network where fires mission command systems resided.

The IEWTPT system resided and produced releasable intelligence reporting on the MPE network, but in a real-world environment, intelligence reporting from U.S. collection assets would occur over SIPRNET. The lack of a cross-domain solution at the tactical (corps and below) level hindered the ability to share intelligence with allies in a timely manner. To share intelligence among allies without a cross-domain solution requires a Soldier-in-the-loop to transfer data manually to the MPE network. This method is neither timely nor effective for quickly transferring large amounts of data. While producing intelligence on the MPE network is helpful in an exercise environment, it does not replicate real-world data flow or restrictions.

USAREUR-AF used the Global Command and Control System-Army (GCCS-A) to move the theater CIP from SIPRNET to MPE by transferring red track data through the Radiant Mercury cross-domain solution. The GCCS-A COP and CIP were both available to all personnel via web browser, allowing any user to visualize the battlefield quickly or query for specific units. The GCCS-A CIP also fed V Corps and subordinate unit Command Post Computing Environment mission command systems, which allowed for a comparison to the V Corps G-2 CIP while providing the authoritative top CIP to all training audiences.

United Kingdom intelligence analysts reported that this iteration of WFX was the first time they could use the MPE network to remain federated during planning and execution. For the duration of the operation, they tracked all battle damage assessments and participated in numerous V Corps battle rhythm events, all on sovereign United Kingdom systems.

One technical interoperability shortfall for the intelligence warfighting function was the lack of a Battlefield Information Collection and Exploitation System (BICES). The BICES can provide a direct link for intelligence between the United States and allied partners while delivering data to the NATO Intelligence Functional System used by tactical units. However, BICES does not communicate with mission command systems. With MPE now accredited to process NATO Secret intelligence, bridging the MPE and BICES networks is critical to ensuring technical interoperability between allied intelligence teams and allowing intelligence from all allies to reach the MPE mission command network.

The Maven Smart System is an emerging U.S. Army initiative that uses artificial intelligence and machine learning for geospatial visualization of data. Multinational interoperability must be considered when implementing the Maven Smart System as the authoritative COP for U.S. forces. If allied and partner nations can successfully navigate the technical requirements to integrate the Maven Smart System into their respective information systems, this will get us one step closer to true convergence.²

Procedural Interoperability

As a tactical warfighting headquarters, it was essential for V Corps G-2 to create a shared understanding of the enemy scheme of maneuver across the battlespace, which is best achieved through synchronization with the V Corps subordinate divisions. V Corps held daily intelligence synchronization working groups (ISWGs) to accomplish this procedural interoperability: two with adjacent and downtrace units and two with higher echelons. This allowed V Corps and its subordinate elements to ensure each echelon had the same CIP of the enemy and the same understanding of what the enemy was likely to do in the next 48 to 96 hours. These ISWGs were essentially analytic conversations, and while V Corps and the subordinate divisions were not always in agreement about the enemy's next move, the units came out of these meetings with a logical, feasible, and, most importantly, synchronized assessment of the enemy scheme of maneuver.

Over time, the format for the ISWG adjusted to create and refine process efficiencies. At the beginning of WFX 24-03, the V Corps analysis and control element (ACE) briefed the overall enemy scheme of maneuver. The subordinate divisions then provided a detailed microanalysis of that enemy scheme of maneuver, a format that allowed the G-2 and subordinate divisions to remain synchronized on the current enemy situation. However, as time progressed, the G-2 and the ACE Chief realized that this format did not adequately provide the subordinate divisions with what they needed most: the corps-level assessment for the next 24 to 96 hours. The ISWG format was therefore adjusted to allow the divisions to brief first on the close fight. The Corps then closed with its assessment of the deep fight. This adjusted format was well received across the formations and provided the subordinate divisions with a more detailed assessment of how V Corps shaped the enemy.

In addition to the daily working groups, the Corps ACE ensured it had multiple conversations with its subordinate divisions outside of the ISWGs to ensure synchronization during the rapidly changing large-scale combat operations. These frequent conversations were especially important from a procedural interoperability standpoint, as allies from Estonia and the United Kingdom could not always access the same networks and tools as the United States intelligence entities.

Members of the V Corps staff and 2nd Corps, Polish Land Forces, staff synchronize their shaping efforts during a command post exercise at Grafenwöhr, Germany, October 26, 2023. (U.S. Army photo by SPC Devin Klecan)

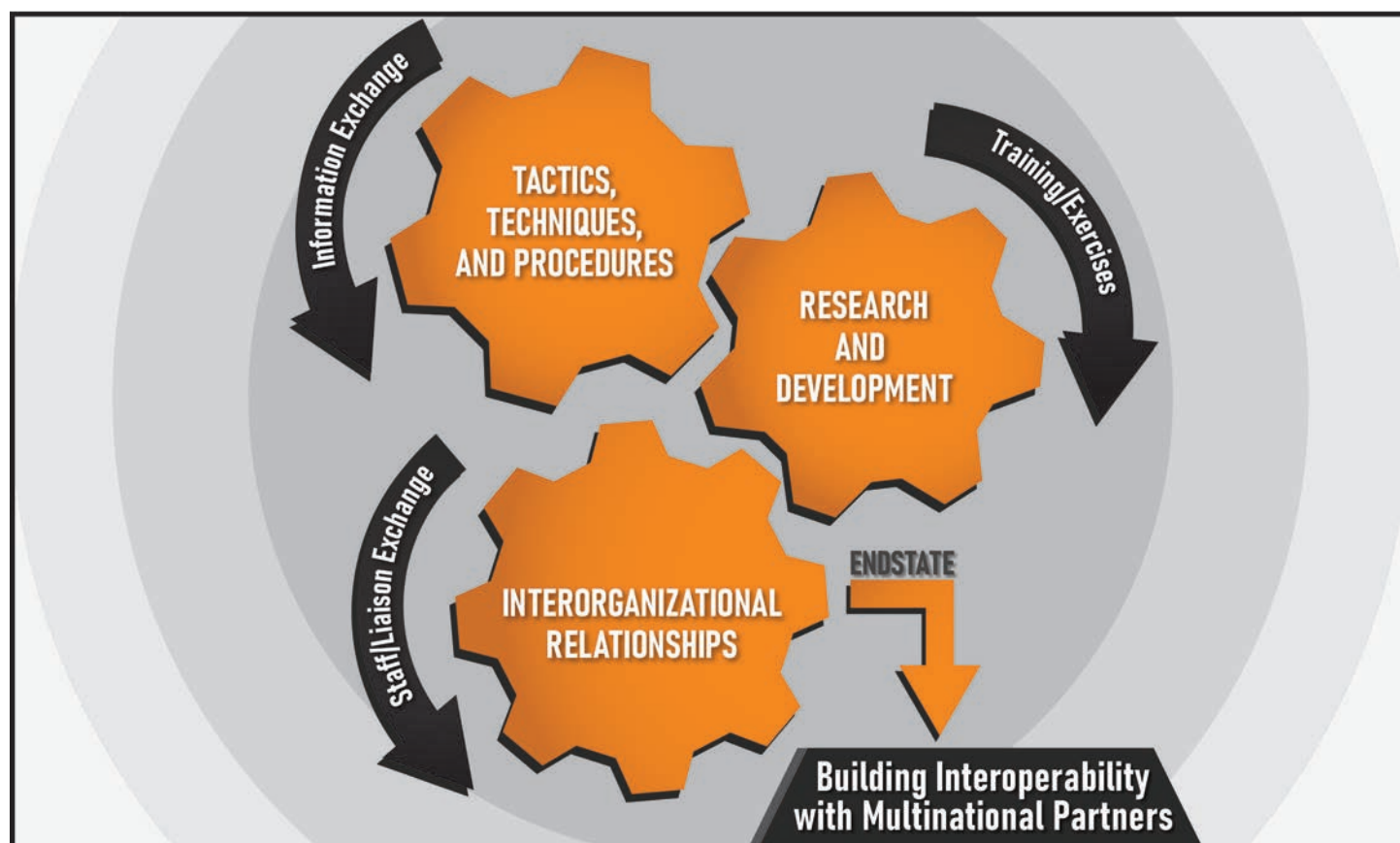


V Corps and subordinate units also passed near real-time information between formations and allies using TransVerse chat.³ V Corps synchronized the intelligence warfighting function across echelons using chat rooms, each focused on a specific intelligence discipline or function, including targeting, battle damage assessments, general military intelligence, and intelligence operations. The United Kingdom accessed TransVerse through Joint Tactical Chat, NATO's secure, text-based chat system, allowing a seamless transfer of intelligence.

Human Interoperability

V Corps leveraged trust and rapport built through numerous previous engagements with multinational partners to overcome interoperability challenges. Maintaining bi-weekly ISWGs and sharing all military decision-making process products early and often created an environment that deconflicted friction and facilitated a collective understanding across all formations. Following Avenger Triad 24, the V Corps G-2 has continued to build relationships with multinational partners by participating in staff-to-staff talks with adjacent corps headquarters and executing intelligence-focused tabletop exercises with adjacent corps G-2s.

WFX 24-03 and Avenger Triad 24 created challenges with downtrace allied divisions that could not participate in planning efforts and engagements before the exercises. U.S. divisions and separate brigades that only provided response cells hindered the ability of V Corps to build upon the human dimension before the WFX because of scheduling conflicts and competing requirements. Establishing sustained relationships with allied downtrace units to train and operate as a combined unit well before exercises or operations and leveraging liaison officers to fill gaps where the corps and divisions have not achieved full technical and procedural interoperability can lead to better human interoperability.




Building interoperability through key concepts⁴

There are also technical issues that the Army must address before future collaborations. During WFX 24-03 and Avenger Triad 24, the successful integration of allied partners into the intelligence warfighting function hinged on the support of personnel from digital liaison detachments and the 4th Security Force Assistance Brigade, who enabled access to the INSCOM Cloud Initiative on MPE and assisted with integration of CIP data with our allies. However, this is not a sustainable solution to the integration problem. In the future, the challenge of the mission command network interoperability will require a technical solution.

Conclusion

Future interoperability efforts should include federation of allied mission command networks with the MPE network to enable full access to the GCCS-A COP and CIP web pages, the INSCOM Cloud Initiative, and other available tools to ensure full technical and procedural interoperability for the intelligence community. Additionally, technical interoperability between the MPE and the BICES would dramatically increase enhanced intelligence collaboration among allies and provide redundant procedural interoperability tools to ensure multiple means exist to collaborate and share intelligence data. IEWTPT use on the lower enclave at a releasable level should be sustained, as it increases situational understanding and targeting efforts for both the United States and partner nations in exercise environments. IEWTPT's ability to generate observation reports, electronic intelligence reports, and imagery reports was critical to the success of all training audiences in the exercise; however, this does not replicate

real-world collection efforts, and there remains a pressing need for a cross-domain solution from SIPRNET to MPE. While interoperability efforts continue to trend in a positive direction, we can take additional steps to innovate and improve our human, procedural, and technical domain goals. 

Endnotes

1. Department of the Army, Center for Army Lessons Learned, *Commander and Staff Guide to Multinational Interoperability* (Fort Leavenworth, KS: Mission Command Center of Excellence, 2023), 57, <https://api.army.mil/e2/c/downloads/2023/01/31/3dadfaa2/20-12.pdf>.
2. Jon Harper, "Palantir Lands \$480M Army Contract for Maven Artificial Intelligence Tech," DefenseScoop, May 29, 2024, <https://defensescoop.com/2024/05/29/palantir-480-million-army-contract-maven-smart-system-artificial-intelligence/>; and Billy Mitchell, "NATO Inks Deal with Palantir for Maven AI System," DefenseScoop, April 14, 2025, <https://defensescoop.com/2025/04/14/nato-palantir-maven-smart-system-contract/>.
3. "Assured Collaboration Solutions Tactical Chat Server (TacChat) Data Sheet," OWL Cyber Defense Solutions, December, 10, 2021, <https://owlcyberdefense.com/wp-content/uploads/2020/12/20-OWL-0438-TacChat-V1.pdf>. TransVerse is an open-source chat client included with the Tactical Chat Server, used by the U.S, Department of Defense, NATO, and Coalition nations.
4. Figure adapted from Figure 2, Department of the Army, Center for Army Lessons Learned, *Commander and Staff Guide to Multinational Interoperability* (Fort Leavenworth, KS: Mission Command Center of Excellence, 2023), 7, <https://api.army.mil/e2/c/downloads/2023/01/31/3dadfaa2/20-12.pdf>; and information provided by the author.

MAJ Robert Deitz currently serves as the G-2X for V Corps. His previous assignment was as the V Corps analysis and control element (ACE) chief. MAJ Deitz has also served as the theater ACE chief for U.S. Forces Korea as well as working in a wide variety of strategic, operational, and tactical intelligence positions.

U.S. Army Soldiers assigned to XVIII Airborne Corps exit a CH-47 Chinook helicopter at Fort Campbell, Kentucky, April 16, 2025. (U.S. Army photo)



THE EXPEDITIONARY MILITARY INTELLIGENCE BRIGADE HEADQUARTERS: A VALUE-ADDED INTELLIGENCE FORMATION

BY COLONEL JARED “JAY” HARTY
AND MAJOR FRED CHRISTOPHERSON

The [expeditionary-military intelligence brigade] E-MIB is an essential corps enabler—it provides the first point of multidomain convergence for our Army’s tactical formations. Its ability to train, maintain, sustain, and employ intelligence capability across the corps close and deep fight is exclusively unique. Without it, Army commanders’ options and access to enterprise intelligence services become prohibitively limited.

—LTG Anthony R. Hale, Deputy Chief of Staff, G-2

Introduction

Army Techniques Publication (ATP) 2-19.3, *Corps and Division Intelligence Techniques*, states that “E-MIBs conduct multidiscipline intelligence operations across multiple domains to support field army/corps/combined joint task force (CJTF)/division operations.... E-MIB headquarters serve as the corps’ entry points to national to tactical organizations, units, capabilities, and data and information and intelligence holdings. E-MIBs receive, integrate, employ, and sustain external intelligence capabilities and elements to support named operations and exercise command and control (C2) over all assigned and attached intelligence elements.”¹

In August 2024, the 525th E-MIB headquarters (HQ) participated in the XVIII Airborne Corps Warfighter Exercise (WFX) 24-05. This article will demonstrate the value an E-MIB HQ, in this case the 525th E-MIB HQ, brings to corps and division commanders by serving as the military intelligence (MI) “anchor point,” providing C2 for all assigned and attached

joint, combined, allied, and interagency MI systems and capabilities. We will discuss the significant support an E-MIB provides to field army, corps, CJTF, and division operations during large-scale combat operations through management and execution of the corps-level MI reception, staging, onward movement, and integration process. Additionally, we will explore how the 525th E-MIB meets future XVIII Airborne Corps, U.S. Army Forces Command (FORSCOM), and Army requirements by employing a Total Army approach via routine collaboration, training, and certification with U.S. Army Reserve and National Guard E-MIB units, as directed in the Army’s 2015 Total Force Partnership Program (TFPP).

Command and Control

The 525th E-MIB, headquartered at Fort Bragg, North Carolina, is assigned one intelligence and electronic warfare battalion (IEW BN) (corps) and three (IEW BNs) (division). These units are:

- ◆ The 519th IEW BN from Fort Bragg, North Carolina, supporting XVIII Airborne Corps HQs.
- ◆ The 319th IEW BN from Fort Bragg, North Carolina, supporting the 82nd Airborne Division.
- ◆ The 302nd IEW BN from Fort Campbell, Kentucky, supporting the 101st Airborne Division (Air Assault).
- ◆ The 103rd IEW BN from Fort Stewart, Georgia, supporting the 3rd Infantry Division.

For WFX 24-05, the brigade headquarters, the 519th IEW BN (Corps), and the 302nd IEW BN (Division) were the WFX training audience, working as response cells in direct support of the corps and division headquarters.

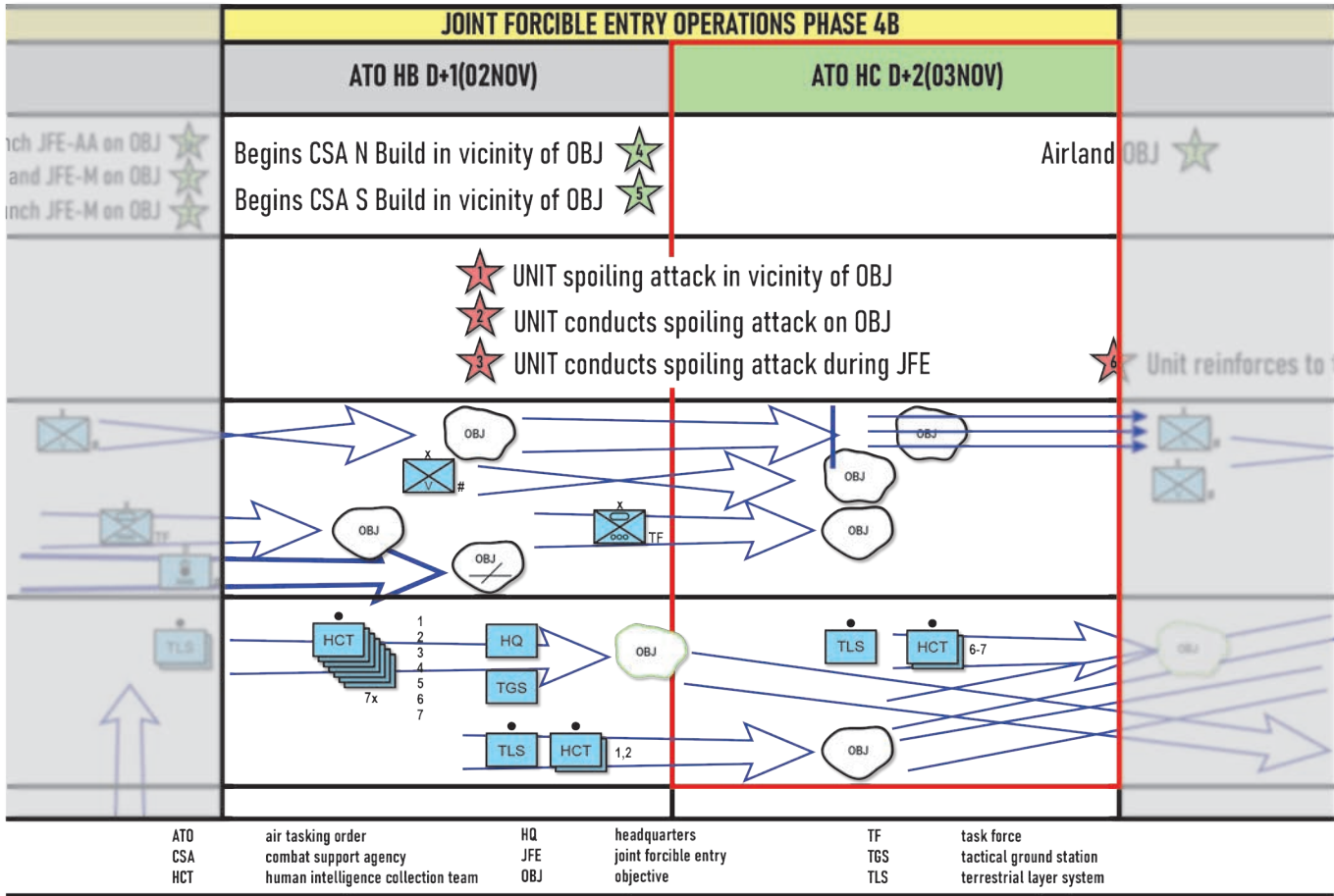
This exercise was the first mission command training program-enabled corps warfighter exercise that the 525th E-MIB HQ participated in as a training audience since its 2019 force design update when the brigade transitioned from an MI brigade to an E-MIB with subordinate IEW BNs. The exercise provided the unit HQ with an excellent opportunity to certify its mission-essential task list functions:

- ◆ Direct operational intelligence activities.
- ◆ Collect relevant information.
- ◆ Distribute operational intelligence.
- ◆ Conduct expeditionary deployment operations at the brigade level.

As the introduction notes, ATP 2-19.3 informs us that E-MIBs maintain C2 over their intelligence elements. During WFX 24-05, the 525th E-MIB staff leveraged multiple products and tools, corps and brigade battle rhythm events, and the XVIII Airborne Corps orders process to help the commander effectively exercise C2 over all assigned and attached intelligence elements. The 525th E-MIB staff also built an updated tactical standard operating procedure to capture the brigade’s warfighting concept and plan accurately.

Participating in commander-to-commander dialogue. The E-MIB commander actively participated in the daily commander-to-commander dialogue meeting with the XVIII Airborne Corps commander. This meeting served as an opportunity to provide the corps commander with a status update on the brigade’s ground-based collection assets, articulate any concerns or risks, and ensure that the brigade remained well-postured to support adjustments to the corps scheme of maneuver. It was immensely valuable for the E-MIB commander to have a seat at the table alongside the other corps separate brigade commanders, as it provided a forum for routine updates to the corps commander on the E-MIB’s ground-based collection capabilities.

Implementing an operations schedule. The brigade’s effective use of the operations schedule, or OPSKED (figure below), helped to enhance the E-MIB commander’s ability to understand, visualize, describe, direct, lead, and assess the brigade’s assigned and attached intelligence elements. The OPSKED effectively enabled the E-MIB commander to “see itself” and served as the brigade’s overall running estimate. In addition to the OPSKED, the brigade leveraged the Maven Smart System,² the XVIII Airborne Corps common operating picture tool. The OPSKED and Maven Smart System helped to enhance and sustain the E-MIB commander’s C2 of their ground-based collection systems more effectively.



The 525th E-MIB Operations Schedule Cut-Out

The Operations Schedule

The operations schedule (OPSKED) is a graphic representation of unit movements depicting the main and supporting efforts of the corps in time and space. The main Blue Forces or BLUFOR decision points and potential RED decision points are also annotated. The OPSKED allows the 525th E-MIB commander to see how the brigade's forces support the main efforts and provide recommendations to the corps commander. Having the OPSKED synchronized with the mission phase and air tasking order cycle allows greater flexibility and the provisioning of recommendations. The E-MIB commander can use the OPSKED to deconflict operational movements and ensure support is provided at the time of need. The OPSKED further allows the brigade staff to ensure resourcing and synchronization of subordinate units with their potential movements.

Leveraging the corps orders process. The E-MIB strove to maximize the XVIII Airborne Corps orders process and implement several corps working groups to help the brigade staff synchronize and stay nested with the corps headquarters. In addition to leveraging the orders process for operational reasons, the brigade's senior warrant officer technicians utilized the orders process to disseminate collection emphasis messages, facilitating uninterrupted intelligence collection operations. Collection emphasis messages highlight specific time-sensitive intelligence requirements that enable the commander's decision-making process.

Developing a new tactical standard operating procedure. The 525th E-MIB staff updated and ultimately created a new E-MIB tactical standard operating procedure to capture the brigade's warfighting concept and plan accurately. This allowed the staff to standardize its systems processes rapidly and better synchronize support for the corps and divisions.

The brigade's experience during WFX 24-05 was challenging. Because the 525th E-MIB HQ and the 519th IEW BN (Corps) just completed a 9-month deployment to Europe immediately preceding WFX 24-05, the brigade missed an opportunity to ensure that its intelligence equities were properly accounted for and task-organized with the appropriate command and support relationships. As a result, the brigade was not actively involved in the WFX planning, which led to the XVIII Airborne Corps WFX 24-05 administrative order containing several inaccuracies and omissions. Once the WFX commenced, the brigade spent several days adjusting its task organization and command and support relationships with the XVIII Airborne Corps and divisions.

An added challenge derived from the Army Force Design Update changes to the E-MIBs and their battalions. These organizational revisions and the doctrine on how the units will be operationally employed are still new within the Army. As a result, the brigade spent considerable time educating the corps and division G-2s and G-3s on correctly tasking and allowing the E-MIB HQs to provide C2 for the corps and division intelligence capabilities.

The E-MIB as the Joint Operational Area's Intelligence Anchor Point

The E-MIB, serving as the MI anchor point, oversees and maintains intelligence elements for the corps area of operations,³ providing many benefits to a corps commander. These benefits include—

- ◆ Providing a single inject point into the corps HQs allows the E-MIB commander, through commander-to-commander dialogue, to assist the corps commander with building a situational understanding of all current and future intelligence capabilities and elements.
- ◆ Receiving, integrating, and sustaining new intelligence systems and capabilities and ensuring their rapid and effective inclusion in the corps G-2's collection plan.
- ◆ Leveraging existing relationships with the Army Service component command, MI brigade-theater, and other intelligence HQs and formations to facilitate replacing and replenishing lost or damaged intelligence systems or capabilities.
- ◆ As an integral part of the command group, the E-MIB commander "serves as the senior national to tactical intelligence integrator for the corps/CJTF command."⁴

During WFX 24-05, the 525th E-MIB exercised two critical intelligence anchor point functions that offer examples of the value added for the corps area of operations. One example was the rapid acquisition of a counterintelligence team. The XVIII Airborne Corps operation called for a turnover of regained territory to host nation forces while building sustainment capability in the corps rear area in a noncontiguous battle space. When the E-MIB HQs conducted the military decision-making process for the mission, it became clear that the 519th IEW BN (Corps) had insufficient counterintelligence capacity to provide adequate collection. The brigade S-3 quickly developed and sent a request for forces (RFF) to the corps G-3; the request was approved, and an additional counterintelligence team was dispatched into the joint operational area. The RFF provided a real-time opportunity for the E-MIB staff to conduct a rapid military decision-making process, identify potential shortfalls in collection capability, and request the necessary reinforcements be sent through the corps up to the Army Service component command quickly and efficiently.

Another example of the value of the E-MIB as an intelligence anchor point in the corps rear area was the rapid reallocation of intelligence capabilities after a battlefield loss. As the divisions were conducting movement from their intermediate staging bases to their assembly areas, the transports carrying a human intelligence collection team (HCT) came under attack and the team was lost. This loss of the human



Soldiers assigned to the 103rd IEW Battalion participate in classroom training using their signals intelligence equipment at Fort Stewart, Georgia, May 07, 2025. (U.S. Army photo)

intelligence collection function reduced the 302nd IEW BN's ability to support the mission of the 101st Airborne Division (Air Assault) to seize a key XVIII Airborne Corps objective. Working with the 519th IEW BN (Corps), the 525th E-MIB staff quickly identified and made available an HCT not scheduled to conduct collection operations until the next phase of the corps operations. Using tools such as the OPSKED and Maven Smart System, the brigade reallocated the available HCT to the 302nd IEW BN in a matter of hours.

The Expeditionary-Military Intelligence Brigade's Total Army Approach

We are a Total Army. By doctrine, by design, the very nature of our service. The only way that we win is when all our formations train and fight together.

—General Andrew Poppas, FORSCOM Commander

The Army's 2015 TFPP creates a framework of partnerships among all components of the total force, enabling units to continue leadership development, share training opportunities, develop staff functionality, and share lessons learned. LTG Chris Donahue, former XVIII Airborne Corps Commander, expressed in his FY 2025 annual training guidance that XVIII Airborne Corps will never fight alone and will always fight as part of a Total Army alongside allies and partners. To that end, the 525th E-MIB has partnered with the 336th E-MIB (U.S. Army Reserve, New Jersey) and the 58th E-MIB (Maryland Army National Guard) to identify training and certification opportunities with the two units. The TFPP allows all three units to leverage their available resources to achieve and sustain a high level of mutual readiness. As of this writing, the 525th E-MIB, in coordination with the XVIII Airborne Corps G-2, subordinate division G-2s, and the 336th E-MIB, has conducted its initial semiannual planning conference to identify training and collaboration opportunities for FY 2025 through FY 2027. In partnership with the Army Reserve and National Guard E-MIBs, these planning events will enable

the XVIII Airborne Corps intelligence warfighting function to plan, resource, and execute quality intelligence training that maximizes each unit's unique capabilities.

The goal of this collaboration, as stated in the November 2023 FORSCOM TFPP order, is tactical-level integration of active and reserve components as a Total Army force supporting the national military strategy and Army commitments worldwide. In pursuit of that goal, the 525th E-MIB will continue to maximize its partnerships with the 336th E-MIB and the 58th E-MIB.

Army Structure Memorandum 25-29 instituted significant changes to the Army force structure, including developing general support MI companies attached to and under the administrative control of their respective division HQs. FORSCOM guidance directs MI brigade commanders to facilitate MI leader development and training. XVIII Airborne Corps leadership expanded on FORSCOM's guidance by directing the 525th E-MIB commander to—

- ◆ Review and provide MI unit training plans and recommendations.
- ◆ Participate in division mission training briefings.
- ◆ Provide guidance for and participate in MI leader development.

This exemplary guidance confirms the need for the E-MIB HQs and solidifies its role as the anchor point for MI capabilities at the corps level.

Conclusion

In this article, we have described how the 525th E-MIB integrated into the daily operations of the XVIII Airborne Corps and its subordinate division G-2s during WFX 24-05 to provide C2 for all MI systems and capabilities. We have provided examples of how the E-MIB's management and execution of the corps-level MI reception, staging, onward movement, and integration process for all assigned and attached joint, combined, allied, and interagency MI systems and capabilities provides vital support to field army, corps, CJTF, and division operations during large-scale combat operations. We have further demonstrated a Total Army approach as directed in the 2015 TFPP via routine collaboration, training, and certification with U.S. Army Reserve and National Guard E-MIB units. In acting as an MI anchor point, the 525th E-MIB demonstrates the significant value and important role of an E-MIB HQ to corps and division commanders. 🌟

Endnotes

1. Department of the Army, Army Techniques Publication (ATP) 2-19.3, *Corps and Division Intelligence Techniques* (Washington, DC: U.S. Government Publishing Office, 08 March 2023), 3-1.
2. Emilia S. Probasco, "How Project Maven and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense," Center for Security and Emerging Technology at Georgetown University, August 2024, <https://cset.georgetown.edu/wp-content/uploads/CSET-Building-the-Tech-Coalition-1.pdf>.
3. Department of the Army, ATP 2-19.3, *Corps and Division Intelligence*, 3-1.
4. Ibid., 3-2.
5. FORSCOM Public Affairs, "Poppas: 'Our Soldiers Stand Ready; Readiness is a Total Army Effort,'" U.S. Army website, October 15, 2024, https://www.army.mil/article/280505/poppas_our_soldiers_stand_ready_readiness_is_a_total_army_effort.

COL Jared B. Harty is the Commander, 525th Expeditionary Military Intelligence Brigade, XVIII Airborne Corps, Fort Bragg, NC. He deployed six times to Kosovo, Iraq, and Afghanistan, serving as an analysis and control element targeting officer in charge, G-2 operations officer in charge, battalion S-2, company commander, G-5 planner, and fusion cell officer in charge. He holds three master's degrees: a master of arts in national security and strategic studies from the U.S. Naval War College, a master of military operational art and science from the School of Advanced Military Studies, and a master of science in administration and management from Central Michigan University.

MAJ Fred Christopherson III is the brigade S-3 for the 525th Expeditionary Military Intelligence Brigade, XVIII Airborne Corps, Fort Bragg, NC. He previously served as the collection manager for XVIII Airborne Corps. MAJ Christopherson has deployed several times throughout his career, most recently returning from Camp Kościuszko, Poland, where he served as the battalion S-3 for the 519th Intelligence and Electronic Warfare Battalion (Corps). He is a distinguished graduate of the U.S. Army Officer Candidate School.

302nd INTELLIGENCE AND ELECTRONIC WARFARE BATTALION (DIVISION): PROACTIVE, REACTIVE, AND ADAPTIVE

**by Lieutenant Colonel Benjamin Polanco, Jr.,
Major Kyle Millard,
Major Nicholas Pena,
and Chief Warrant Officer 3 Robert G. Entenmann II**



Introduction

The 302nd Intelligence and Electronic Warfare (IEW) Battalion (Division) participated in Warfighter Exercise (WFX) 24-05 with the 101st Airborne Division (Air Assault), marking a significant milestone in the unit's evolution and integration. As a recently activated battalion, the 302nd IEW Battalion faced the dual challenge of refining its operational concepts while addressing the limitations of its force structure and capabilities. This article delves into the journey through the initial preparations, the obstacles encountered, and the subsequent adjustments to the battalion's operational concepts and force structure. We will examine the evolution of the battalion's proactive operational concepts, the reactive steps taken to define key IEW battalion roles and responsibilities supporting division intelligence efforts, and the adaptive intelligence processes and production required for large-scale combat operations on the road to Army 2030 and 2040.

Proactive: Operational Concepts

Due to the rapid expansion of IEW battalions within expeditionary-military intelligence brigades (E-MIBs) and a lack of supporting doctrine, the 302nd IEW Battalion has proactively taken steps, aided by its superior commands and staff, to

codify and deploy operational concepts in space and time. These concepts provide the necessary foundational framework while staying fluid to evolve with current Army initiatives such as Total Army Analysis 25-29, Army Structure 2025-2029, Transformation in Contact, Command and Control (C2) Fix, and doctrine relating to large-scale combat operations and multidomain operations.

Operational Concept One—Forward Deployed. Figure 1 below illustrates the 302nd IEW Battalion's primary operational concept with the intent to support the 101st Airborne Division's unique capability of long-range, large-scale air assault. Long-range, large-scale air assault is a concept in development whose objective is to move a mobile brigade combat team (BCT) 500 nautical miles in one period of darkness.¹ The dispersion of the forward detachments and headquarters would ensure intelligence support within the G-2, division artillery, and rear command post.

Operational Concept Two—Reach Capable. Figure 2 on the next page depicts an alternate operational concept for the 302nd IEW Battalion's intelligence operations occurring both forward and within reach. Simultaneously displaced efforts ensure the intelligence requirements are met. Disaggregation

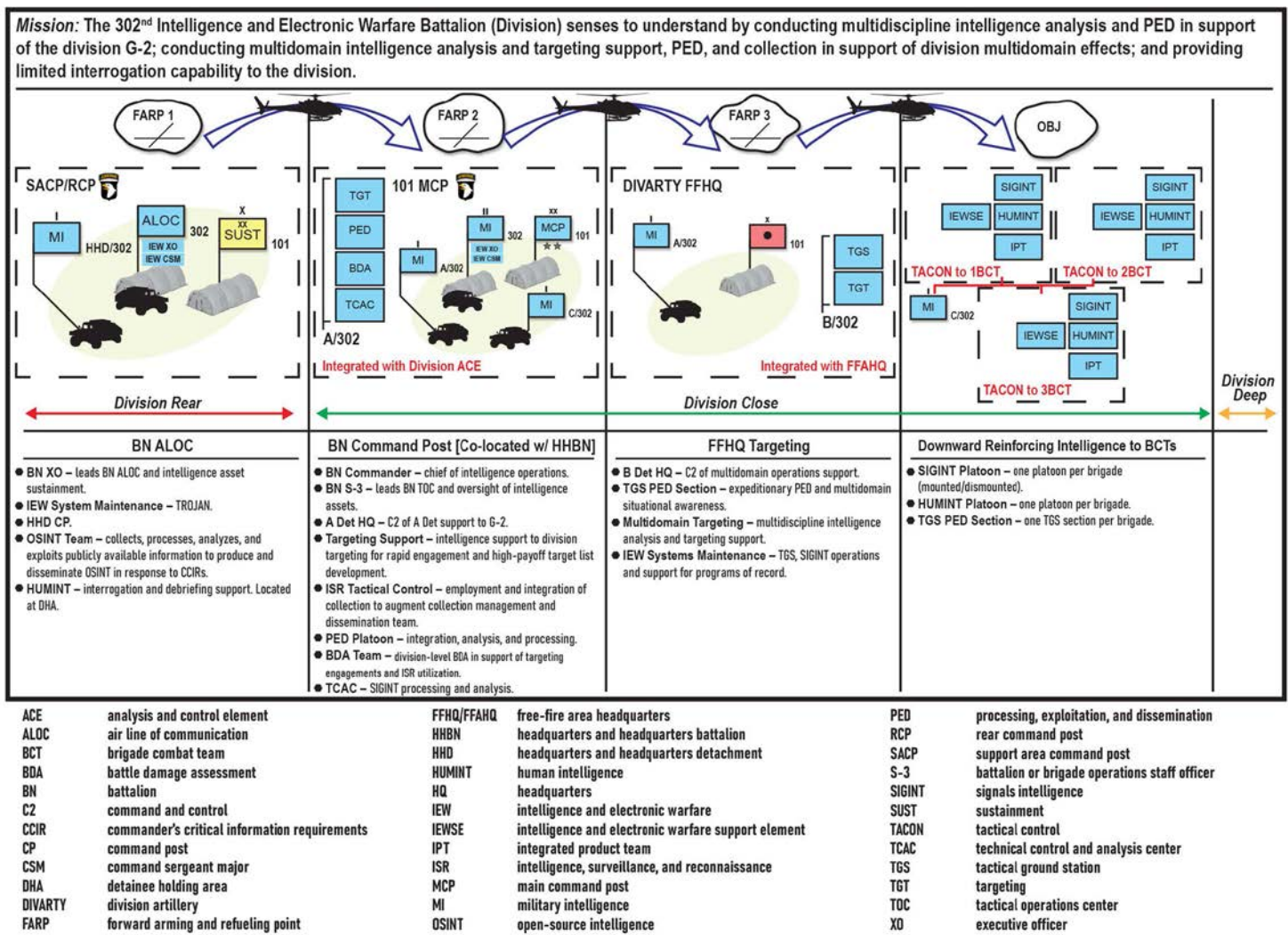


Figure 1. 302nd Intelligence and Electronic Warfare Battalion (Division) Primary Operational Concept (figure adapted from author original)

Mission: The 302nd Intelligence and Electronic Warfare Battalion senses to understand through the employment of tactical collection capabilities and analysis of multidiscipline intelligence in direct support to the 101st Airborne Division (Air Assault).

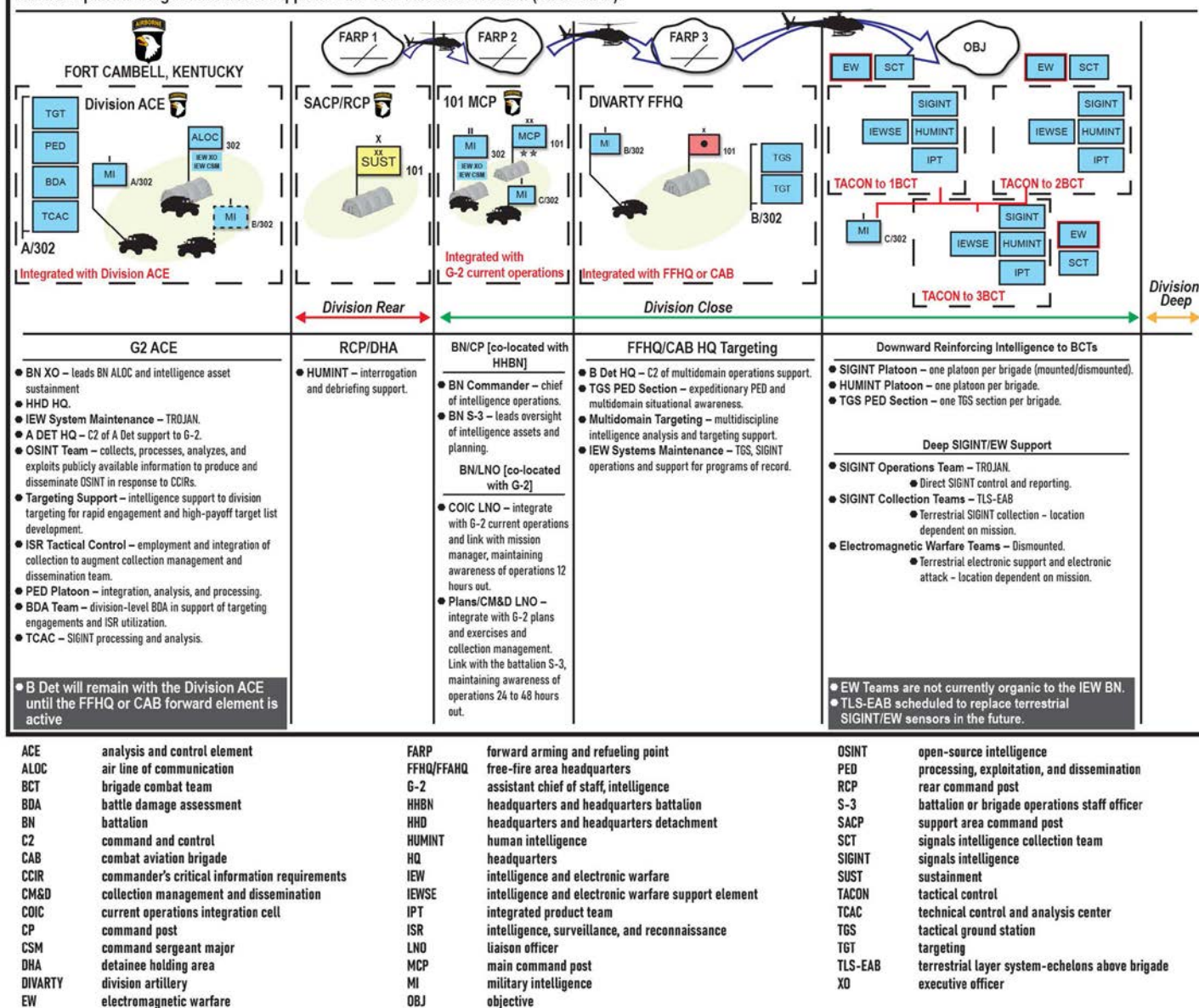


Figure 2. 302nd Intelligence and Electronic Warfare Battalion (Division) Alternate Operational Concept (figure adapted from author original)

may cause an unwanted duplication of effort and/or a lack of shared understanding. Ensuring roles and responsibilities are properly codified between the division G-2 and the battalion, both for primary intelligence operations and alternate- and contingency-level battle drill events is essential. Maintaining the division's battle rhythm and disseminating finalized intelligence below and above echelon will garner success within a properly defined relationship.

Emerging technologies and cloud-based initiatives are all bandwidth intensive and require sufficient data transport to provide adequate download and upload speeds to maintain intelligence production that is efficient, effective, and timely. Reach capabilities ensure that the combined 101st Airborne Division G-2 and 302nd IEW Battalion intelligence teams are employed while reducing the division's forward footprint. The relationship between the number of Soldiers utilizing systems and the bandwidth necessary to maintain effective

employment is easy to understand. The art of employing reach capabilities is ensuring the right team members are forward to understand and interpret the results of the data displayed rapidly.

Over the past year, the 302nd IEW Battalion flexed personnel from various command post (CP) locations with mixed results due to changes in programs of record, bandwidth issues, and other mission requirements. This resulted in too many variables to solidify the proper balance for all operations. Thus, mission-dependent requirements remain the critical planning element for success and require constant communication between the division intelligence enterprise and the battalion to place capabilities effectively in support of analysis and collection requirements.

One lesson learned from this exercise is that IEW battalions must maintain multiple operational concepts to ensure divisions receive sufficient support. These concepts are based



The command sergeant major of 302nd Intelligence Electronic Warfare Battalion, 525th Expeditionary Military Intelligence Brigade (E-MIB), 101st Airborne Division (Air Assault), receives the colors from the brigade commander of the 525th E-MIB, during the 302nd IEW Battalion's activation ceremony on Fort Campbell, Kentucky, September 15, 2023. (U.S. Army photo)

on the nature of the operation being conducted, and they will vary across battalions based on support requirements.

A second lesson learned is the need to base organic data transport needs on the number of bandwidth-heavy cloud-based initiatives. Throughout the exercise, all capabilities hinged on access to the division's tactical network, SECRET Internet Protocol Network (SIPRNET), and Joint Worldwide Intelligence Communications System. With no organic data transport at the battalion level, using the division's network is imperative. This would also be true if brigades were integrated into the conflict. The 302nd IEW Battalion currently does not have an integrated tactical network capability or limited lower tactical internet capability, making it reliant on the supported unit for communications. The primary tools used by all sections were the Army Intelligence Data Platform (AIDP),² Maven Smart System (MSS),³ and the U.S. Army Intelligence and Security Command (INSCOM) Cloud Initiative.⁴

A secondary issue became the lack of training on these systems. MSS was implemented en masse a week before the exercise started, leaving insufficient time for analysts and users to become proficient with the system. AIDP was used in the past but not on a large scale, leading to users learning the system in real time during the WFX. Additionally, the initial deployment of Foundry-based applications, such as Sim Box and Estimates App, into AIDP led to rapid learning requirements and workflow changes before the mission's execution.⁵

Reactive: Key Roles and Responsibilities

Throughout WFX 24-05, the battalion defined and refined the roles and responsibilities of key leaders and teams.

IEW Battalion Commander. The first was the role of the IEW battalion commander. The battalion experimented with various concepts on where and how to employ the commander to codify the role of chief of intelligence operations. We learned that the battalion commander must remain integrated with the division G-2 and collection manager to provide proper C2 of the battalion's intelligence capabilities. Additionally, attendance at the assessment working group, collection working group, and operations synchronization meeting aided the battalion in defining and planning intelligence support for the operation. This ensured maximum asset employment and made it possible to identify gaps and seams in coverage, specifically in the vicinity of the brigade to the division intelligence handover line. Once these were identified, the commander could best advise how to facilitate requests for assets from higher headquarters.

Command Group. The battalion S-3 integrates with battalion staff and the division G-35/G-5 to ensure that organic assets are appropriately tasked to reflect the current collection guidance from the collection manager and G-2. This provides better coordination of movement with friendly force operations. The executive officer and command sergeant major remain with the battalion CP to integrate with the higher headquarters

and ensure support to the battalion. They take the lead in ensuring personnel and equipment replacements are reported and incorporated into the formation to minimize capability degradation. The executive officer runs the battalion CP in the commander's absence and ensures the commander receives updates when time and the commander's return permits. Ideally, the battalion CP is co-located with the division G-2.

Mission Manager. The mission manager position is not assigned but was created by the battalion out of necessity. The mission manager looks at information collection assets, named areas of interest, and priority intelligence requirements as encapsulated in the G-2 collection management and dissemination section's intelligence, surveillance, and reconnaissance (ISR) plan and determines which specific collection matrix ISR lines the processing, exploitation, and dissemination (PED) team will support. The G-2 collection management and dissemination section determines the allocation of assets against specific collection focus areas such as situation development, target development, and battle damage assessment (BDA). The mission manager then directs PED efforts toward those focus areas. Finally, the mission manager briefs the collection manager or the IEW battalion S-3 no later than 2200 the day before execution to confirm allocation and emphasis.

Intelligence, Surveillance, and Reconnaissance Assessments Team. The ISR assessments team determines ISR effectiveness and conducts BDA; however, with only a five-person team, BDA became the sole focus during the exercise. Currently, the Army does not have doctrine or procedures to follow for conducting BDA, which means the responsibility for this process and how to execute it falls on each division. Initially, the G-2 used AIDP to display BDA, but as the exercise progressed, several flaws in the system prevented an accurate tracking mechanism. This resulted in the G-2 switching to analog battle tracking using Microsoft Excel on shared Microsoft Teams over SIPRNET. Utilizing Microsoft Office 365 on SIPRNET enabled real-time sharing and made the product readily accessible to all within the G-2 and on the current operations integration cell floor; however, research is ongoing for a system to streamline and standardize BDA reporting and tracking.

Tactical Ground Station PED Section. The Tactical Ground Station PED section in Bravo Detachment is similar to Alpha Detachment's PED platoon, except it is expeditionary. The Reach Capable Operational Concept, used during this exercise, integrated Bravo Detachment PED with Alpha Detachment PED at the analysis and control element. This integration allowed more personnel to exploit both organic and echelons above division assets collecting within the area of operations. It also enabled a stable pipeline to conduct PED without network loss or latency interruptions as both detachments' PED operated under the same bandwidth constraints. The Tactical

Ground Station PED section can also operate comparably to Bravo Detachment's multidomain operations targeting section. It can be attached to the division artillery or the division main command post, providing PED support for the same functions the targeting team would execute.

Charlie Company—MI Company (Division Support). As the IEW battalion's military intelligence company providing division support, Charlie Company's role in the exercise offered a unique insight into potential future challenges for the division as it employs this newly established company. The IEW battalion staff must invest time to ensure proper employment and command support relationships between the company, battalion, and division during operations. As collectors for the division working in the division's brigade combat teams' (BCTs') battle spaces, support is crucial to accomplish their mission.

As an additional challenge, the 101st Airborne Division is participating in the C2 Fix initiative.⁶ Due to their participation, intelligence generation through PED-specific procedures is manually produced and hand-delivered by the division analysis and control element. The BCTs operate on Sensitive but Unclassified—Encrypted networks, which limits the teams' ability to send classified data back to the division. During the exercise scenario, this limitation had minimal impact; however, implementing Charlie Company assets moving forward within the C2 Fix construct will likely require changing the battalion's modified table of organization and equipment (MTOE). Alternatively, the battalion must source commercial- or government-off-the-shelf solutions to ensure connectivity.

Another crucial issue for the 302nd IEW Battalion is the logistics behind asset replacement for Charlie Company. During WFX 24-05, the 302nd IEW Battalion relied on the 101st Airborne Division and 525th E-MIB to provide critical assets and personnel replacement after battlefield losses. The 525th E-MIB works in direct partnership with XVIII Airborne Corps, which allowed it to streamline asset replacement through standard reporting and ensured minimal gaps in collection coverage inside the division and corps areas of operation. To avoid any degradation to operations, the IEW battalion must report asset and personnel replacement requirements to the E-MIB and its supported division.

Finally, the 101st Airborne Division is developing a concept to habitually align some Charlie Company assets to support the BCTs moving forward. The plan will allow the BCTs to integrate these capabilities through training and provide predictability before operations. This initiative, in turn, will require an analytical support element directly aligned with the BCTs to reside in the division G-2. Figure 3 depicts the 101st Airborne Division's plan to habitually align Charlie Company, 302nd IEW Battalion assets within the division's intelligence warfighting function supporting framework.

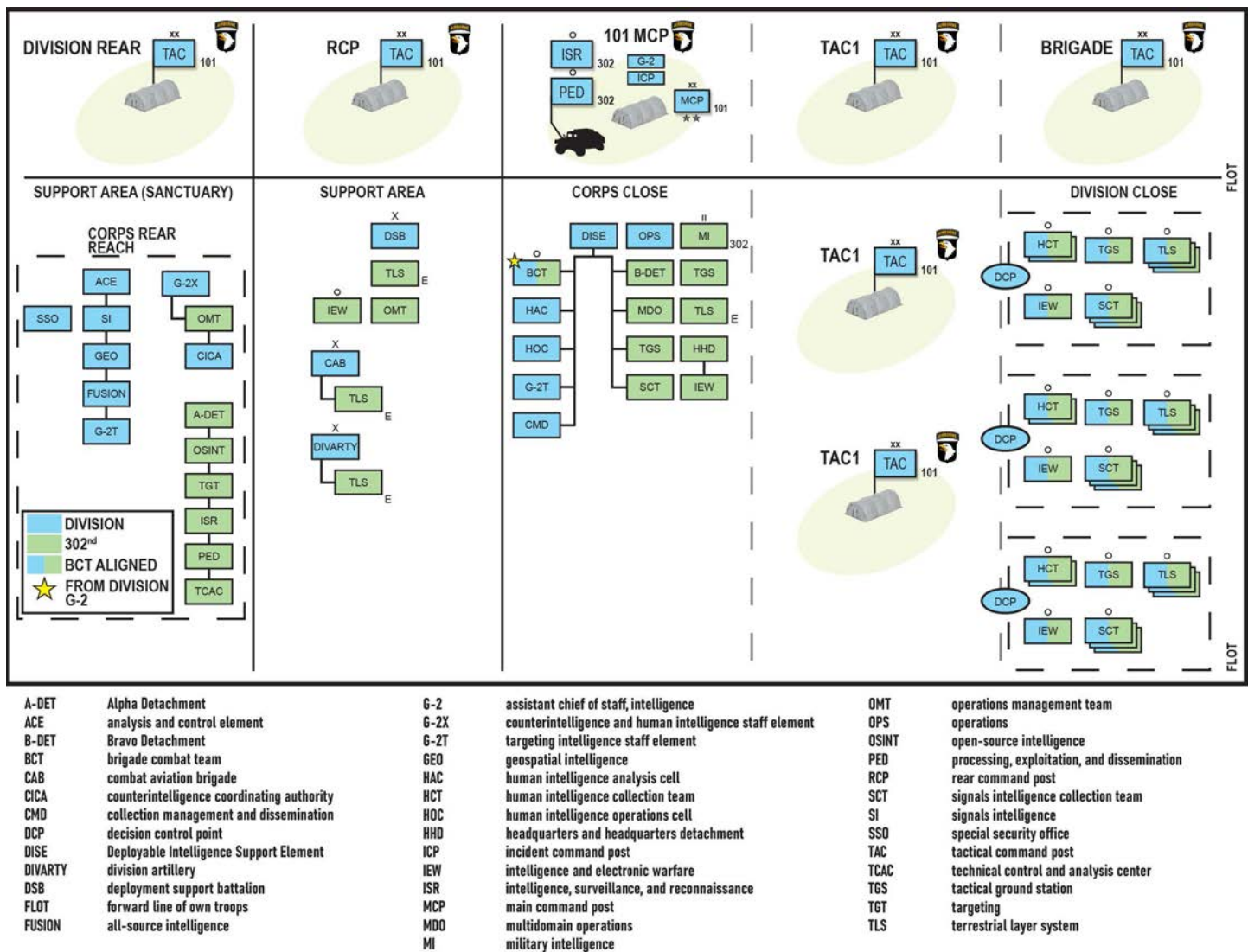


Figure 3. 302nd Intelligence and Electronic Battalion (Division) and G-2 Habitual Alignment Framework (figure adapted from author original)

Adaptive: Intelligence Processes versus Production

Emerging technologies, cloud-based initiatives, and the sunseting of legacy mission command and intelligence transport, sensors, systems, and processors demand that the 302nd IEW Battalion remains vigilant to procure, incorporate, utilize, and maintain all programs of record both internal and external to the MTOE. These changes to mission command and intelligence architecture are currently experimental, in development, and ultimately extensive; however, doctrinal intelligence processes will remain valid throughout. Intelligence production requirements must also remain adaptive to meet the desired outputs of echelons below, at, and above division.

These changes present a real and significant problem for division intelligence operations, including challenges for—

- ◆ Information collection synchronization and management.
- ◆ PED.
- ◆ Common intelligence picture.
- ◆ Decide, detect, deliver, and assess.

- ◆ Sensor to shooter.
- ◆ Dissemination of finalized intelligence.
- ◆ Situational development, target development, and BDA.

Adaptive solutions have been and will continue to be developed to mitigate these problems; however, legacy systems are still included in the MTOE for the division and the IEW battalion (division) while new and emerging technologies continue to be developed and deployed.

Cloud-based solutions, particularly AIDP, have broadened the ability of division intelligence operations to share and collaborate at echelons above division. Since it is cloud-based, using the AIDP training environment to its full potential requires significant planning, scheduling, and requests for support. Nevertheless, the 101st Airborne Division G-2 and 302nd IEW Battalion Soldiers were trained effectively within weeks and then battle-tested over several large-scale training exercises. With prioritized division intelligence system efforts still in development, the 101st Airborne Division and the 302nd IEW Battalion have utilized this known deficiency to deploy AIDP boldly and effectively, proving its value to U.S. Army Forces

Command (FORSCOM), INSCOM, and the U.S. Army Training and Doctrine Command (TRADOC).

Prior planning is essential for large-scale exercises like WFX 24-05 but has become significantly more difficult due to emerging technologies and cloud-based initiatives. Intelligence programs of record currently fielded and in development are designed to increase ease of use and require little to no maintenance. However, significant changes to the intelligence architecture may require significant problem-solving skills during execution. During WFX 24-05, the 302nd IEW Battalion deployed a small data management team to identify these problems before execution and to formulate workflows within and to support the intelligence process. The data management team was also responsible for maintaining communication with the AIDP field service engineers to ensure present and persistent data flow and, more specifically, an uninterrupted message traffic data flow.

One of the data management team's workflows targeted the employment of AIDP as a collaboration tool. It is essential to know that the interdependency of AIDP tools with other tools (e.g., Gaia, Graph, Dossier) is an architecture. The data management team developed a map architecture and standard operating procedures for each tool's intended purpose, enabling the 101st Airborne Division G-2 and 302nd IEW Battalion analysts to navigate AIDP's internal products for collaboration and data sharing. Additionally, to compensate for the AIDP training stack's inability to peer with MSS and its Target Workbench application,⁷ the data management team developed an AIDP Graph to house the high-payoff target list targeting priorities according to air tasking order day. Pre-generated objects (high-payoff target list-specific equipment) streamlined object development and confirmation status to enable an efficient and effective targeting process.

What is Peering?

Peering or network peering is a method of managing the direct connection and data exchange between two or more computer networks without passing through a third-party service provider. The term peering refers to the agreement between two parties (ISP or Company) willing to exchange data that is beneficial to both.⁸


Weeks before the WFX execution, the data management team also developed applications with AIDP field service engineers to parse the U.S. Message Traffic Format (USMTF). The SIM Box application yielded the best results for parsing USMTF, but it had some limitations, such as message time lapses from batched message flow. Through their efforts, AIDP's ability to parse USMTF produced the best visual fidelity of enemy movement during a large-scale exercise. The Mission Command Training Program projects that 140,000 to 160,000 messages are generated during a ten-day WFX. However, due to the appropriate use of intelligence collection assets above

division, WFX 24-05 generated over 350,000 messages, and AIDP displayed correct object icons for hundreds of emplaced obstacles and defensive positions. Proper parsing of USMTF reconnaissance exploitation reports led to this result, but duplicate reports, specifically BDA, may have contributed to the total. These solutions, developed to avoid problems or in the absence of existing solutions, were recorded by Mission Command Training Program observer coach/trainers and relayed to the programs of record for development as well as to FORSCOM, INSCOM, and TRADOC.

Report writing applications do not currently exist within Palantir's "Family of Systems," which includes AIDP-Cloud, AIDP-Tactical Edge, MSS, and Capability Drop-1. These systems can send USMTF-generated messages, such as target intelligence data and enemy situation reports; however, reports that provide situational development to echelons below, lateral to, and above division do not exist. During WFX 24-05, the 101st Airborne Division G-2 and 302nd IEW Battalion utilized AIDP's Dossier⁹ tool to develop the intelligence running estimate, which was used to finalize an intelligence summary for publication.

Finally, these emerging technologies and cloud-based initiatives provide near-perfect graphic representations of the operational environment. Often, these graphics are data-intensive, and disseminating them using traditional primary, alternate, contingency, and emergency (PACE) methods can be risky. It is essential, therefore, to remember the need for a simple text format—for example, Variable Message Format—when designing an effective PACE plan within a C2 Fix environment. A simple text format enables echelons to prepare intelligence for dissemination through multiple means, whether chat, email, data packages, or voice communications.

Conclusion

WFX 24-05 served as a test and a catalyst for the 302nd IEW Battalion's operational development. The exercise highlighted critical shortfalls, such as only partial integration of the battalion staff and detachments, insufficient equipment and personnel, and the challenges posed by reliance on external network services. However, it also underscored the battalion's ability to adapt and evolve its operational concept to meet the demands of the 101st Airborne Division's split operations. The invaluable lessons learned from WFX 24-05 drive home the battalion's need to develop multiple operational concepts, ensure comprehensive training on key systems, and integrate more robust communication capabilities. As the 302nd IEW Battalion continues to refine its strategies and capabilities, it is better positioned to provide critical intelligence support in increasingly complex and dynamic operational environments. 

Endnotes

1. Josh Luckenbaugh, "AUSA News: Army Practices New Air Assault Concept Without New Helicopter," Army News, National Defense, October 15, 2024, <https://www.nationaldefensemagazine.org/articles/2024/10/15/army-practices-new-air-assault-concept-without-new-helicopter>.
2. "Army Intelligence Data Platform ('AIDP')," Palantir Technologies, Inc., https://www.palantir.com/assets/xrfr7uokpv1b/7JAWiSA6yA5MLDAD1AsX7I/c256437b1c29bad5747633123957b4b7/AIDP_AUSA_2_updated2.pdf.
3. "Maven Smart System," The Missile Defense Advocacy Alliance, 2025, <https://missiledefenseadvocacy.org/maven-smart-system/>.
4. Loren Blinde, "INSCOM Posts Cloud Platform RFI," Biz Opps, Intelligence Community News, August 3, 2021, <https://intelligencecommunitynews.com/inscom-posts-cloud-platform-rfi/>.
5. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: Government Publishing Office, 01 October 2023), B-3. The Foundry Intelligence Training Program is a critical enabler for Army global readiness. It provides resources to train military intelligence Soldiers and civilians at the strategic, operational, and tactical levels.
6. Michelle K. Donahue, "The C2 Fix Initiative: What it Means for Sustainment Forces," U.S. Army website, January 22, 2025, https://www.army.mil/article/282485/the_c2_fix_initiative_what_it_means_for_sustainment_forces.
7. "Target Workbench: Collaborate Across the Target Lifecycle," Palantir Technologies, Inc., 2023, https://www.palantir.com/assets/xrfr7uokpv1b/1lqzwzpemtBSm98TNCczao/49bbc30cbec4d2d4d189ab27bd07376c/Palantir_Target_Workbench_1.pdf.
8. Admin, "What is Network Peering? Definition, Types, and Benefits," EDGE DC (blog), October 24, 2023, <https://edge.id/articles/what-is-network-peering>.
9. "Dossier," Palantir Technologies, Inc., 2025, <https://www.palantir.com/offerings/defense/secure-collaboration/capabilities/#dossier>.

LTC Benjamin Polanco, Jr. is the Commander, 302nd Intelligence and Electronic Warfare (IEW) Battalion (Division), 525th Expeditionary-Military Intelligence Brigade (E-MIB). He began his career as a military intelligence (MI) officer detailed to the infantry and served as a mechanized infantry platoon leader and executive officer while assigned to 2nd Battalion, 7th Cavalry Regiment and 1st Battalion, 12th Cavalry Regiment, 3rd Brigade Combat Team (BCT), 1st Cavalry Division. LTC Polanco has served in various staff and command intelligence positions within 1st Infantry Division (Military Transition Team); 717th MI Battalion (National Security Agency-Texas); 4th Battalion, 10th Special Forces Group (Airborne); 101st Airborne Division (Air Assault); North Atlantic Treaty Organization Rapid Deployable Corps-Italy; and U.S. Army Central. He most recently served as the Assistant Chief of Staff G-2 for the 1st Theater Sustainment Command. LTC Polanco has deployed to Afghanistan, Africa, Iraq, and Saudi Arabia.

MAJ Kyle Millard is the executive officer, 302nd IEW Battalion (Division), 525th E-MIB. He has previously served as the G-2 analysis and control element chief for the 101st Airborne Division (Air Assault); the S-2 for 2nd BCT, 101st Airborne Division; as a MI company commander and battalion S-2 in 1st BCT, 101st Airborne Division. He holds a bachelor's degree in global security and intelligence from Embry Riddle Aeronautical University and a master's degree in business and organizational security management from Webster University.

MAJ Nicholas Pena is the operations officer, 302nd IEW Battalion (Division) 525th E-MIB. He has previously served as the battalion S-2 for 2nd Battalion, 7th Infantry Regiment, 1st Armored BCT, 3rd Infantry Division; as the brigade assistant S-2 for 1st Armored BCT; and as an intelligence observer coach/trainer with 1st Army East. He holds a bachelor's degree in business management from the University of Central Florida and a master of business administration from Vanderbilt University.

CW3 Robert G. Entenmann II is the S-3 intelligence operations chief, 302nd Battalion (Division), 525th E-MIB. He currently serves as the lead data manager. Before his current assignment, he deployed with the 101st Airborne Division (Air Assault) to Poland as the Task Force-101 Division Tactical Command Post G-2 fusion officer in charge. He holds a bachelor's degree in political science from Adelphi University and he is a recent graduate of the Master Intelligence Data Strategy Course.

The 2nd Stryker Brigade Combat Team, 2nd Infantry Division at Joint Base Lewis-McChord conducts a validation exercise for prototype command post equipment in support of Program Executive Office Command, Control and Communications-Tactical's Command Post Integrated Infrastructure program. (U.S. Army photo)



U.S. ARMY COMMAND POST SURVIVABILITY

BY SSG DAVID S. BALL

Editor's Note: This article was written in early 2024 as part of a professional writing competition open to the Army Soldiers and civilians of the 305th Military Intelligence Battalion, Fort Huachuca, Arizona. Competitors drew upon their operational and institutional experience as well as subject matter experts from across the Military Intelligence Corps to address challenges facing the intelligence warfighting function. For this competition, writers tailored their articles to the Indo-Pacific Command's area of responsibility.

Introduction

To address the pacing threat posed by China in the Indo-Pacific Command (INDOPACOM) region, the United States Army must increase command post (CP) survivability without neglecting the needs of the intelligence warfighting function. In his 2024 *Military Review* article, Ian Sullivan noted, "In 2015, China's People's Liberation Army (PLA) embarked upon the most ambitious, extensive, and far-reaching reform and modernization program in its history."¹ China's rapid military modernization also requires the United States Army to adapt, embracing smaller, more mobile CPs with intelligence architecture, dedicated bandwidth, and reduced electromagnetic signatures to maintain critical mission command and intelligence functions.

Command Posts and the Warfighting Functions

Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces*, describes the importance of U.S. Army CPs: "At every echelon of command, each commander establishes a command and control system—the arrangement of people, processes, networks, and command posts that enable commanders to conduct operations."² CPs provide a physical location from which to exercise command and control, one of the six warfighting functions, but this is not accomplished without support from the other warfighting functions.

Winning conflicts in a multidomain operational environment requires the convergence and synchronicity of the fires, sustainment, protection, movement and maneuver, and intelligence warfighting functions to establish combat power through command and control.³ In other words, these separate warfighting functions work together as a dynamic team, prioritizing tasks to defeat the Nation's enemies. The figure on the following page illustrates the combat power model, which clarifies how the warfighting functions work together.

Command and Control Warfighting Function

The related tasks and a system that enables commanders to synchronize and converge all elements of combat power.

Tasks

- Command forces
- Control operations
- Drive the operations process
- Establish the command and control system



Command and Control System

- People
- Processes
- Networks
- Command posts

Combat Power Model⁴

The intelligence warfighting function supports operations, providing the commander and staff the information necessary for informed decision making. Key tasks of this warfighting function include intelligence support to force generation, support to situational understanding, conducting information collection, and providing intelligence support to targeting.⁵

Today, CPs provide commanders with the benefit of up-to-date tactical information and intelligence-sharing capabilities among critical staff sections. Support requirements for modern CPs include radio frequency-emitting antennas, numerous generators, and a variety of vehicles, all of which create an easily identifiable physical and digital footprint. This type of CP may have been acceptable when combating technologically inferior adversaries, like during the counter-insurgency operations in Iraq and Afghanistan. However, it becomes more problematic when faced with adversaries capable of multidomain operations, such as China, which “has focused on disrupting US command-and-control capabilities.... China could employ a variety of means, including jamming, cyberwarfare, and attacks on communications satellites.”⁶ Disrupting a CP disrupts the “brains” of an operation, which can lead to uncoordinated lines of effort. The United States Army must concentrate on the survivability of CPs when considering the threat China poses to the INDOPACOM region.

People’s Liberation Army Modernization

The People’s Republic of China (PRC) expends significant effort toward observing armed conflict elsewhere in an effort to modernize their forces: “What gives China, the second-largest military spender in the world... the upper hand is the fact that it has been studying the American way of war for a long time, formulating its own grand strategy and modernizing its military.”⁷ The bottom line is that the PRC is now considered by many in the intelligence community to be America’s foremost pacing threat.

Chinese scrutiny of the American way of war reveals the value of modernizing the footprint and capabilities of CPs. For example, discussing China’s interest in the United States military’s Joint All-Domain Command and Control (JADC2) project, which aims to integrate its sensors and weapons in a robust network using artificial intelligence, Stew Magnuson writes in his 2023 Business Insider article, “The People’s Liberation Army is working on its own version of JADC2 while simultaneously seeking ways to disrupt or destroy the U.S. system.” Magnuson further notes that the PRC will most likely continue to focus on technology that would identify signatures and networks associated with United States CPs.⁸ The PLA recognizes the importance of shared intelligence supporting effective CPs.

Once command and control nodes are identified, the PLA can target United States Army CPs throughout INDOPACOM areas of operation by suppressing information systems or using lethal strikes in the same way that Ukraine did “in summer 2022 when it used new U.S.-supplied HIMARS [High Mobility Artillery Rocket System] GPS [Global Positioning System]-guided rockets to target Russian command posts near the front lines,” thereby exploiting the perceived technological advantage of the Russian Army. Ukraine capitalized on the resulting disruption to retake much of its territory.⁹

The first photo on the following page shows an example of a Russian CP at Kherson International Airport decimated by Ukrainian rockets. The Russian Army likely underestimated Ukraine’s intelligence gathering and capability to target large static command and control nodes. This imagery clearly demonstrates the dangers of not investing in CP survivability against adversaries.



Satellite imagery from 15 March 2022 shows a large fire and a number of destroyed aerial assets at Russian-occupied Kherson International Airport, Chornobaivka, Ukraine, following a Ukrainian attack. (Image © 2022 Planet Labs PBC)

The CPMoD solution is modular and tailorable, and higher echelons require a distinct level of information fusion. For example, “Effective support area intelligence operations require the centralization of dedicated personnel and military intelligence (MI) equipment. To meet the current need, FM 3-0, *Operations*, established the rear command post, formerly called the support area command post (SACP) for corps and division headquarters.”¹⁴ When facing an enemy like the PRC, the rear CP and subordinate commands must be more agile.

Project Manager Mission Command develops mission command capabilities across the warfighting functions. The larger footprint of a division- or corps-level CP can become more mobile using the integrated mission command capabilities provided by the Command Post Computing Environment and the Mounted Mission Command. Supported by the Army’s Common Operating Environment, these interoperable mission command and situational awareness capabilities provide several essential, easy-to-use applications to include a common operational picture through a single mission command suite operated and maintained by Soldiers.¹⁵

This capability has already been tested at the National Training Center at Fort Irwin, California. It may help counter the PLA’s recent technological advances in identifying adversary command and control nodes like the forward or rear CP. The Command Post Computing Environment addresses intelligence sharing challenges that likely will be encountered in the INDOPACOM geography when occupying non-contiguous areas of operation.

Increasing U.S. Army Command Post Survivability

The Army Futures Command’s Command and Control Cross-Functional Team, one of six cross-functional teams, is working toward smaller, more mobile CPs to increase survivability and provide the technical infrastructure necessary for commanders to make timely decisions. According to the Program Executive Office Command, Control, Communications, and Network, aligning with the Army’s priorities for streamlining and modernizing tactical communications networks, the current “Command Post Integrated Infrastructure (CPI2) program will transition to the Command Post Modernization (CPMoD) program.”¹⁰ These CP designs incorporate innovative technologies that will, among other things, “support Army Network direction and strategic objectives,” expand expeditionary capabilities, improve the tactical computing environment, and incorporate energy-informed operations.¹¹

CPs may be able to balance lethality, speed, and precision without sacrificing the network infrastructure necessary for intelligence sharing. The CPI2 program recognizes this balancing problem and is developing solutions for the division, brigade, and battalion using feedback from Soldiers.¹² The redesigned CPs drastically decrease set-up and tear-down times while providing necessary network support for intelligence architecture. “As the program shifts to its next iteration . . . it will focus on including more flexible integrated command post capabilities.”¹³

It is important to remember that command and control within CPs at each echelon may look different.



The Army’s Technical Exchange Meeting 11, held in Savannah, GA, December 12-13, 2023, featured a prototype display of a Joint Light Tactical Vehicle integrated with Command Post Integrated Infrastructure capabilities. (U.S. Army photo by Paul Tardy)



Soldiers with the 2nd Stryker Brigade Combat Team, 2nd Infantry Division work inside a Mission Command Platform during Command Post Integrated Infrastructure training exercises at Yakima Training Center, Joint Base Lewis-McChord, in April-May, 2021. (U.S. Army Photo)

Intelligence Architecture Considerations

Intelligence architecture supporting mobile CPs designed to counter China in the INDOPACOM region will not likely be one size fits all. Still, it should be designed to be simple, intuitive, integrated, interoperable, and scalable to suit the needs of multidomain operations at different echelons.¹⁶ This will help to counter the PLA's ability to employ antiaccess and area denial activities, such as jamming, cyber warfare, and attacks on communications infrastructure, intended to disrupt intelligence operations. A robust intelligence architecture enhanced by the Command Post Computing Environment will enable information sharing and more agile CPs.

Intelligence collection management supported by the Command Post Computing Environment will be a critical capability in the INDOPACOM region. There is a high probability that Chinese military operations will focus on paralyzing adversary information systems, and the Command Post Computing Environment will provide survivability options for the United States Army. To counter China's focus on manipulating the electromagnetic spectrum, "The U.S. Army must expedite and prioritize the integration of collection management and sensor management tasks and capabilities supporting multidomain operations (MDO) capable forces in joint and coalition environments under joint all-domain command and control."¹⁷

Introducing mobile CPs with an intelligence architecture capable of integrating legacy systems for intelligence support and collection management will be important in meeting modern threats like the PRC. In the July 2020 *Military Intelligence Professional Bulletin*, Michael Kossbiel noted that "Applications on commercial off-the-shelf laptops will replace Command Post of the Future and Distributed Common Ground System-Army laptops....The planned future state converges

all warfighting functions' Army Battle Command Systems programs of record onto one suite of software and one server."¹⁸

One example of updated software that will support modern CPs facing threats like China in the INDOPACOM is the Army Intelligence Development Program. Implementation of this program will require adjustments to the current intelligence architecture within the proposed three-phase, two-year implementation plan.

Conclusion

China's PLA will likely continue to invest in its ambitious modernization initiative in an effort to compete with the United States Army. Emphasizing how intelligence supports CP survivability increases the chances of winning a conflict with China in the INDOPACOM region. Intelligence collection management through commercial off-the-shelf enhancements and adaptive intelligence architecture through innovative field systems will give the intelligence warfighting function a more comprehensive suite of tools to support CP survivability. 🌟

Endnotes

1. Ian M. Sullivan, "Three Dates, Three Windows, and All of DOTMLPF-P: How the People's Liberation Army Poses an All-of-Army Challenge," *Military Review* 104, no.1 (January-February 2024): 14-25, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2024/Sullivan/>.
2. Department of the Army, Army Doctrine Publication (ADP) 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 1-20.
3. Ibid., 1-19.
4. Figure 1-2 from Department of the Army, ADP 6-0, *Mission Command*, 1-20.
5. Department of the Army, ADP 2-0, *Intelligence* (Washington, DC: GPO, 31 July 2019), 2-2-2-3.

6. Michael Peck, "Ukraine's Attacks on Russian Commanders Have the US Army Worried about its Own 'Fat and Ponderous' Command Posts," *Military & Defense*, Business Insider, July 6, 2023, <https://www.businessinsider.com/ukraine-attacks-on-russia-us-army-command-post-vulnerability-2023-7>.
7. Hyun Ji Rim, "The US-China Strategic Competition and Emerging Technologies in the Indo-Pacific Region: Strategies for Building, Dominating, and Managing Networks," *Asian Perspective* 47, no. 1 (Winter 2023): 1-25, <https://dx.doi.org/10.1353/apr.2023.0000>.
8. Stew Magnuson, "SPECIAL REPORT: China Pursues Its Own Version of JADC2," *National Defense*, July 13, 2023, <https://www.nationaldefensemagazine.org/articles/2023/7/13/china-pursues--its-own-version-of--jadc2>.
9. Peck, "Ukraine's Attacks on Russian Commanders."
10. "Command Post Modernization," Project Manager Interoperability, Integrations and Services, Organizations, Program Executive Office Command, Control, Communications, and Network (PEO-C3N), n.d., <https://peoc3n.army.mil/Organizations/PM-Interoperability-Integrations-and-Services/Command-Post-Modernization/>.
11. Lisa Heidelberg and Kathryn Bailey, "Command, Unencumbered," *Army AL&T*, April-June 2018, 86-92, <https://asc.army.mil/web/news-alt-amj18-command-unencumbered/>.
12. "Command Post Modernization," Project Manager Interoperability, Integrations and Services, Organizations, PEO-C3N, n.d., <https://peoc3n.army.mil/Organizations/PM-Interoperability-Integrations-and-Services/Command-Post-Modernization/>.
13. Mollie Ryan, "Future Conflicts Demand Flexible and Mobile Command Posts," U.S. Army website, February 20, 2024, https://www.army.mil/article/273842/future_conflicts_demand_flexible_and_mobile_command_posts.
14. Julee R. Thomas, "The Vitality of Synchronized Intelligence Operations for a Division Support Area Command Post," *Military Intelligence Professional Bulletin* 47, no. 2 (April-June 2021): 36, <https://mipb.ikn.army.mil/media/myqf4tqu/2021-04-06-the-vitality-of-synchronized-intelligence-operations-for-a-division-support-area-command-post.pdf>; and Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: GPO, 21 March 2025), 79.
15. "Program Manager Mission Command," Organizations, PEO-C3N, n.d., <https://peoc3n.army.mil/Organizations/PM-Mission-Command/>; "Tactical Mission Command," PM Mission Command, Organizations, PEO-C3N, n.d., <https://peoc3n.army.mil/Organizations/PM-Mission-Command/Tactical-Mission-Command/>; "Mounted Mission Command," PM Mission Command, Organizations, PEO-C3N, n.d., <https://peoc3n.army.mil/Organizations/PM-Mission-Command/Mounted-Mission-Command/>; and Kris Osborn, "Common Operating Environment Assists Army Modernization," U.S. Army website, February 19, 2013, https://www.army.mil/article/96650/Common_Operating_Environment_assists_Army_modernization/.
16. Donald Beattie and Robert Coon, "Improving Intelligence Sharing," *Military Intelligence Professional Bulletin* 44, no. 4 (October-December 2018): 26, <https://mipb.ikn.army.mil/media/1uodqayc/mipb-2018-10-12-full-issue.pdf#view=fit&page=27>.
17. Michael T. Kossbiel, "The Future of Collection Management in Multi-Domain Operations," *Military Intelligence Professional Bulletin* 46, no. 3 (July-September 2020): 30, <https://mipb.ikn.army.mil/media/lnfb1rqc/2020-07-09-the-future-of-collection-managament-in-multi-domain-operations.pdf>.
18. Ibid.

SSG David Ball is currently an instructor at the Intelligence Analyst Basic Course at Fort Huachuca, AZ. He has served in the Active Duty Army, Air Force Reserves, and Army National Guard. SSG Ball's previous assignments include serving as an intelligence team leader for the 1st Combined Arms Battalion, 252nd Armored Regiment, North Carolina Army National Guard, analysis and control element intelligence team leader for the XVIII Airborne Corps, and all-source analyst for U.S. Central Command. He received a bachelor's degree cum laude in intelligence from American Military University with intelligence fundamentals professional certification.



PEOPLE'S LIBERATION ARMY VERSUS THE UNITED STATES ARMY: WHO WINS IN THE NETWORK MODERNIZATION FIGHT?

by Lieutenant Colonel Randie O'Neal (Retired)

Occupation of the Scarborough Shoal

In a possible near future, the People's Republic of China (PRC), after an increase of tensions with the United States and coalition forces in the Indo-Pacific Theater, commences the occupation of Scarborough Shoal in the South China Sea, some 220 kilometers from the Philippines. The PRC has stated that this shoal is necessary for the defense of the People's Republic of China and critical for the protection of their sovereign right to the freedom of navigation.¹



Disputed territory in the Indo-Pacific Region (graphic public domain by Voice of America)

Elements of the People's Liberation Army Navy occupy positions within these contested waters and declare a 12-mile limit in and around the shoal—an overt violation of previous international agreements and protocols. In response, and at the request of the Philippine president, a combined joint task force (CJTF) of the United States, Philippine, Japanese, and Taiwanese forces announce a combined joint operations area extending from the Spratly Islands, including Taiwan and the Japanese islands of Taketomi, Ishigaki, Tarama, and Miyakojima.

The United States deploys three U.S. Pacific Air Forces air wings that include a mix of strike, bomber, intelligence, surveillance, and reconnaissance, and support aircraft to the former Clark Air Base, Luzon. The U.S. Army's 25th Infantry Division from Hawaii, bolstered with U.S. Army maritime elements, moves to forward bases in the Philippines to provide sustainment and mobility for the forces in and around the combined joint operational area and the CJTF. A U.S. Marine expeditionary brigade deploys to the western coast of the island of Luzon, with some elements forward based on the island of Palawan. From the start, the CJTF experiences communications interoperability problems with coalition members and host nation elements. Tactical communications between the United States and Philippine forces are hampered as jamming and cyberspace attacks shut down key infrastructure, delay the deployment of forces, and render host nation utilities and telecommunications inoperable. Unknown entities on social media who notice Japanese participation in the CJTF announce, "The Japanese reoccupation of Luzon has begun." This announcement prompts public demonstrations and Japanese flag burnings across the Philippine islands.

Demonstrations and protests in Manila bring the city to a standstill as the government struggles to maintain order. The local press and social media call for the expulsion of "foreign occupiers" and an ouster of the sitting president. The PRC offers the Philippines \$50 million of immediate aid, with another \$50 million in Dragon's Gift² conditional assistance and loans over 10 years. The Dragon's Gift mandates the deployment of Chinese specialists in the country to remediate and rebuild infrastructure and assist in developing agriculture and other projects. The sole condition for providing this assistance is that the Philippines must cede the Scarborough Shoal to the PRC and expel any "foreign forces" currently residing in the Philippines and any territory it controls.

Editor's Note: This article was written in early 2024 as part of a professional writing competition open to the Army Soldiers and civilians of the 305th Military Intelligence Battalion, Fort Huachuca, Arizona. Competitors drew upon their operational and institutional experience as well as subject matter experts from across the Military Intelligence Corps to address challenges facing the intelligence warfighting function. For this competition, writers tailored their articles to the Indo-Pacific Command's area of responsibility.

Introduction

This work examines the People's Liberation Army's (PLA's) strategy to counter the United States Army's efforts to modernize its networks as part of the Joint All-Domain Command and Control strategy. A review of the relevant literature indicates that most of the PLA's efforts focus on replicating our strategic and doctrinal efforts, as well as our technology. The PLA's systems approach to warfare is its version of our joint multidomain operations; however, China has expanded the

continuum of warfare beyond the kinetic phase into the right now. The PLA began this fight well over ten years ago, and it continues to this day.

If the PRC develops its doctrine into actionable warfighting systems capable of affecting the United States presence and forward deployment to support key Indo-Pacific allies, this or a similar scenario may become a reality.

People's Liberation Army: Modernization Across Domains

The PLA is rapidly modernizing its capabilities across all warfare domains. It is also developing its own version of the Joint All-Domain Command and Control, which is the U.S. joint force "warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed

Members of the People's Liberation Army Information Warfare Support Force browse online news on desktop computers. (Image from the National Security Archive)



of relevance.”³ This modernization is changing how the PLA defines warfare in its doctrine; it now views modern warfare as a “contest between opposing operational systems” rather than merely opposing armies.⁴ Further, the PLA views conflict in terms of systems confrontation and systems destruction.

The PLA’s approach to warfare separates systems into two categories:

- ◆ Large, integrated systems made up of multiple, smaller systems (an interconnected system of systems).
- ◆ Individual systems that execute specific functions, such as command and control (C2), fires support, electronic warfare, intelligence, surveillance, and reconnaissance, logistics, and sustainment.

This approach is designed to identify targets both before and during a conflict.

Underlying this doctrinal framework are two concepts that aim to transform the PLA: *informationized warfare* and *intelligentized warfare*. Informationized warfare is described as the strategic implementation of information technology in the digital age with the aim of improving C2 and operations across the warfighting functions and the spectrum of conflict.⁵ Intelligentized warfare “seeks to increase the pace of future combat by effectively fusing information and streamlining decision making, even in ambiguous or highly dynamic operating environments.... It also amplifies the nascent concepts embodied by the Military-Civil Fusion effort.”⁶ This strategy focuses on acquiring technologies such as quantum computing, semiconductors, fifth-generation mobile network/long-term evolution (5G/LTE) data, nuclear and aerospace technology, gene editing, and artificial intelligence to achieve Chinese military dominance. These technologies are the backbone of an informationized and intelligentized PLA. “Careful alignment

of military and civilian efforts enables the synchronization of efforts and streamlines the fielding process for the PLA.”⁷

For the PLA, the final steps in its efforts to counter peer and near-peer threats are to enable its operational and tactical forces through the informationization and intelligentization of its integrated joint service capabilities and the use of emerging and disruptive technologies and techniques, which are described as—

- ◆ Attrition warfare through intelligent swarms of unmanned aircraft systems or other platforms to overwhelm the adversary’s ability to respond.
- ◆ Cross-domain (joint) warfare that will integrate capabilities across land, sea, air, space, and cyberspace, as well as the emerging cognitive domain.
- ◆ Artificial intelligence-based space confrontations that will deny and destroy the adversary’s use of space-based C2, global positioning systems (GPSs), and intelligence, surveillance, and reconnaissance capabilities.
- ◆ Cognitive control operations that will improve information processing in support of situational awareness and decision making at the operational and tactical levels.⁸

These capabilities currently appear aspirational, even for Western militaries. However, given the assets and resources the PLA is devoting to the effort, it is likely the PLA may achieve some breakthroughs, providing China with a significant advantage, as demonstrated by its cyberspace capabilities in recent years.

What works against China is its lack of operational military experience in modern warfare, its other significant efforts, such as the Belt and Road Initiative’s international infrastructure projects, and its declining population.⁹ All three hamper

China's ability to field an effective military and a technological and industrial workforce competent enough to actualize this great leap forward. Nevertheless, it is likely the PLA may see some significant improvements to their C2 and intelligence within 8 to 10 years, as well as advancements in cross-domain operations that they could leverage against peers, near peers, and other adversaries in the Indo-Pacific region. Given China's aspirations for informationized warfare and intelligentized warfare in the near future, what does this all mean?

The PLA has methodically analyzed the strategy, doctrine, tactics, and wars that the United States (China's primary adversary) and other adversaries in the Indo-Pacific region have fought since the early 1990s. This analysis has resulted in a review of China's warfighting capabilities across the five military domains—land, maritime, air, space, and cyberspace—to which they have added a sixth: the cognitive domain. Even in Western military science, the cognitive domain materializes as a distinct domain that molds how an adversary perceives information to gain knowledge and understanding. Using this analysis in combination with the concepts of informationized warfare and intelligentized warfare, the PLA has determined that warfare will further fall into two distinct realms: systems confrontation and systems destruction.

Systems Confrontation: The War Before the War

Systems confrontation is defined as “a contest among adversarial systems”¹⁰ waged not only in the traditional domains of land, air, and sea but also in space, cyberspace, and even the psychological domain. This emerging domain encompasses the PLA's concept of *cognitive domain operations*, which expands on traditional psychological warfare using information to influence the adversary's thought processes, ranging from peacetime public opinion to wartime decision making,¹¹ as well as the Western notion of *cognitive warfare*, which expands the accepted continuum of warfare into how individuals perceive information to gain knowledge and understanding.¹²

Cognitive Warfare

While cognitive warfare lacks a widely accepted definition, initial proposals contain at least one of three common themes:

- ◆ The intent to influence specific individuals and groups on political matters, understanding that war is a continuation of politics by other means.¹³
- ◆ The explicit targeting of human cognition—how people perceive and interpret information to gain knowledge and understanding.¹⁴
- ◆ The use of psychology and advanced technologies to target individuals or groups precisely.¹⁵

Systems confrontation is a duel between opposing military operating systems, with the center of gravity being the information architecture. The destruction of key technological capabilities, weapons, and organized personnel can paralyze

an enemy's operating system. An approach integrating land, sea, air, cyberspace, and space domains can render opposing information systems inoperable, thus achieving information dominance. Systems confrontation gives the PLA a better understanding of its adversaries, allowing it to find their weaknesses and counter their strengths. The PLA wants to infiltrate and probe its adversaries' human and technical systems for weaknesses.¹⁶

One example of these targeted intrusion activities is Operation Shady Rat (2006–2011), which targeted systems around the world, identified key information, and exfiltrated hundreds of terabytes of research data (technical, defense, infrastructure, and organizational) back to the PRC for exploitation and use.¹⁷ Many experts believe the operation is still ongoing today.¹⁸ Another example is the U.S. Office of Personnel Management data breach between 2013 and 2015. This data breach targeted security clearance records and compromised the personal information of over 21 million cleared U.S. federal employees and contractors.¹⁹ The information acquired through such active cyberspace operations has furthered the PRC's technical capability to develop better weapons, disrupt or destroy key information technology infrastructure, and further develop human intelligence sources through influence and coercion using compromised personal data. Systems confrontation is “the war before the war,” pervasive and ongoing. It strikes at the adversary's human, physical, and technical systems to develop them as targets in the event of a conflict.

Systems Destruction: Target and Destroy the Systems

Systems destruction intends to “disrupt, paralyze, or destroy the operational capability of the enemy's operational systems.”²⁰ This goal is achieved through a mix of “kinetic and non-kinetic strikes against key points and nodes.”²¹ Systems destruction begins at the onset of open conflict with an adversary, taking advantage of the groundwork laid through systems confrontation. Systems destruction specifically targets four key areas:

- ◆ Information flow of the adversary's operational systems.
- ◆ Essential elements of the adversary's operational system (e.g., C2, reconnaissance, intelligence, and firepower assets).
- ◆ Operational architecture of the adversary's operational system (e.g., C2 network, reconnaissance network, intelligence network, or firepower network).
- ◆ “Time sequence and/or tempo of the adversary's operational architecture.”²²

Systems destruction targets these four areas with the intent to “undermine the operation system's own

‘reconnaissance-control-attack-evaluation’ process.”²³

Having described the PLA’s possible future capabilities, let’s examine its key target: the U.S. Army and its network modernization efforts.

U.S. Army Network Modernization

One of the most important (and targetable) of the U.S. Army’s six modernization priorities is the modernization of its networks. These networks include command post mobility, secure wireless communications, cybersecurity, and edge computing.²⁴ The improvement and expansion of network capabilities will enable the U.S. Army to fight and win in a multidomain environment by maintaining peer and near-peer adversary communications and information technology overmatch in the next 5 to 10 years. This nests within the U.S. Army’s intent to be “capable of conducting Multi-Domain Operations (MDO) as part of an integrated Joint Force in a single theater by 2028, and ready to conduct MDO across an array of scenarios in multiple theaters by 2035.”²⁵

Network Modernization Initiatives

- ◆ *Command post mobility* is the ability for a command post to quickly displace, move, and operate on the move, with the idea that the fight doesn’t stop because the command post is moving. Ground forces need ruggedized, hardened, on-the-move equipment and ability networking. This means that the command post is small, adapts to any terrain, and is reliable in the face of unanticipated weather, power, and cyberspace conditions.²⁶
- ◆ *Secure wireless communications* is a newer class of deployable, small wireless access systems that bring the benefits of classified wireless access to warfighters in the field. It allows warfighters to use commercial smartphones, tablets, and laptops to access classified information over Wi-Fi and 5G.²⁷
- ◆ *Cybersecurity* is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. As an emerging warfighting domain, cyberspace has gained significance because it transcends and touches all other domains. The Department of Defense considers cyberspace to be at the same level as traditional land, sea, and air warfighting domains. With our ever-increasing use of the cyberspace domain and the expansion of connectivity and devices available to tactical forces, the requirement to secure and defend these networks from disruption and destruction is a top priority.²⁸
- ◆ *Edge Computing* involves bringing computing capabilities to where the mission is in the field. It means that data does not have to travel back to a data center to be processed or analyzed. With the expectation that communications will be degraded from the start of large-scale combat operations, the Army wants to decentralize communications and make tactical networks function like forward data centers that will host situational awareness, mission command, and command and control applications and databases.²⁹

People’s Liberation Army: Countering U.S. Modernization

The PLA’s demonstrated pervasive capabilities in technical collection, offensive and defensive cyberspace operations, open-source intelligence, and human intelligence make the U.S. Army’s network modernization the most important and most targetable of its modernization priorities.³⁰ The PLA’s doctrinal shift and its concentration on systems confrontation and warfare are direct challenges to our network modernization efforts, affecting all aspects of how the U.S. Army will conduct multidomain operations.

These efforts will directly affect how intelligence is collaborated, coordinated, and disseminated throughout the operational environment. The network is connected to every warfighting function, including intelligence; if it is degraded, disrupted, or compromised, our ability to provide situational awareness and timely intelligence to the commander in support of multidomain operations will be significantly degraded.

Avoiding Disruption and Countering People’s Liberation Army Actions

Fortunately, Army network modernization is still in the early stages, and we know what the PLA is planning. At the operational and tactical levels, the Army must emphasize training on analog procedures for the military decision-making process and other intelligence warfighting function tasks, particularly during intelligence preparation of the operational environment, to ensure continuity in the event of disruption and as backups to our digital systems. Also, our tactical and operational forces should exercise and practice these analog tactics, techniques, and procedures at home stations, and they should be evaluated regularly at combat training centers on their use of analog methods across all warfighting functions.

While our systems are still in the developmental and early operational phases, we must emphasize cybersecurity for networked systems. We must also develop built-in, stand-alone, unplugged capabilities that allow systems to continue operations when the network is disrupted, compromised, or out of service.

Other remedies across the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy spectrum might include an aggressive mix of—

- ◆ Heightened operations security on developmental efforts (doctrine, organization, personnel, training, and policy).
- ◆ Expanded research into low bandwidth and stand-alone solutions that could relay content through proximity connects while disconnected (materiel).

- ◆ Low-signature communications systems that would allow connectivity to the network using high-frequency, wired, mesh, or other connectivity options (facilities and materiel).

Other actions could involve assisting host nations with cybersecurity for critical infrastructure such as networks, telecommunications, utilities, etc., as well as assisting in developing and refining analog tactics, techniques, and procedures. Providing this assistance will help avoid operational disruptions and maintain continuity of operations in the coalition environments.

Impact on the Warfighter

Operating in an environment where digital networks are vulnerable to disruption may limit the ability to communicate. Therefore, warfighters must train to fight across all warfighting functions in analog methods. Emphasize analog intelligence procedures to support the commander, learn to operate without connectivity, and understand that regular training with the analog options is necessary.

We need to explore and expand on the importance of the cognitive domain in relation to networks. We must broaden our awareness of the use of social media and other perception-generating systems and their influence on operations by both the PLA and the U.S. Army in the Indo-Pacific Region. As the cognitive domain becomes more significant, Army

intelligence professionals must consider how perception influences operations before forward deployments.

Conclusion

Although the PLA seems to have a head start in its efforts to modernize and counter U.S. Army network modernization efforts, we must realize that much of what they have done is a product of replication and mimicry, with little or no a priori experience, effort, or research. The PRC's advanced persistent threat operations,³¹ like Operation Shady Rat, might provide technical details, specifications, and other information about our network modernization activity, but their methods were compromised. However, we should not be complacent—we must recognize that our networks, however modernized they are, are under constant, advanced, persistent attack. Further research into low-bandwidth, stand-alone solutions and minimal signature communications that could serve as a survivable fallback must be developed. We also must plan for the disruption and denial of our networks and train on analog procedures as a contingency solution, allowing us to continue the multidomain fight. So, who wins the network modernization fight? The United States can by reinforcing analog procedures and working closely with coalition partners on communications, operations, and cyberspace security.

Now, let's review our notional scenario again, but this time, we'll incorporate the countermeasures we've discussed. 🌟

Coalition Forces Prevent Occupation of the Scarborough Shoal

Upon the commencement of the PLA's actions to take the Scarborough Shoal, the United States Army deploys training elements to work with the Philippine Army tactical and operational units to provide training on staff procedures and interoperability. At the same time, the United States sends cyber-focused advise and assist teams to review the Philippine national cyberspace infrastructure and local network surety. At their home stations, the U.S. Army and Marines emphasize using analog tactics, techniques, and procedures while working in digitally austere environments. As the PLA Navy's actions become more provocative, the GPS and radio communications of coalition forces on the eastern coast of Luzon are increasingly inaccurate and periodically disrupted. However, because the coalition forces have trained in alternative, analog methods, this is a minor inconvenience. United States military operational and tactical personnel and their Philippine counterparts work in coordination and engage the host nation's civilians, employing many of them to assist as interpreters and laborers, both skilled and unskilled. The PLA Navy's inability to intimidate the coalition forces results in an operational standdown and a pullback from the area around the Scarborough Shoal. In the aftermath, the Philippine president thanks the United States and requests the permanent basing of United States forces in the Philippines after a forty-year absence.

Endnotes

1. Andrea Chloe Wong, "The 2012 Scarborough Shoal Standoff: Analyzing China in Crisis with the Philippines," *Encounters and Escalation in the Indo-Pacific: Perspectives on China's Military and Implications for Regional Security*, NBR Special Report No. 108, ed. Oriana Skylar Mastro (Seattle, Washington: The National Bureau of Asian Research, 2024), 75.
2. Min Ye, "The Dragon's Gift: An Empirical Analysis of China's Foreign Aid in the New Century," *International Trade, Politics, and Development* 6, no. 2 (2022): 73-86, <https://doi.org/10.1108/ITPD-06-2022-0010>.
3. Department of Defense, JADC2 Cross-Functional Team, *Summary of the Joint All-Domain Command & Control (JADC2) Strategy* (Washington, DC, 2022), <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf>.

4. Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), iii, https://www.rand.org/pubs/research_reports/RR1708.html.
5. Department of the Army, Army Techniques Publication (ATP) 7-100.3, *Chinese Tactics* (Washington, DC: Government Publishing Office [GPO], 09 August 2021), 1-9–1-10. Change 1 was issued on 24 November 2021.
6. Department of the Army, ATP 7-100.3, *Chinese Tactics*, 1-10–1-11; and Department of State, *Military-Civil Fusion and the People's Republic of China* (Washington, DC, 2020), <https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf>.
7. Department of the Army, ATP 7-100.3, *Chinese Tactics*, 1-11.

8. Michael C. Horowitz and Lauren Kahn, "DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military," *Council on Foreign Relations* (blog), November 4, 2021, <https://www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape>.
9. Laura Silver and Christine Huang, "Key Facts About China's Declining Population," Pew Research Center, December 5, 2022, <https://www.pewresearch.org/short-reads/2022/12/05/key-facts-about-chinas-declining-population/>; and James McBride, Noah Berman, and Andrew Chatzky, "China's Massive Belt and Road Initiative," *Council on Foreign Relations* (blog), February 2, 2023, <https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative>.
10. Engstrom, *Systems Confrontation and System Destruction*, ix.
11. Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief* 19, no. 16 (September 6, 2019), <https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/>.
12. Andrew MacDonald and Ryan Ratcliffe, "Cognitive Warfare: Maneuvering in the Human Dimension," *Proceedings* (U.S. Naval Institute) 149, no. 4 (April 2023), <https://www.usni.org/magazines/proceedings/2023/april/cognitive-warfare-maneuvering-human-dimension>.
13. Ibid. MacDonald and Ratcliffe's note consisted of commentary stating, "inclusion of the word 'political' distinguishes cognitive warfare from economic tools—such as targeted advertisements—that seek to influence behavior for profit."
14. Paul Ottewell, "Defining the Cognitive Domain," *Over the Horizon*, December 7, 2020, <https://othjournal.com/2020/12/07/defining-the-cognitive-domain/>.
15. Koichiro Takagi, "The Future of China's Cognitive Warfare: Lessons from the War in Ukraine," *War on the Rocks*, July 22, 2022, <https://warontherocks.com/2022/07/the-future-of-chinas-cognitive-warfare-lessons-from-the-war-in-ukraine/>.
16. Engstrom, *Systems Confrontation and System Destruction*, ix.
17. Dmitri Alperovitch, *White Paper Revealed: Operation Shady Rat* (Santa Clara, CA: McAfee, 2011), http://graphics8.nytimes.com/packages/pdf/technology/mcafee_shadyrat_report.pdf.
18. "The Biggest Hack in History—Operation Shady Rat," Hacked.com, <https://hacked.com/the-biggest-hack-in-history-operation-shady-rat>.
19. U.S. Congress, House Committee on Oversight and Government Reform, *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, 114th Cong., 2d sess., H. Rep., <https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf>.
20. Engstrom, *Systems Confrontation and System Destruction*, iii.
21. Ibid.
22. Ibid., 18.
23. Ibid., x–xi; and Li Yousheng [李有升], Li Yin [李云], and Wang Yonghua [王永华], eds., *Lectures on the Science of Joint Campaigns* 《联合战役学教程》 (Beijing: Military Science Press [军事科学出版社], 2012), 74.
24. Charlie Kawasaki, "Four Future Trends in Tactical Network Modernization," *Industry Insight, Army AL&T*, (January–March 2019): 122–125, https://asc.army.mil/docs/pubs/alt/archives/2019/Jan-Mar2019_ArmyALT.pdf.
25. Department of the Army, *2019 Army Modernization Strategy: Investing in the Future* (Washington, DC: GPO, October 2019), 3, <https://stratml.us/pdfs/AMS.pdf>.
26. Kawasaki, "Trends in Tactical Network Modernization," 123–124.
27. Ibid., 124.
28. Ibid., 124–125.
29. Ibid., 125.
30. Department of the Army, Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations, 2028* (Fort Eustis, VA: TRADOC, 27 November 2018), <https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf>.
31. Advanced persistent threats are "stealthy cyberattack[s] in which a person or group gains unauthorized access to a network and remains undetected for an extended period. The term's definition was traditionally associated with nation-state sponsorship, but over the last few years we've seen multiple examples of non-nation state groups conducting large-scale targeted intrusions for specific goals." Sarah Maloney, "What Is an Advanced Persistent Threat (ATP)?" *Malicious Life* (blog), Cybereason, <https://www.cybereason.com/blog/advanced-persistent-threat-apt>.

LTC (Retired) Randie O'Neal is an intelligence professional with over 40 years of service to the U.S. Army as an officer and a contractor. After his retirement as a lieutenant colonel in 2014, he worked as a contractor for Program Manager-Saudi Arabia National Guard and U.S. Military Training Mission Saudi Arabia in support of training, modernization and transformation initiatives. He is currently a senior instructor for the Intelligence Analysis Committee at Ft. Huachuca, AZ. Notable assignments during his military career include as the all-source intelligence production section leader for Joint Task Force Panama (U.S. Army South) during Operation Promote Liberty; Commander, Company B, 104th Military Intelligence Battalion; G-2, 63rd Regional Readiness Command; Counterterrorism Mission Management Center team leader, National Security Agency; and as an advisor team leader and camp commander in support of the Headquarters, Iraqi Federal Police and the Kurdish Peshmerga Zeravani during Operations Iraqi Freedom and New Dawn.