MI PROFESSIONAL BULLETIN

January–June 2022
PB 34-22-2

SEMIANNUAL ONLINE COLLECTION

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

Mailing Address
MIPB (ATZS-DST-B), DOTD, USAICoE, 550 Cibeque St., Fort Huachuca, AZ 85613-7017.

This publication is approved for public release. Distribution unlimited.

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

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

By Order of the Secretary of the Army:

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

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army

2309502

MI PROFESSIONAL BULLETIN

January–June 2022

CONTENTS

Human Intelligence Employment during Multidomain Operations

by Warrant Officer 1 David L. McGillivray

A United States special operations Service member conducts reconnaissance in support of Operation Resolute Support in southeast Afghanistan, April 2019. (U.S. Army photo by SGT Jaerett Engeseth). Adapted from original

Introduction

Throughout the joint phases, U.S. Army human intelligence (HUMINT) collectors conduct the full spectrum of HUMINT operations (source operations, liaison, screening, interrogation, and debriefing). The information obtained during these operations helps set the theater, influence situational understanding, and enable decision making. Additionally, HUMINT often assists with providing the answer to the commander's "why?"

The Army conducts multidomain operations in support of joint forces through four strategic roles arranged by purpose:[1]

- ✦ Shape operational environments.
- ✦ Prevent conflict.
- ✦ Conduct large-scale ground combat.
- ✦ Consolidate gains.

To support joint operations, Army HUMINT must successfully align their relationship of the Army strategic roles with the joint phases. Army HUMINT operations can occur across multiple domains and in multiple theaters, spanning all phases of operations. When armed conflict with adversaries becomes unavoidable for the United States, our forces' daily intake of detainees may include thousands of enemy prisoners of war, many of whom possess unique intelligence that only Army HUMINT can exploit.

HUMINT Operations across the Army Strategic Roles

Army HUMINT doctrine informs us how and when to employ the various HUMINT functions across the Army's strategic roles and joint phases to help provide commanders and staffs with detailed and current knowledge of our adversaries.

Shape Operational Environments and Prevent Conflict. The Army strategic roles of shape operational environments and prevent conflict correspond with the joint *shape* phase and *deter* phase.[2]

Shape Phase. During the shape phase, Army HUMINT collectors focus primarily on overt debriefing programs, source operations aimed at adversary hard targets, and the establishment of responsive source networks in advance of conflict. It is important to note that most commanders have Army HUMINT collectors in their formations who are capable of performing advanced levels of source operations. Unfortunately, most tactical Army units do not have the requisite authorities or mission to conduct those functions during shaping activities. Commanders should remain aware

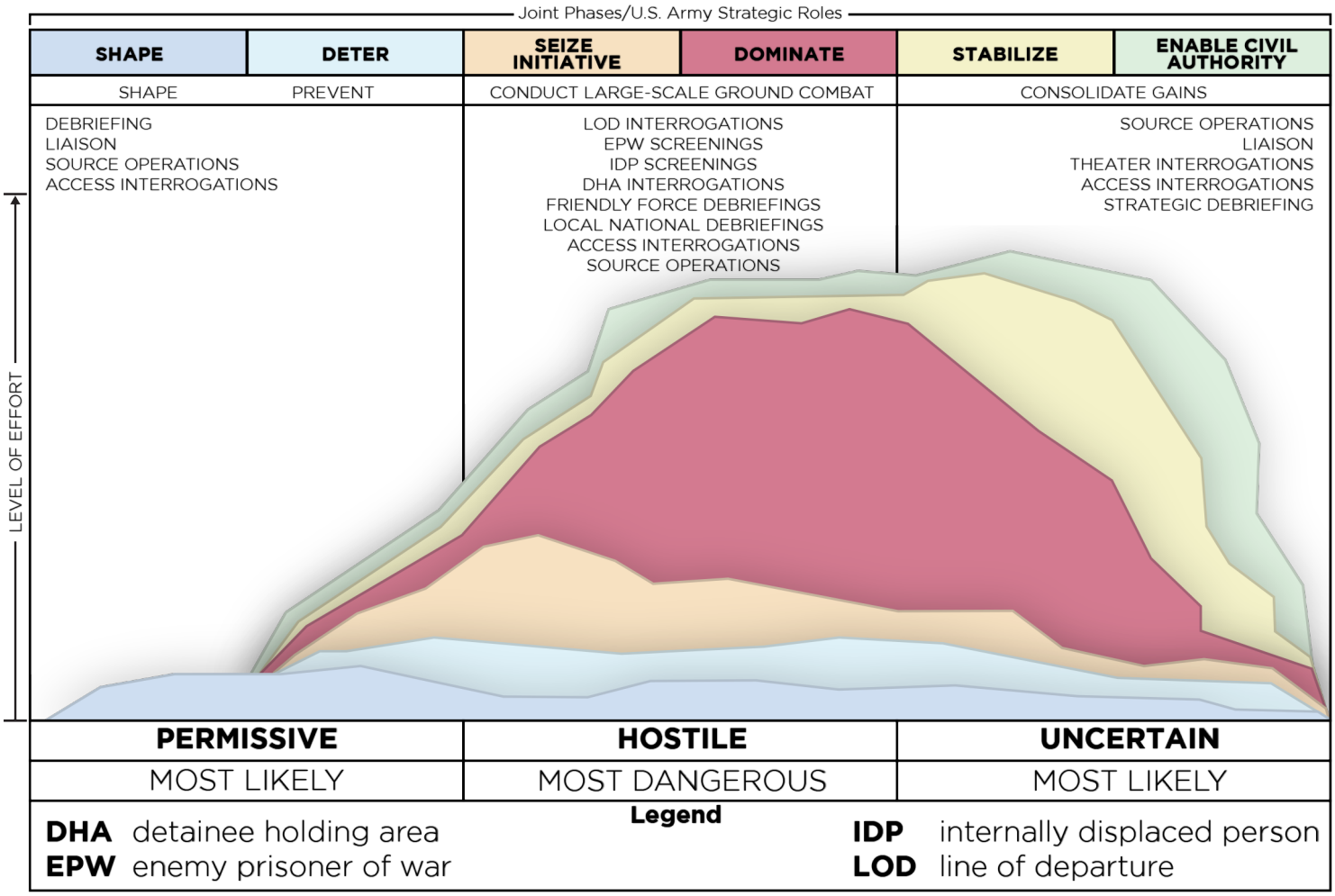


Figure 1. HUMINT Level of Effort across Army Strategic Roles[3]

of the HUMINT capabilities within their units and seek to maximize those capabilities where applicable. To fulfill the mission of setting the theater, shaping, and deterring while in a competitive environment and in advance of conflict, Army HUMINT collectors must be actively involved in identifying, engaging, and collecting from HUMINT sources to prepare the operational environment and maintain HUMINT readiness.

> **The intent of the deter phase is to prevent an adversary from undesirable actions through the posturing of friendly capabilities and demonstrating the will to use them....Many actions in the deter phase build on activities from the previous phase and are conducted as part of security cooperation.[5]**

HUMINT collectors can also perform liaison. Liaison with coalition forces can occur during the shape phase, including liaison with alliance partners (for example, the North Atlantic Treaty Organization, Five Eyes, and other treaty partners). Shaping activities occur throughout all operations. HUMINT provides support to shaping activities with the end state of helping to set conditions for successful theater operations. In this phase, HUMINT helps to increase commanders' situational understanding of both allies and adversaries in the area of responsibility, as well as the operational environment. Additionally, HUMINT supports efforts to gain and enhance international legitimacy and multinational cooperation by developing allied and friendly military capabilities and improving intelligence sharing in hopes of mitigating crisis.[4] Some of the activities HUMINT collection focuses on during this phase are:

- Enemy activities.
- Criminal elements' operations.
- Effects on the area of operations.
- Proxy actions or intent.
- Strategic facilities and networks.
- Unstable governments.
- Allied communications limitations or military skills.

Deter Phase. During the deter phase, HUMINT collectors continue to focus on debriefing programs and source operations. It is vital that these activities continue from the shape phase into and throughout the deter phase. HUMINT collectors will continue with many of the same tasks from the shape phase with adjustments to collection efforts based on commanders' information requirements. HUMINT prioritizes efforts based on the environment changing from a stable (shape) environment to a potentially threatening (deter) environment. As the operational environment evolves, the commander's efforts shift based on the intelligence warfighting function efforts. Collection requirements may change when indications and warnings create decision points for commanders that push the environment to the next phase–seize initiative.

Tailoring forces and task organization to a specific purpose is a crucial facet of deterrence activities. Therefore, HUMINT collection teams should remain flexible in meeting the commander's intent and changing their collection focus based on the commander's guidance. Their overt collection operations may evolve to more sophisticated source operations, and sources may be passed between units or agencies to support potential offensive operations. Coordination and deconfliction occur with joint and allied partners to focus on specific targets, as well as information sharing across the combined joint operating environment.

HUMINT leaders should begin to plan for any crisis that may involve internally displaced persons or enemy prisoners of war. The Army has refocused on conflict in large-scale combat operations with peer and near-peer threats. To prepare, HUMINT Soldiers must plan for large-scale screening and interrogation operations during both the seize initiative

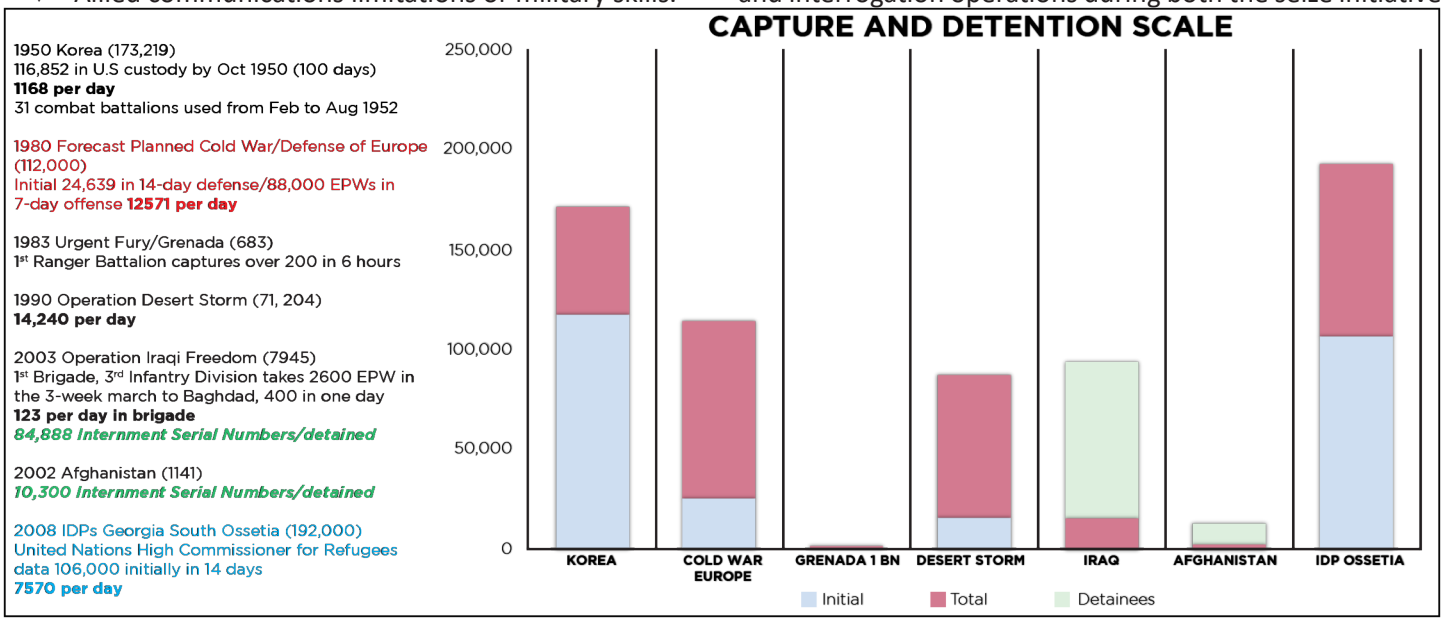


Figure 2. Enemy Prisoners of War/Internally Displaced Persons Historical Capture and Detention Rates[6]

phase and the dominate phase in order to support the commander's decision making. An increased focus on liaison between friendly forces is necessary for the sharing and coordination of information and sources. Army HUMINT will identify pockets of instability within local ethnicities, tribes, religions, and people groups to provide early warning of a civil or military-civilian incident. In doing so, Army HUMINT will identify the concerns of the various factions of the populace, allowing opportunities to assist local governance and bolster citizens' confidence in their government.

Conduct Large-Scale Ground Combat

The Army strategic role of conduct large-scale ground combat relates to the joint *seize initiative* phase and the *dominate* phase.[7]

Seize Initiative Phase. During the seize initiative phase, HUMINT collectors conduct screening operations to identify defectors, internally displaced persons, and enemy prisoners of war, as well as to identify personnel who may be able to provide information in response to information collection requirements. Screening may occur at or near the line of departure, detainee holding areas, urban population centers where internally displaced persons/refugees tend to migrate, or internally displaced persons/refugee camps. The most relevant information is likely to come from the interrogations of enemy prisoners of war and debriefings of internally displaced persons because of the rapid expiration of valid information in a dynamic operational environment. Source operations may continue, but the speed and nature of operations within the seize initiative phase do not create a permissive environment conducive to sophisticated full-cycle source operations. HUMINT collection will focus on the collection of information pertaining to enemy dispositions, intentions, plans, order of battle, enemy courses of action and intent, capabilities, and morale, as well as assisting in battlefield damage assessment.

HUMINT enables a commander's information advantage during the seize initiative phase; the more rapidly and thoroughly HUMINT collectors can screen and interrogate enemy prisoners of war, the better enabled commanders will be to seize and maintain the initiative. It is essential to drive focused collection with a forward-thinking collection management plan that provides time for planning HUMINT operations and is analyzed and disseminated no later than the combined arms rehearsal. Focused collection driven by collection tasks guidance gives commanders the best operational picture and helps fires support combat operations through the targeting of the high-priority target list. Units must plan for detainee operations in coordination with the unit provost marshal and higher headquarters to ensure support for such operations.

During the seize initiative phase, commanders must consider committing large amounts of combat power to detainee-handling tasks. With proper placement of HUMINT collection teams forward toward the forward line of troops, screening operations can assist with transferring detainees to detainee collection points or detainee holding areas. Collectors conducting interrogations in consolidation areas will benefit from HUMINT collection teams properly screening detainees at or near point of capture. The expedient interrogation of detainees can provide commanders with timely, relevant, accurate, predictable, and tailored information.

Operation Red Dawn: Premier Interrogation Capability

After coalition forces invaded Iraq in March 2003, toppling its government, the United States military launched an intensive manhunt for the deposed dictator, Saddam Hussein, who had escaped Baghdad when the capital fell. During Operation Red Dawn, U.S. troops extracted Hussein from a hole in the ground in Tikrit. Months of meticulous intelligence gathering through interrogations by United States Army SSG Eric Maddox played a pivotal role in the operation—considered the biggest triumph of the Iraq War—with no trigger pulling or drone strikes.[8]

Dominate Phase. During the dominate phase, Army HUMINT's primary focus is interrogating, screening, and debriefing. Brigade-assigned HUMINT collection teams will continue to focus on battlefield interrogations in support of maneuver elements, while expeditionary-military intelligence brigade HUMINT collection teams and U.S. Army Reserve HUMINT capabilities will focus on division and higher requirements. When established within a joint area of operations, the joint interrogation and debriefing center (JIDC) is the theater-level interrogation effort.

The JIDC conducts intelligence interrogation and debriefing collection operations to support contingency and combat operations in the joint operations area. Typically, it is administratively and operationally self-sufficient and operates within a theater or strategic detention facility. The military intelligence battalion (interrogation) command, staff, personnel, and equipment form the primary operational capability of the JIDC.

Capture rates and availability of interrogator-certified personnel play a large part in how many detainees can yield intelligence value within a set timeframe. Time is HUMINT's most critical asset. The longer enemy prisoners of war are in custody, the less valuable their information is. It is crucial that

U.S. Army photo

A military police Soldier demonstrates a body search on a detainee as part of detainee operations training at the Joint Multinational Readiness Center, Hohenfels, Germany.

the interrogation of enemy prisoners of war occur as soon as possible after their capture. That is why HUMINT collection teams on the forward line of troops are so beneficial to satisfying priority intelligence requirements. The exception is enemy prisoners of war who many have knowledge of strategic significance, such as campaign planning; these individuals should be sent to higher-echelon facilities, in rear areas, for more in-depth interrogation.

Commanders and staff must anticipate and plan for potentially high rates of capture, especially during the dominate phase. If coalition forces are breaking the enemy's will to resist, mass surrenders on the battlefield can complicate and tax the maneuver element, as well as the brigade's enablers charged with removing potential detainees from the battlefield. Screening operations, tactical questioning, and interrogations can all be negatively affected when a unit is inundated with a high number of detainees during a mass surrender.

The collection manager is vital throughout all planning and specifically for interrogation operations. HUMINT must anticipate and leverage collection managers to plan for mass surrenders during large-scale combat operations at all echelons. If we know the threat characteristics, including the threat structure for a unit, we can anticipate whom we will face, including their reserve and adjacent units, which will provide our forces with tactical advantage. Through source operations and battlefield interrogations as well as interrogations within detainee holding areas, Army HUMINT can help identify enemy intentions, tactics, and techniques. It can also help identify the potential for the enemy to attempt to slow our tempo with a variety of obstacles such as chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) threats, criminal elements/proxies, or special forces personnel to impede our logistical lines.

During the dominate phase, HUMINT must position forward and coordinate with maneuver elements to conduct intelligence interrogations of detainees with time-sensitive information at or near the point of capture. When units afford HUMINT the ability to interrogate as close to the point of capture as possible—rather than waiting to interrogate in rear areas—HUMINT enables commanders to rapidly converge effects. Given a robust communications suite and a tactical vehicle with appropriate armament, HUMINT can push forward at or near the point of capture to interrogate and exploit potential time-sensitive information and documents enabling friendly forces to dominate the enemy.

Additionally, HUMINT can provide input to battle damage assessments, which are critical in the dominate phase. Battle damage assessments help the commander see better through the fog of war.

Consolidate Gains

The Army strategic role of consolidate gains includes the joint *stabilize* phase and the joint *enable civil authority* phase.[9]

Stabilize Phase. During the stabilize phase, military units performing stability tasks operate in a complex environment with and among many actors. Much like the other phases, stabilize provides a constant "ebb and flow" of challenges for military commanders. Although there may be a fleeting elation within the local populace following the end of major combat operations, the complex nature of stability operations tends to overwhelm a military commander with multiple problems all at once. ATP 3-07.5, *Stability Techniques*, discusses the need to secure the peace, empower the host nation's intelligence and security apparatus, secure borders, and protect key personnel and facilities following combat operations.[10] These crucial actions are all in line with the principles of stability:[11]

- Conflict transformation.
- Unity of effort and unity of purpose.
- Legitimacy and host-nation ownership.
- Building partner capacity.
- Rule of law.

To execute the tasks in the stabilize phase, a robust intelligence effort and partner information sharing are necessary. With freedom of movement and HUMINT-specific collection emphasis, Army HUMINT will excel in this phase to provide commanders unique intelligence information that is otherwise unavailable. Army HUMINT will partner with the host nation to conduct necessary interrogations of persons held in foreign custody. This assists in transforming conflict and legitimizing host-nation security forces. Having the proper authorities and agreements with the host nation will allow HUMINT, through source operations, to assist in targeting bad actors that may be undermining host-nation and U.S. stabilization efforts. HUMINT can and should work closely with special operations forces to identify points of friction with the host nation, partner forces, and local populace that may hinder stabilization efforts. It is vital that Army HUMINT work closely with security forces to identify threats during this phase.

Enable Civil Authority Phase. During the enable civil authority phase, Army HUMINT collectors will focus on overt debriefings, source operations, liaison, and ongoing theater interrogations to continue gathering information of intelligence value. This focus will assist civil authority to regain its ability to govern and administer the services and other needs of the population. For commanders to reach their military end state, legitimate civil authority must be established to the point where further outside military intervention is unnecessary. Once we transfer responsibility for political and military affairs to the host nation, Army HUMINT collectors may still conduct operations while the host nation's national army, police, and other security forces are established.

Conclusion

Army HUMINT can provide commanders with critical and unique intelligence throughout all phases of joint operations. Army HUMINT conducts full-spectrum HUMINT operations to set the theater, shape the commander's understanding, and enable the commander's decision making. Army HUMINT can play a vital role to inform leaders at all levels of the Army and Department of Defense; Army HUMINT can be uniquely suited to gather information otherwise unavailable to commanders. Army HUMINT must provide effective support across the range of military operations to the Army as a discipline of the intelligence warfighting function in order to achieve our national objectives.

Endnotes

1. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 1-14. Change 1 was issued on 6 December 2017.

2. Department of the Army, FM 3-0, *Operations*, 1-14.

3. Graphic is adapted from figures found in Department of the Army, FM 3-0, *Operations*, 1-12, 1-14.

4. Department of the Army, FM 3-0, *Operations*, 1-13.

5. Ibid.

6. The data points for this graphic were gathered by Headquarters, Department of the Army G-2X with assistance from Headquarters, Department of the Army Office of the Provost Marshal General.

7. Department of the Army, FM 3-0, *Operations*, 1-14.

8. Volker Janssen, "The Surprising Interrogations That Led to Saddam Hussein's Capture," History.com, A&E Television Networks, November 8, 2018, updated January 31, 2019, https://www.history.com/news/saddam-hussein-capture-iraq-interrogations-eric-maddox.

9. Department of the Army, FM 3-0, *Operations*, 1-14.

10. Department of the Army, Army Techniques Publication 3-07.5, *Stability Techniques* (Washington, DC: U.S. GPO, 31 August 2012).

11. Ibid., 1-1.

References

Department of the Army. Army Doctrine Publication (ADP) 3-0, *Operations.* Washington, DC: U.S. Government Publishing Office (GPO), 31 July 2019.

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

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

Department of the Army. *Army Intelligence Training Strategy 2020.* May 2020.

Department of the Army. *Army Multi-Domain Transformation, Ready to Win in Competition and Conflict, Chief of Staff Paper #1.* 16 March 2021.

Department of the Army. Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028.* Fort Eustis, VA: TRADOC, 6 December 2018.

"Joint Operating Environment." Joint Chiefs of Staff website. Accessed 14 October 2020. https://www.jcs.mil/Doctrine/Joint-Concepts/JOE/.

WO1 David McGillivary currently serves in the 1st Cavalry Division, 2nd Armored Brigade Combat Team S-2. He has 13 years of operational experience in the human intelligence (HUMINT) field, ranging from strategic collection to tactical leadership, to institutional instruction. WO1 McGillivray has served as a strategic debriefer, source operations collector, and team leader in Afghanistan, and as a HUMINT manager within a division G-2X. His military service covers nearly the full spectrum of Army HUMINT operations. He is an Advanced Operations Course–HUMINT graduate, and most recently is involved with the development of the annual interrogation proficiency test concept.

THE NEED FOR AN ADVANCED INFORMATION COLLECTION PLANNERS COURSE

by Major Ryan McGraw, Major Michael Heim,
Chief Warrant Officer 4 Dale Hunter,
and Chief Warrant Officer 3 Trent Taylor

U.S. Air Force photo by MSgt. Eric Petosky

Personnel provide command and control information at the 612th Air and Space Operations Center, supporting U.S. Southern Command, February 2010.

Confirming a High-Payoff Target

During a future conflict, human intelligence (HUMINT) reports indicate a high-payoff target (HPT) in the enemy's support zone. To confirm this report, the collection manager quickly reviews the intelligence collection matrix for available assets and identifies a signals intelligence (SIGINT)-equipped U-2 that could potentially verify the HPT. However, after reviewing the reconnaissance, surveillance, and target acquisition annex, he realizes the equipped SIGINT sensor cannot collect the target's specific radio frequency signature. He considers national SIGINT collection, but based on the sensors' locations, he realizes that between the periodicity and information dissemination time, the target will likely be gone. Finally, the collection manager considers redirecting the division MQ-1C Gray Eagle to verify the report. Although the target is inside the enemy's air defense range, the collection manager considers the air defense system's probability of kill as low risk at current altitude. He also reviews the enemy's electronic warfare order of battle and current battle damage assessment and determines the risk level is acceptable. After receiving approval from his commander, the collection manager, in coordination with G-3 current operations, directs the MQ-1C to confirm the presence of the HPT for destruction by fires.

Introduction

The vignette to the right describes a typical scenario that a collection manager will face in a future conflict against a peer or near-peer enemy. It also represents a scenario that the Army's current collection management training programs do not fully address. Although the Army hosts or has access to several information collection-related courses, these courses provide only a basic understanding of information collection doctrine and platform capabilities because they focus on either the brigade or the combatant command level, creating a gap at the echelons in between.

The Army needs a more advanced course that addresses the challenges of collection management in large-scale combat operations. While the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance (AIDP–ISR) currently meets most of these requirements, it is a yearlong program and only certifies a handful of officers and warrant officers each year. The Army needs an advanced Information Collection Planners Course (ICPC), tailored to the Army's doctrinal processes, that provides the necessary training for collection management teams at a division or higher, to request, task, and direct collection assets during large-scale combat operations.

Current Training

The Army's primary course for training collection managers is the ICPC at Fort Huachuca, Arizona. The ICPC is designed for intelligence leaders. It trains the development of information requirements, the specific application of information collection tasks, and the intelligence architecture and capabilities necessary to support information collection. Students learn to employ organic and attached intelligence collection assets at the brigade combat team (BCT). They also learn to request information and support from higher headquarters and intelligence agencies to provide the commander effective intelligence support.

The Army's other major training program is the AIDP–ISR program. It provides students the resources to attend a variety of Army, joint, and interagency intelligence courses to build expertise in intelligence disciplines, collection management, and supported staff functions such as targeting. Graduates of this program serve a 1-year utilization tour as a collection manager on a division or corps-level staff. While this program largely meets the requirements for collection management, the significant resources required limit enrollment to 14 to 16 students per year. This creates a considerable gap in training between the collection management chiefs and the rest of the collection management staff at divisions and corps. This program is also unavailable to National Guard and Reserve Soldiers, creating a significant educational gap in their formations.

In addition to ICPC and AIDP–ISR, the Army also provides a variety of other courses that are of value to collection managers, even though collection managers are not the primary training audience. These courses include the Cavalry Leaders Course, Joint Firepower Course, Digital Intelligence Systems Master Gunner Course, and other intelligence discipline-focused courses. The joint community and the Defense Intelligence Agency also offer collection management-related courses, but these courses focus on the operational and

strategic level. Although these classes are valuable, they are both intellectually disparate and geographically separate, requiring a significant investment for training collection management teams.

A Proposed Course Design

The proposed course design for an advanced ICPC covers four broad topic areas:

- ✦ Collection management and intelligence preparation of the battlefield (IPB).
- ✦ Army collection management.
- ✦ Integrating the intelligence community.
- ✦ Intelligence architecture.

An advanced ICPC would centralize these topics under one curriculum and enable instructors to tailor course material for collection management through an Army lens.

Collection Management and Intelligence Preparation of the Battlefield. This area would cover three focus areas:

- ✦ Terrain and weather impacts on collection.
- ✦ Specific information requirement (SIR) development.
- ✦ Threats to Army intelligence collection assets.

Terrain and weather impacts on collection would cover the effects of terrain on signals and on SIGINT collection; RQ-7 Shadow and MQ-1C weather limitations; and the way in which other weather, terrain, or civil considerations hinder or enhance collection capabilities.

SIR development would cover resources and information required to build SIRs from threat characteristics and threat models.[1] This covers topics such as developing an electronic order of battle, unique measurement and signature intelligence (MASINT) signatures of equipment, and resources available to help research these unique signatures.

Threats to Army intelligence collection assets would focus on the specific abilities of various air defense platforms to destroy Army intelligence collection assets, electronic warfare systems and their impacts on collection, and current adversary deception capabilities. The overall objective is to provide collection management teams with the ability to articulate opportunities for and limitations of collection during the IPB process.

Army Collection Management. This area would cover the employment of Army intelligence collection assets. Of all the Army intelligence community assets, air and ground cavalry squadrons would receive the most attention in order to help bridge the knowledge gap between collection managers and cavalry leaders.[2] This would focus on rates of march, coverage areas, and planning considerations for both air and ground cavalry squadrons. For SIGINT and HUMINT employment, classes would educate students on task organization, disposition, and employment of teams during large-scale ground combat operations. Students would learn the advantages and disadvantages of weighting teams in the close fight versus the consolidation/secure area and of centralizing control versus distributing teams. They would also learn about the effectiveness of these platforms against various targets. Training in unmanned aircraft systems would focus on airspace management through airspace control measures and fire support control measures and on risk mitigation measures for operating these platforms in contested airspace. The objective of this topic is to provide collection management teams with the knowledge to conduct collection operations management during combat.

Integrating the Intelligence Community. This area would broaden collection managers' education outside the Army through a focus on Joint Force Air Component Command (JFACC) operations, orbital mechanics for space-based

Photo by Thom Williams

Soldiers practice direction finding and triangulating signals while attending the Tactical Signals Intelligence Course at the U.S. Army Intelligence Center of Excellence at Fort Huachuca, AZ.

collection, and detailed capabilities briefs on select theater and national-level collection platforms. JFACC operations would educate students on the Air and Space Operations Center's organization and processes. Students would learn the air tasking order cycle and the role of the Air and Space Operations Center in its development. During orbital mechanics, students would learn the orbits of space-based capabilities and the way in which they affect their collection opportunities. Finally, a more in-depth capabilities brief on the common theater and national-level collection platforms would cover the sensors and processors on board these platforms and the specific signatures they collect. Overall, this topic enables collection management teams to conduct effective collection requirements management when requesting theater and national-level assets.

Intelligence Architecture. This area would cover Army and national intelligence architecture to help collection management teams understand how intelligence travels from the sensor to their command post. This topic would also cover collection management during competition. The Army intelligence architecture instruction would pull heavily from the Digital Intelligence Systems Master Gunner program and cover the sensors, processors, output, and transport layers required for providing intelligence at the tactical level. National intelligence architecture classes would expand upon this by highlighting the unique requirements for ingesting intelligence collected from theater and national-level intelligence platforms. Specifically, this topic should explain the architecture required for collection requirements and intelligence to flow between national intelligence nodes, such as the National Reconnaissance Office, Air Force Distributed Common Ground System ground stations, the 116th Military Intelligence Brigade, and tactical command posts.

Photo courtesy of Program Executive Office Intelligence, Electronic Warfare & Sensors

The Tactical Intelligence Targeting Access Node's (TITAN) modular systems mounted on a Joint Light Tactical Vehicle contribute to its deep sensing intelligence gathering capabilities.

This class should also highlight existing friction points between Army and national-level architecture and current and emerging capabilities that address them. Finally, collection management during competition would provide a brief overview of the national intelligence support plan as well as the Global Force Management Allocation Plan and its effect on intelligence, surveillance, and reconnaissance (ISR) apportionment at the strategic level. Collection management during competition would also include an overview of national repositories and other repositories that collection managers use to research existing requirements and submit new ones. Examples of national repositories are—

- Community On-Line Intelligence System for End-Users and Managers (COLISEUM).
- Collection Requirements Analysis Tool for the Enterprise (CRATE).
- Geospatial Intelligence Information Management Services (GIMS).
- National SIGINT Requirements Process (NSRP).
- Cross Domain Intelligence Release (CDIR).
- National MASINT Requirements System (NMRS).

The training objective of collection management during competition is to enable collection management teams to either leverage existing national requirements or submit new requirements to support their commander's intelligence requirements in garrison and exercises.

In addition to understanding the national to tactical architecture, this topic would cover the roles and responsibilities of collection managers in designing the output requirements of collection platforms. This would cover concepts like message formats and dissemination mechanisms. This would help ensure that the collection management architecture from sensor to shooter enables rapid information dissemination and target prosecution by minimizing the analysis required. Ensuring collection management teams conduct the proper planning and coordination can result in supporting assets generating intelligence in a structured data format that results in information passed within minutes or even seconds.

Course Implementation

In order to implement this course, we recommend replacing one or two iterations of the current ICPC calendar with the advanced ICPC. This has the added benefit of bringing advanced ICPC knowledge into the basic ICPC classroom through shared instructors. Additionally, while the advanced ICPC is designed for division and corps-level collection management teams, senior BCT-level collection managers could also benefit. We envision advanced ICPC students as staff sergeants, chief warrant officer 2s, captains who have attended the Military Intelligence Captain's Career Course, and above.

To ensure students have the required level of knowledge prior to attendance, students must either graduate from basic ICPC or complete an online prerequisite course and pretest. This ensures that students have a basic understanding of collection management doctrine and ISR capabilities before arrival and enables more advanced-level discussions. This course would last 4 weeks.

Finally, the course should leverage sister courses and their instructors in order to synchronize instruction and reduce the intellectual burden on ICPC instructors. For example, instructors from the ground and air cavalry leaders' courses could teach the cavalry squadron employment classes using virtual instruction. Additionally, the Aviation Mission Survivability Office could assist with the development of the threats to Army intelligence community platforms, and instructors from the U.S. Air Force ISR Operations Course could teach JFACC operations. Sharing this course load would require substantial coordination but would have the benefit of ensuring students receive training nested with their sister courses. In addition, the course manager position for the ICPC should receive the "3F" additional skill identifier in order to leverage the experience of AIDP–ISR warrant officer graduates when teaching this course.

Conclusion

When the Army studied its ability to conduct large-scale ground combat operations, it identified deep sensing as one of 17 capability gaps. While the Army and Military Intelligence Branch have given considerable attention to the material and organizational solutions needed to eliminate this gap, the effectiveness of its reorganizations and new technology will be lessened if not paired with equal attention on training and education. The AIDP–ISR program has taken a step in the right direction with the creation of baseline requirements for students assigned as future division and corps chiefs of collection management, but more investment is needed in other members of the collection management team. An advanced ICPC will significantly increase the ability of divisions and corps to conduct information collection during large-scale combat operations by providing well-trained collection management team members capable of rapidly and effectively directing or requesting intelligence community assets to answer their commander's priority intelligence requirement or locate HPTs.

In summary, the Army needs a course tailored for the Army's unique requirements to teach division and corps collection management teams how to win against a peer or near-peer threat during multidomain operations.

Endnotes

1. ATP 2-01, *Collection Management*, indicates that specific information requirements (SIRs) facilitate matching requirements to capabilities. This means collection managers must have an in-depth understanding of specific characteristics for each piece of enemy equipment in order to fully develop SIRs. Department of the Army, Army Techniques Publication 2-01, *Collection Management* (Washington, DC: U.S. Government Publishing Office, 17 August 2021).

2. Current best practices recommend providing a member of the cavalry squadron to help integrate the cavalry squadron into reconnaissance and security efforts. This course strives to eliminate that requirement.

MAJ Ryan McGraw is the I Corps collection manager and an Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance (AIDP–ISR) graduate. Selected previous assignments include military intelligence company commander, battalion S-2, National Training Center observer coach/trainer, and 8th Army collection manager.

MAJ Michael Heim is the 1st Armored Division Analysis and Control Element Chief. Selected previous assignments include military intelligence company commander, battalion S-2, and brigade combat team assistant S-2 with 1st Stryker Brigade Combat Team, 25th Infantry Division, and 8th Army deputy collection manager. He is a graduate of the AIDP–ISR program.

CW4 Dale Hunter is a military occupational specialty 351M (Human Intelligence Collection Technician). Selected previous assignments include all-source theater collection manager for Resolute Support, 4th Infantry Division G-2X officer in charge, and 2nd Brigade Combat Team, 1st Cavalry Division, operations management team officer in charge. He is a graduate of the AIDP–ISR program.

CW3 Trent Taylor serves as an Intelligence Collection Planners Course instructor and deputy course manager at Fort Huachuca, AZ. He is a 13-year veteran of Army geospatial intelligence (GEOINT) and a graduate of the AIDP–ISR. His assignments include 25th Infantry Division, Army GEOINT Battalion, 513th Military Intelligence Brigade-Theater, 3rd Infantry Division, and Delta Company, 304th Military Intelligence Battalion.

IGNORING THE ELEPHANTS IN THE ROOM: STRATEGIC BARRIERS TO CLIMATE CHANGE INITIATIVES

by Chief Warrant Officer 4 Charles Davis

Suzhou, China (Photo by Dai Luo)

Editor's Note: The author submitted this article to the* Military Intelligence Professional Bulletin *in November 2021, before the Russian invasion of Ukraine. The article does not address the impact of sanctions imposed by the United States and our allies.

Introduction

Regardless of your political views or beliefs on climate change, climate change does have an influence on geopolitical factors. For the intelligence professional, understanding that climate change interconnects globally with social, economic, and political security contributes to conducting informed threat assessments and decision making.

In his foreword to the 2021 *Climate Adaptation Plan*, Secretary of Defense Lloyd Austin directed the Department of Defense to "include the security implications of climate change in all our risk analyses, strategy development, and planning." He further directed that climate risk be addressed in the National Defense Strategy.[1] Lines of effort for this plan include climate-informed decision making and a trained and equipped climate-ready force. These efforts are all in line with supporting President Biden's Executive Order 1408, *Tackling the Climate Crisis at Home and Abroad*.

In September 2021, President Biden addressed the United Nations General Assembly, pledging to work with Congress to increase funding for developing nations to $11.4 billion in support of their climate change initiatives. The intent is to aid in achieving a global initiative of $100 billion per year to support climate action in vulnerable countries.

President Biden is committed to "cutting greenhouse gas emissions 50 to 52 percent below 2005 levels in 2030, reaching a 100 percent carbon pollution-free power sector by 2035 and achieving a net-zero economy by no later than 2050."[2] These are bold and aggressive measures against a global threat. However, similar to the evaluation of operational courses of action, our adversaries have a vote. Press reporting suggests China understands its contribution to the crisis and a need for change. Additionally, recent reporting indicates that Russia understands it too has no choice but to participate and do its part. However, actions by both states suggest they are likely to negate any collective progress by other countries. This article will identify those behaviors and activities that may undo a U.S. investment of $330.6 billion by the 2050 goal.

Banking and Climate Change

The United States has already limited government financing of overseas fossil fuel projects and will likely turn its attention to private sector lending. However, Chinese initiatives continue to drive coal project financing, and "four American banks—JPMorgan Chase, Wells Fargo, Citi, and Bank of America—remain the largest financiers of fossil fuel projects overall, having collectively financed more than $800 billion in such projects worldwide since 2016."[3] (See Figure 1 on the next page.)

"From 2014 to 2017, six Chinese banks participated in syndicated loans worth $143 billion for 165 energy and transportation projects in 32 [Belt and Road Initiative] BRI countries."[4] Additionally, from 2006 to 2017, China commissioned 692 gigawatts of coal-fired capacity, more than twice the amount commissioned in the rest of the world combined.[5] These activities have not gone unnoticed. Other nations' negative press and restrictive trade measures caused China's central government to begin restricting new coal plants in 2016, including restrictions on permitting in nearly every province (with exceptions for projects located in impoverished areas and for residential heat and power projects). "In 2017, the central government began suspending hundreds of coal projects, with 98 [gigawatts] GW shelved in January and 93 GW in September."[6] However, these efforts appear short-lived.

China's Appetite for Coal

The Global Energy Monitor assesses, "While [the] appetite for new coal power investments is slowing throughout most of the world, it is on the rise in China. In 2020, China

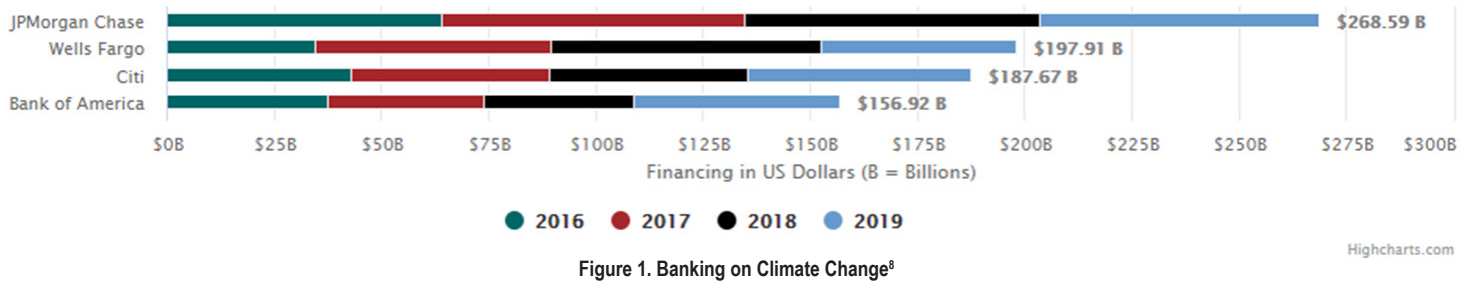


Figure 1. Banking on Climate Change[8]

built over three times as much new coal power capacity as all other countries in the world combined—the equivalent of more than one large coal plant per week. In addition, over 73 gigawatts of new coal power projects were initiated in China, five times as much as in all other countries, while construction permits for new coal projects also accelerated."[7]

While China's home use of fossil fuels is clearly on the rise, many Belt and Road Initiative projects are also tied to energy-producing coal plants. According to the Natural Resources Defense Council, Chinese financial institutions are the world's largest investor in overseas coal plants, using international development funds to create $15 billion in coal projects from 2013 to 2016. The Natural Resources Defense Council further asserts there is another $13 billion in proposed funding.[9]

Many of the coal proposals are part of the China-Pakistan Economic Corridor, a multibillion-dollar plan that includes $33 billion in energy infrastructure projects, primarily fossil fuels. In 2016, the Pakistani magazine *Centerline* reported the majority of the China-Pakistan Economic Corridor would be coal-based plants, with $5.8 billion worth of coal power projects expected to be completed by early 2019 as part of the China-Pakistan Economic Corridor's "early harvest" projects.[10] A more recent report by Greenpeace and counterparts Sierra Club and CoalSwarm indicates Asia is the leader in new coal power construction. Chinese companies and banks are involved in 240 coal-fired power projects in 25 of the 65 countries along the Belt and Road Initiative.[11] (See Figure 2 on the next page.) Most recently, in September 2021, the Pakistan Matiari-Lahore transmission line started operations. Coal-based power plants at Thar, Port Qasim, and Hub produce the electricity for this power service.[12]

Belt and Road Initiative Spending

While estimates of spending vary, Morgan Stanley anticipates that Belt and Road Initiative spending could reach $1.2 to $1.3 trillion by 2027.[13] To date, the energy and transportation sectors have been the primary focus of Belt and Road Initiative investment, with energy estimated to compose 44 percent of all Belt and Road Initiative spending.[14] This should not be surprising. China targets developing nations, and these countries tend to view fossil fuels as cheaper and as more reliable than renewables. In Bangladesh, India, and Indonesia, for instance, state development plans explicitly call for constructing new coal plants.

"Restrictions imposed by the World Bank, the Asian Development Bank, and the United States during the Obama administration have made China the world's primary source of coal financing."[15] Countries taking advantage of China's willingness to finance and construct these plants include "Bangladesh, Pakistan, Serbia, Kenya, Ghana, Malawi, and Zimbabwe. China is also financing about half of proposed new coal capacity in Egypt, Tanzania, and Zambia."[16] In order to meet renewable energy Nationally Determined Contributions for 31 of the Belt and Road Initiative countries studied, the Global Development Policy Center estimates the need for $486.62 billion by 2030.[17]

Nationally Determined Contributions

[Nationally Determined Contributions] NDCs are national climate plans that national governments aim to implement to combat climate change. NDCs typically include climate-related contributions, policies, and measures. Most NDCs include emissions-reduction commitments and have mitigation objectives for 2030 or earlier. Collectively, these country-driven contributions and objectives lay out the global path toward low-carbon development, and they are increasingly recognized by multilateral development banks and incorporated into their strategy and planning processes with client countries.[18]

"Today, China's leadership has embedded 'eco-civilization' in the Communist Party's constitution, as the clean, green principle on which it is planning the next phase of China's economic development….The result is that while China is making commendable efforts to clean up at home and to reduce its carbon emissions, the Belt and Road Initiative threatens to lock China's partners into the same high-emission development that China is now trying to exit….190 countries agreed under the Paris climate accord to try to keep the global average temperature rise below 2 degrees Celsius (C) and as close to 1.5 degrees C as possible. The energy finance think tank Carbon Tracker estimates that this will require a complete phaseout of coal worldwide by 2040. That, in turn, means that 100 [gigawatts] GW a year, or one coal plant a day, will need to close from now to 2040, a goal that is directly undercut by China's coal investments."[19]

Russia's Reliance on Fossil Fuels

China is not our only competitor that sees reliance on fossil fuels as a key to its economic stability and national objectives. Russia is certainly not a champion for change when it comes to oil and natural gas or conversions to renewable energy.

Map 1 | **Belt and Road Coal–Fired Power Projects with Chinese Involvement, by Number and Installed Capacity**

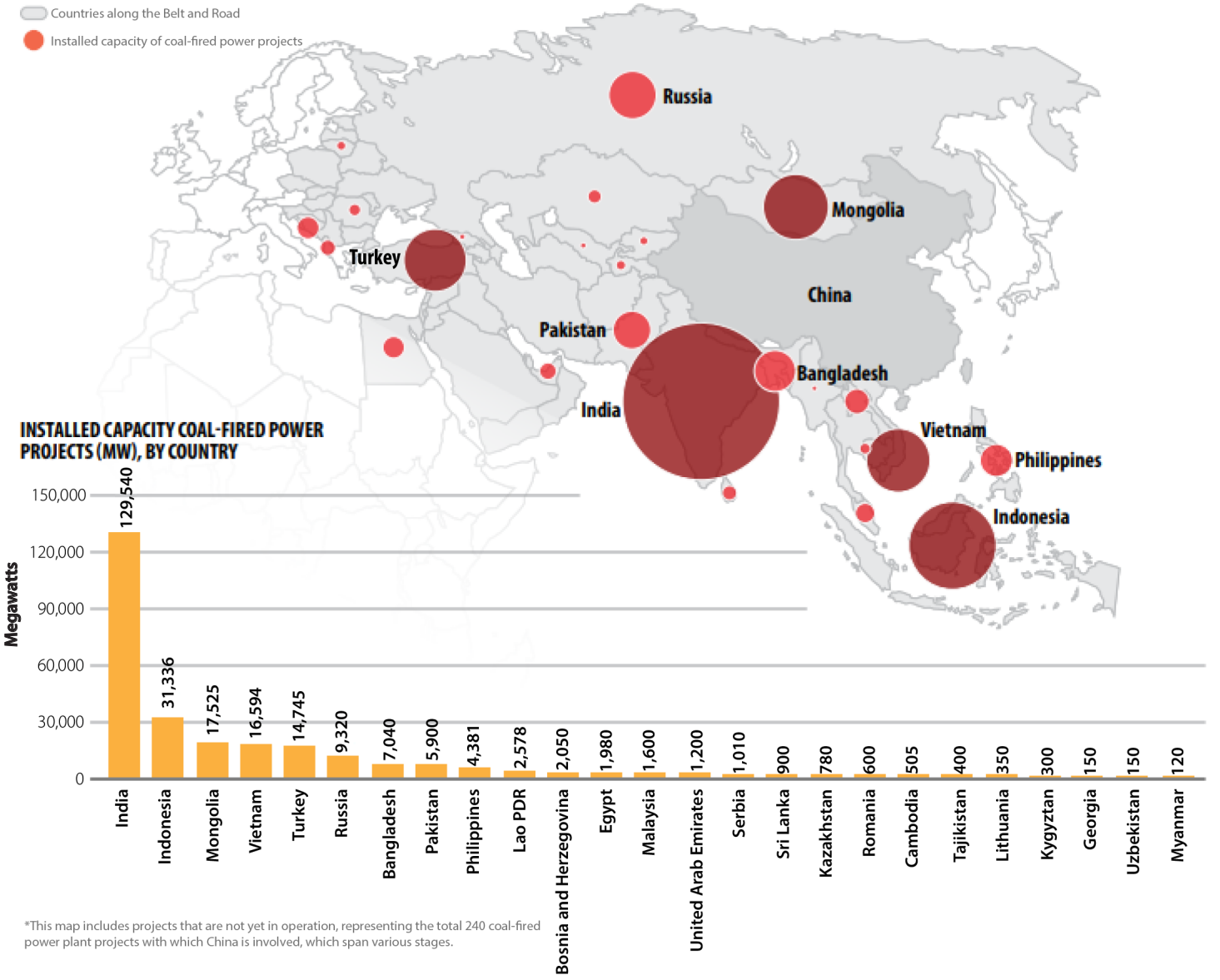


Figure 2. China's Involvement in Coal-Fired Power[21]

The Lowy Institute, an Australian-based think tank, indicates, "Russia is the world's fourth largest emitter of greenhouse gases, pumping out five percent of the world's carbon. It is also a significant source of methane emissions, often from creaky gas pipelines. Yet Russia only ratified the Paris Agreement in September 2019, four years after its conclusion. And its Nationally Determined Contribution lodged in November 2020 was a modest effort, rather devoid of ambition."[20]

Reporting from *The Moscow Times* suggests, "The Russian establishment was caught off guard by the long-term threat to the entire functioning of the country's economy posed by the global goal of decarbonization and net zero emissions. Nearly all of Russia's main foreign trade partners have declared their ambition to become carbon-neutral by 2050 (or 2060, in China's case). And the [European Union's] EU's carbon border adjustment mechanism—hotly discussed in Russia—is only a small part of the raft of EU regulations."[22]

Anatoly Chubais, the former Russian deputy prime minister, expressed concern over the considerable effects on Russian exports that green initiatives would have. Chubais said this green transition might cause a 10 percent loss in Russia's gross domestic product. Oil and gas revenues currently account for one-third of the Russian budget; as one of the world's largest energy exporters, Russia's oil and natural gas exports constitute almost 40 percent of the Russian budget.[23] Russian president Vladimir Putin is in no position to accept a 10 percent loss in gross domestic product or conduct budget cuts to the tune of 40 percent. Simply put, diversifying energy supplies away from fossil fuels poses a long-term threat to the Russian economy.

In 2019, *The Moscow Times* quoted the Russian energy minister, Alexander Novak: "Over the last 10 years, Russia has boosted its annual coal production by more than 30 percent to a total of 440 million tons, and the country is now the

world's third-largest producer."[24] In 2020, the Climate Change Performance Index ranked Russia 52nd out of 61 countries worldwide for its adoption of climate change goals. Putin has not developed a strategy or demonstrated an interest in lowering carbon levels by 2050. Furthermore, it does not appear Russia is planning to phase out fossil fuel subsidies or forgo its new coal terminals currently under construction.[25] Almost half of Russia's current 58 coal mines in operation have opened in the course of the last 20 years, and several more are in the making, including in the Arctic.[26]

> "Russia is likely to experience infrastructure damage from permafrost thaw, more frequent and intense wildfires, and increased erosion.[27]"

Russia's Energy Plans

In the Taymyr Peninsula, the large territory stretching into the far northern Kara Sea, there are plans for extractions of more than 25 million tons per year over the next 5 years. The Vostok Coal Company will begin use of its license on the northeastern tip of the peninsula. The license areas of the Severnaya Zvezda (Northern Star) company are located nearby. These projects will result in two major port terminals for coal.[28] While Russia is projected to replace much of its own coal use with natural gas, which will leave a reduced carbon footprint at home, those projections also reflect only 4 percent of the energy mix will come from renewable sources by 2035.

Russia's most powerful business lobby, the Russian Union of Industrialists and Entrepreneurs, has a different take on the crisis. David Iakobachvili, chairman of the Russian Union of Industrialists and Entrepreneurs' Committee on Corporate Social Responsibility and Sustainable Development, told *The Moscow Times*, "We have to maximize our sales of gas, oil and coal as much as we can without stopping while there is still a buyer for it, and use that money to stimulate innovations in new technologies so we can keep up with other economies."[29]

Even as countries around the world are planning green transition efforts, Russia is considering the investment of three to five scientific and industrial centers in Siberia. The idea is to provide incentives for a workforce to relocate and drive further development of the Siberian region, strengthening the Russian economy. The president of the Russian Geographical Society, Sergei Shoigu, believes that southern Siberia has the potential to produce greater quantities of cooking coal and that the Kansk region shows promise in coal chemical production.[30] Lending credibility to the proposal, Viktoria Abramchenko, one of the government's main curators of the Siberian Federal District, was in full support.[31] Putin pointedly stated that Russia's "historic task" is to increase the Far Eastern population by expanding the local industrial potential, creating new jobs and improving living standards.[32] According to a November 2021 piece by U.S.-based think tank The Jamestown Foundation, "At the annual gathering of the Valdai Club (October 18–21), [Putin] not only decried the ostensible crisis of Western capitalism but also dismissed the search for global solutions to global problems as unrealistic."[33]

Significance of the Permafrost

The head of Russia's Rosneft Oil Company, Igor Sechin, asserted energy transition plans should be discussed more closely with industry, suggesting world leaders are not the only parties that have a say.[34] Russian challenges to the green effort go on as permafrost, covering roughly two-thirds of Russia, is rapidly thawing. "More dramatic freeze-thaw cycles in the subsoil are eroding urban infrastructure in Russia's Arctic cities, home to more than 2 million people, and pose a mounting risk to Russia's 200,000 kilometers of oil and gas pipelines, not to mention thousands of miles of roads and rail lines bridging some of Russia's widest rivers."[35]

Permafrost thaw was responsible for a diesel storage tank near Norilsk toppling and spilling 21,000 tons of diesel into the Ambarnaya River and surrounding subsoil.[36] "At its current rate of thaw—about 1 degree Celsius per decade—Russia's permafrost layer will stop freezing completely in three decades….According to one study, a 30 to 99 percent reduction in near-surface permafrost would release an additional 10 to 240 billion tons of carbon and methane into the atmosphere and potentially put the globe 'over the brink' by 2100."[37]

In 2019, the United Nations' Intergovernmental Panel on Climate Change (IPCC) published a 1,000-page document titled *Special Report on the Ocean and Cryosphere in a Changing Climate*.[38] Based on the report's findings, "even if the world manages to hit the IPCC target of limiting global warming to 2 degrees Celsius by 2100, around 25 percent of the permafrost near the surface could be lost."[39] Estimates indicate these effects are irreversible. "When the bacteria turn the carbon in the Arctic into [carbon dioxide] CO2 and methane, it accelerates a feedback loop. The more methane and carbon released, the more warming [occurs]."[40] (See Figure 3.) Even facing all this research and the findings, it is unlikely Russia will cooperate willingly with what amounts to a destruction of its economy and a significant loss of influence and economic control over neighbors that provide a buffer to North Atlantic Treaty Organization (NATO) expansionism and the advance of Americans.

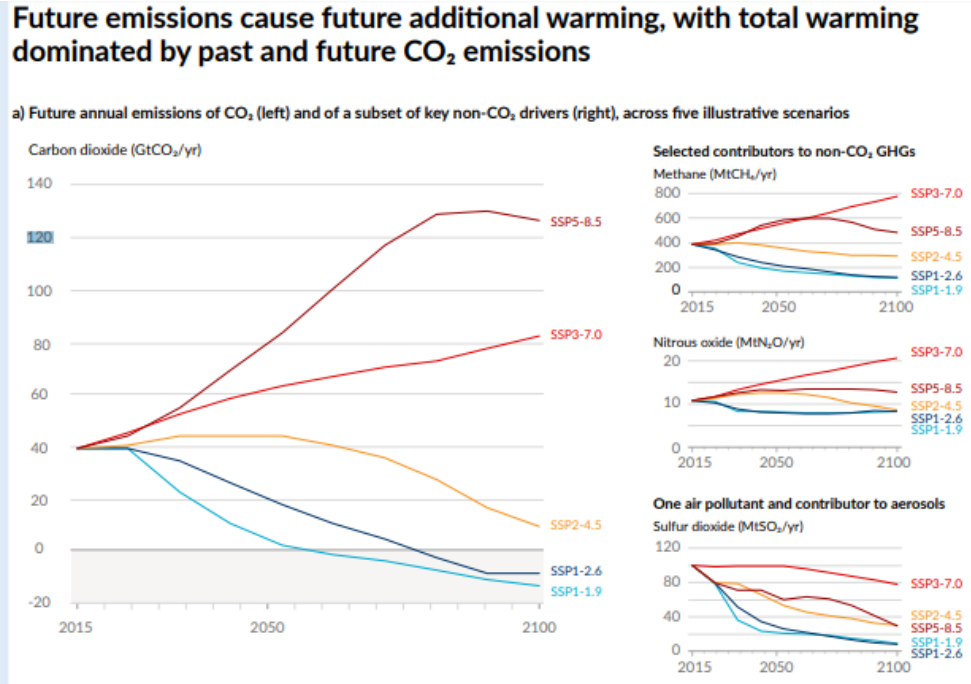


Figure 3. Future Emissions Cause Future Additional Warming[41]

Conclusion

Climate change is increasing geopolitical tensions as countries become more cognizant of the mounting environmental effects of greenhouse gas emissions. Russia considers the climate agenda to be a threat to its national security and economy as the unassailable facts surrounding permafrost thaw and carbon emissions reshape the global landscape. China has made, at least on paper, significant commitments to greening its economy and lowering carbon emissions; however, there is a degree of international skepticism about China's ability and true intention to meet its ambitious goals. In the meantime, the intensifying physical effects caused by climate change will likely lead to regional and country-level instability and conflict.

Viewing these challenges with geopolitical empathy, one might consider the risk of instability among our NATO partners and a military confrontation with a near-peer threat while facing multiple economic and political challenges by a pacing threat. The U.S. investment of national treasure is considerable, and given the loss our adversaries anticipate, we are likely to see a net-zero gain or worse at the end of this effort. Lachlan Carey, associate fellow in the Energy and Climate Change Program at the Center for Strategic and International Studies, summed it up: "It's the sort of elephant in the room.... When we look at any measure of global emissions or any scenario of how we reach the Paris targets, it relies a whole lot on China's transitioning away from its reliance on coal. So the Belt and Road, to the extent it has really significant impact on climate change and its trajectory—is the extent to which China is using it to export its capacity in the coal sector."[42] Our adversaries have a vote that we cannot ignore.

Endnotes

1. Department of Defense, Office of the Undersecretary of Defense (Acquisition and Sustainment), *Department of Defense Climate Adaptation Plan* (Washington, DC, 1 September 2021), 1, https://www.sustainability.gov/pdfs/dod-2021-cap.pdf.

2. The White House, "Fact Sheet: President Biden Renews U.S. Leadership on World Stage at U.N. Climate Conference (COP26)," November 1, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/01/fact-sheet-president-biden-renews-u-s-leadership-on-world-stage-at-u-n-climate-conference-cop26/.

3. Jennifer Hillman and Alex Tippett, "The Climate Challenge and China's Belt and Road Initiative," *Guest blog*, Council on Foreign Relations, March 31, 2021, https://www.cfr.org/blog/climate-challenge-and-chinas-belt-and-road-initiative.

4. Lihuan Zhou, Sean Gilbert, Ye Wang, Miquel Muñoz Cabré, and Kevin P. Gallagher, *Moving the Green Belt and Road Initiative: From Words to Actions* (Washington, DC: World Resources Institute, October 2018), 12, https://www.bu.edu/gdp/files/2018/11/GDP-and-WRI-BRI-MovingtheGreenbelt.pdf.

5. Adam Wentworth, "China considers imposing tough clean air standards across 80 cities," Climate Action, 29 June 2018, https://www.climateaction.org/news/china-considers-imposing-tough-clean-air-standards-across-80-cities.

6. Christine Shearer, Neha Mathew-Shah, Lauri Myllyvirta, Aiqun Yu, and Ted Nace, *Boom and Bust 2018: Tracking the Global Coal Plant Pipeline* (EndCoal, March 2018), 9, https://endcoal.org/wp-content/uploads/2018/03/BoomAndBust_2018_r4.pdf.

7. Global Energy Monitor and Centre for Research on Energy and Clean Air, *China Dominates 2020 Coal Plant Development* (February 2021), 1, https://globalenergymonitor.org/wp-content/uploads/2021/02/China-Dominates-2020-Coal-Development.pdf.

8. "Explore the Data," Banking on Climate Chaos, accessed 29 November 2021, https://www.bankingonclimatechaos.org/bankingonclimatechange2020/.

9. Huileng Tan, "China is massively betting on coal outside its borders—even as investment falls globally," CNBC, April 6, 2018, https://www.cnbc.com/2018/04/06/china-is-massively-betting-on-coal-outside-its-shores--even-as-investment-falls-globally.html.

10. Sabahat Ali, "China, Pakistan Economic Corridor: salients and importance," *Centreline*, October 11, 2016, https://centreline.com.pk/2016/10/11/china-pakistan-sabahat-ali/. The term "early harvest" was coined for projects that are likely to be completed in the next few years as opposed to longer-term ones. "CPEC projects have entered early harvest stage," *Express Tribune*, August 11, 2017, https://tribune.com.pk/story/1478687/cpec-projects-entered-early-harvest-stage-sun-weidong.

11. Ren Peng, Liu Chang, and Zhang Liwen, *China's Involvement in Coal-Fired Power Projects along the Belt and Road* (Beijing: Global Environmental Institute, May 2017), 1, http://www.geichina.org/_upload/file/report/China%27s_Involvement_in_Coal-fired_Power_Projects_OBOR_EN.pdf.

12. "PM Khan inaugurates Matiari-Lahore power transmission line," MM News, September 30, 2021, https://mmnews.tv/pm-khan-inaugurates-matiari-lahore-power-transmission-line/.

13. Hillman and Tippett, "The Climate Challenge."

14. Zhou et al., *Moving the Green*.

15. Hillman and Tippett, "The Climate Challenge."

16. Isabel Hilton, "How China's Big Overseas Initiative Threatens Global Climate Progress," Yale Environment 360, January 3, 2019, https://e360.yale.edu/features/how-chinas-big-overseas-initiative-threatens-climate-progress.

17. Zhou et al., *Moving the Green*, 37.

18. Ibid., 20.

19. Hilton, "How China's Big Overseas Initiative."

20. Ian Hill, "Is Russia finally getting serious on climate change?" The Interpreter, 1 November 2021, https://www.lowyinstitute.org/the-interpreter/russia-finally-getting-serious-climate-change.

21. Ren, Liu, and Zhang, *China's Involvement*, 1.

22. Tatiana Mitrova, "Is Russia Finally Ready to Tackle Climate Change?" *Moscow Times*, September 7, 2021, https://www.themoscowtimes.com/2021/07/28/is-russia-finally-ready-to-tackle-climate-change-a74639.

23. Emre Gürkan Abay, "Shift to clean energy may adversely affect Russian economy, its ties with EU," Anadolu Agency, 8 October 2021, https://www.aa.com.tr/en/economy/shift-to-clean-energy-may-adversely-affect-russian-economy-its-ties-with-eu/2386225.

24. Atle Staalesen, "Gloom in horizon as Russia announces it will boost digging of coal," *Barents Observer*, August 23, 2019, https://thebarentsobserver.com/en/2019/08/gloom-horizon-russia-announces-it-will-surge-digging-coal.

25. Jan Burck, Ursula Hagen, Niklas Höhne, Leonardo Nascimento, and Christoph Bals, *Climate Change Performance Index, Results 2020* (Bonn: Germanwatch, NewClimate Institute, and Climate Action Network, 2020), 22–23, https://ccpi.org/wp-content/uploads/ccpi-2020-results-the_climate_change_performance_index-1.pdf.

26. Staalesen, "Gloom in horizon."

27. National Intelligence Council, Office of the Director of National Intelligence, *National Intelligence Estimate: Climate Change and International Responses Increasing Challenges to US National Security Through 2040* (Washington, DC, October 21, 2021), 15, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2253-national-intelligence-estimate-on-climate-change.

28. Staalesen, "Gloom in horizon."

29. Evan Gershkovich, "How Does a Powerful Russian Lobby Plan to Halt Climate Change? With Coal, Oil and Gas," *Moscow Times*, September 7, 2021, https://www.themoscowtimes.com/2019/11/15/how-does-a-powerful-russian-lobby-plan-to-halt-climate-change-with-coal-oil-and-gas-a68173.

30. "Shoigu named places for the construction of new cities in Siberia," RBC, 6 September, https://www.rbc.ru/politics/06/09/2021/6131fa0f9a7947199b6163d1#.

31. "Putin called the growth of the population in the Far East a historical task," TASS, 2 September 2021, https://tass.ru/obschestvo/12284963.

32. Ibid.

33. Pavel K. Baev, "Spurning Pair of International Summits, Putin Denounces Globalization," *Eurasia Daily Monitor* 18, no. 165 (November 1, 2021), https://jamestown.org/program/spurning-pair-of-international-summits-putin-denounces-globalization/.

34. "Green Crossing over the Alps," *Kommersant*, 28 October 2021, https://www.kommersant.ru/doc/5052761.

35. Heather A. Conley and Cyrus Newlin, "Climate Change Will Reshape Russia," Center for Strategic and International Studies, January 13, 2021, https://www.csis.org/analysis/climate-change-will-reshape-russia.

36. "Norilsk Nickel: Mining firm pays record $2bn fine over Arctic oil spill," BBC News, 10 March 2021, https://www.bbc.com/news/world-europe-56350953.

37. Conley and Newlin, "Climate Change."

38. United Nations Intergovernmental Panel on Climate Change, *Special Report on the Ocean and Cryosphere in a Changing Climate* (2019), https://www.ipcc.ch/srocc/chapter/technical-summary/.

39. Brian Resnick, "Melting permafrost in the Arctic is unlocking diseases and warping the landscape," Vox Media, November 15, 2019, https://www.vox.com/2017/9/6/16062174/permafrost-melting.

40. Resnick, "Melting permafrost in the Arctic."

41. Working Group I Technical Support Unit, *Climate Change 2021, The Physical Science Basis, Summary for Policymakers* (Geneva: Intergovernmental Panel on Climate Change, 2021), 13, https://www.ipcc.ch/report/ar6/wg1/downloads/report/IPCC_AR6_WGI_SPM_final.pdf.

42. Jan Ellen Spiegel, "The potential climate consequences of China's Belt and Roads Initiative," Yale Climate Connections, February 17, 2020, https://yaleclimateconnections.org/2020/02/the-potential-climate-consequences-of-chinas-belt-and-roads-initiative/.

CW4 Charles Davis serves on the faculty of the Warrant Officer Career College. He currently instructs international strategic studies at all levels of warrant officer education. CW4 Davis is a graduate of the U.S. Army War College Strategic Broadening Program and holds a master's degree with honors in intelligence studies from American Military University. CW4 Davis is also a recipient of the Military Intelligence Corps Knowlton Award.

Chinese Emerging Technological Convergence: Enabling Intelligent Warfare with Artificial Intelligence

by Chief Warrant Officer 5 Jason A. Kinsey

China's Emerging Technology Ambition

During his confirmation hearing in 2021, Secretary of Defense Lloyd Austin stated, "China is ascending. Russia is also a threat…but China is the pacing threat."[1] Aside from focusing on countering United States interests in the region, China has identified strategic goals to complete the modernization of national defense and the military by 2035, as outlined in its most recent defense strategy, *China's National Defense in the New Era*. The convergence of technologies like artificial intelligence, big data, the Internet of Things, and unmanned weaponry serves as an evolution for the People's Liberation Army (PLA) modernization effort to *intelligentization*, or intelligent warfare.[2]

Intelligentization

Intelligentization is the uniquely Chinese concept of applying [artificial intelligence's] AI's machine speed and processing power to military planning, operational command, and decision support….The PLA's agenda for intelligentization may prove quite expansive, extending across all concepts in which AI might have military relevance in enabling and enhancing war-fighting capabilities, from logistics to early warning and intelligence, military wargaming, and command decision-making.[3]

U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-92, *The Operational Environment and the Changing Character of Warfare*, linked China's ascension to the continued advancement of emerging and disruptive technologies in the next 10 to 15 years.[4] The ability to conduct intelligent warfare and achieve a decisive strategic and tactical advantage in all-domain operations will require the technological convergence of artificial intelligence and next-generation communications. These technology enablers will foster a robust military Internet of Things to facilitate the data management required for autonomous decision making and intelligent weaponry. China's ability to achieve technological superiority by 2035 or sooner will give the PLA the ability to undermine United States deterrence efforts regionally and permit China to limit United States influence globally.

In a 2020 Department of Defense report to Congress, PLA strategists believe that "victory in future warfare…will depend upon which side can more quickly and effectively observe, orient, decide, and act [OODA] in an increasingly dynamic operating environment."[5] This belief will fuel the PLA's artificial intelligence efforts to develop sophisticated machine learning and deep learning algorithms for deployment in autonomous command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems, enhancing awareness in an increasingly complex operating environment. Additionally, these algorithms will simultaneously endow PLA platforms to degrade and deny an adversary's capabilities, complicating their OODA loop and increasing destructive course-of-action employment.

The Difference between Deep Learning and Machine Learning

Deep learning is a subset of machine learning. Machine learning is about computers being able to think and act with less human intervention; deep learning is about computers learning to think using structures modeled on the human brain. Machine learning requires less computing power; deep learning typically needs less ongoing human intervention. Deep learning can analyze images, videos, and unstructured data in ways machine learning can't easily do.

While basic machine learning models do become progressively better at whatever their function is, they still need some guidance. If an artificial intelligence algorithm returns an inaccurate prediction, then an engineer has to step in and make adjustments. With a deep learning model, an algorithm can determine on its own if a prediction is accurate or not through its own neural network.[6]

Following the victory of Google's AlphaGo, a deep neural network consisting of supervised and reinforcement learning algorithms, at the Go human world championship in 2016, PLA strategists recognized the potential for intelligentization to surpass human command decision making.[7] The China State Council followed up in 2017 with the release of an aspirational document titled *New Generation Artificial Intelligence Development Plan*, establishing the framework to become the global leader in artificial intelligence by 2030.[8] The plan highlighted many of China's efforts to advance artificial intelligence technologies, including voice and facial recognition, autonomous learning, swarm intelligence, robotics, and unmanned systems.[9] While identifying components necessary for intelligent warfare, the document also promoted

the importance of military-civil fusion to stimulate artificial intelligence innovation in the name of national security and an intelligentized PLA.[10] Chinese president Xi Jinping later nationalized military-civil fusion efforts, anticipating that top-down policies and state-owned enterprises will afford China an innovation advantage in the emerging technology sector and enable intelligent warfare.[11]

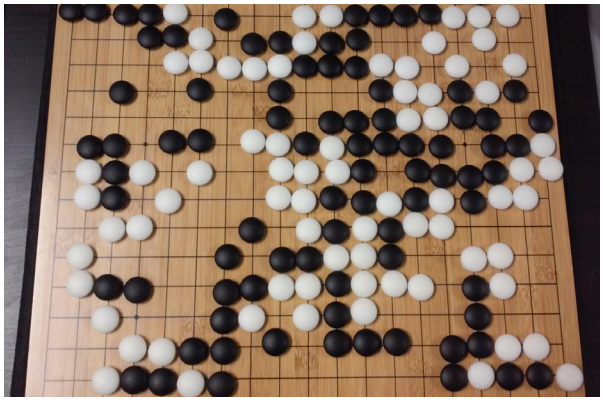
The Artificial Intelligence Lifeline

Just as information is crucial for multi-echelon decision making, the successful employment of artificial intelligence for intelligent warfare requires the accumulation and integration of information across all operational domains, marking the need for effective data management analytics. In recent years, strategists and PLA officers have written countless articles in official Chinese journals and publications, spotlighting the importance of data management in support of intelligent warfare, likening data to combat power and the blood of intelligent warfare.[13] PLA writings go on to describe the necessity for data management in support of command decision making, calling for data mining and deep learning algorithms to autonomously learn from the multifaceted data streams ingested from sensors and systems across the multidomain battlespace.[14]

With state-sponsored initiatives and strategies like military-civil fusion, the PLA is actively exploring ways to integrate and disseminate the blood of intelligent warfare for improved situational awareness across echelons and supporting targeting for precision strike capabilities.[15] Army Futures Command has a similar effort, Project Convergence, to use artificial intelligence and autonomous systems to link multidomain sensors and shooters to neutralize enemy ISR and long-range fires.[16] For these efforts to be successful, data-hungry artificial intelligence algorithms require a sophisticated communications infrastructure to foster collaboration between a sensor-rich environment of manned and unmanned C4ISR platforms providing critical information to accommodate decision making and targeting.

AlphaGo

The game of Go, which originated in China more than 2,500 years ago, is an abstract war simulation. Players start with a completely blank board and place black and white stones, one at a time, to surround territory. Once placed, stones do not move, and they're removed only if they're "killed"—that is, surrounded completely by the opponent's stones…Because there are so many directions any given game can move in, Go is a notoriously difficult game for computers to play. In 2016, the Google-owned artificial intelligence company DeepMind shocked the world by defeating South Korean Go champion Lee Se-dol four matches to one with its AlphaGo AI system.[12]



5G: Emerging Technology Enabled by Next-Generation Communications

Ongoing deployment of the fifth-generation (5G) infrastructure provides the foundation for enabling the data-rich military Internet of Things. 5G aims to deliver higher speeds (up to 100 times faster than fourth generation) and lower latency (within 1 millisecond) communications and enhance massive machine-to-machine communications.[17] Aside from speed, radio frequency (RF) agility or RF spectrum management sets 5G apart from legacy generations, allowing data optimization for reliable, instantaneous, and abundant device and sensor connectivity. To accomplish this, 5G will rely on several innovations like millimeter-wave transmissions, small cell base stations, massive multiple-input and multiple-output antennas, and beamforming.[18]

Millimeter wave, a novel feature of 5G, allows for expansion of the RF spectrum for wireless devices to the 24 to 39 gigahertz (GHz) range, creating RF agility.[19] Essentially, 5G will operate in two groups: below 6 GHz, which existing wireless mobile communications use, and millimeter wave, depending on the network conditions, requirements, and device capabilities.[20] Artificial intelligence innovations supporting big data analytics, cloud, and edge computing, millions of small cell base station deployments, massive multiple-input and multiple-output antennas, and beamforming enhancements provide 5G dual-use opportunities. With military-civil fusion, Chinese engineers can develop 5G-capable intelligentized military platforms interoperable with legacy communications infrastructure yet able to adjust to a complex operating environment.

The 2020 United States–China Economic and Security Review Commission's Annual Report to Congress highlighted China's ambitious 5G plan. The commission noted China relies on a "cluster of revolutionary new technologies," including artificial intelligence, robotics, interconnected sensors, and 5G, to surpass the United States economically and militarily.[21] Backing that initiative, the People's Republic of China unveiled a state-sponsored "new infrastructure" investment strategy totaling $1.4 trillion on 5G architecture, artificial intelligence initiatives, and other telecommunication efforts to benefit defense and commercial industries.[22] Designed to fortify China's goal of reducing foreign dependence on technology and gaining a first-mover advantage in 5G, the funding enables innovations in autonomous unmanned systems and other dual-use technologies.[23] With more than 200 million 5G users, 144 million 5G devices, and 700,000 base stations deployed in China, there are projections for another 600,000

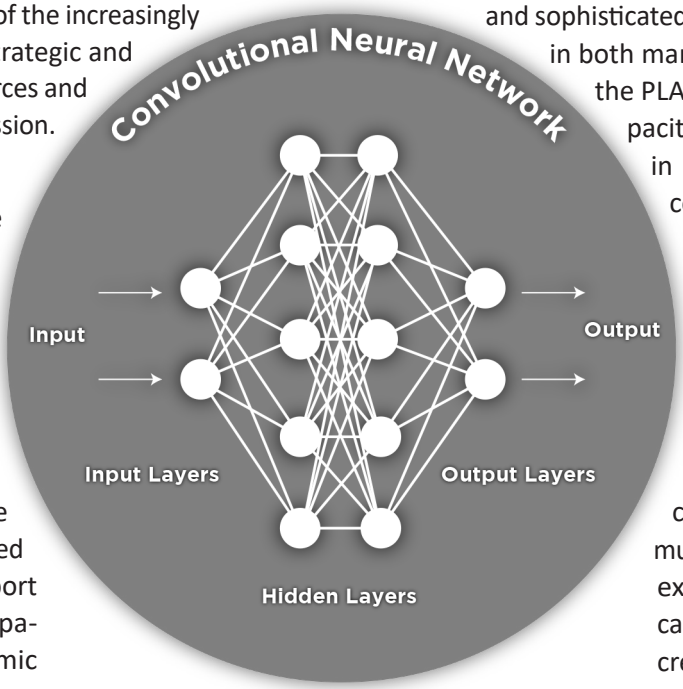
base stations in 2021.[24] These numbers represent commercial 5G deployments, yet as previously mentioned, Chinese military-civil fusion mandates that emerging technologies like 5G also be developed for dual-use military applications.[25]

Chinese military strategists and scientists have also labeled 5G as vital to enhancing C4ISR by increasing machine-to-machine connectivity between sensors while also facilitating human-machine interaction in a complex operating environment.[26] The PLA is unlikely to incorporate commercial 5G standards for military use. Rather, the PLA will leverage the favorable commercial aspects of 5G and subsequent generations for implementation into military applications. China's extensive involvement in the development of next-generation communications standards, combined with military-civil fusion efforts, provides an advantage over the United States.

While no evidence suggests China has successfully fielded an intelligentized weapon system, the conditions are optimal for the PLA to achieve intelligentization before the United States forces. China's technological convergence of artificial intelligence and next-generation communications will aid the ubiquitous fielding of unmanned C4ISR and weapon systems. This will foster a military Internet of Things ecosystem to fulfill accelerated command decision making and targeting by amplifying situational awareness of the increasingly complex battlespace, posing a strategic and tactical threat to United States forces and our ability to deter Chinese aggression.

PLA Intelligentization

Strategically, the convergence of artificial intelligence and next-generation communications provides China with opportunities to better understand United States capabilities and subsequent vulnerabilities. Motivated by the successes of AlphaGo-like artificial intelligence systems and reliant on sophisticated deep learning algorithms to support wargaming and analysis-like capabilities, China can use algorithmic warfare to compete against and potentially outwit United States strategic options. The data bloodlines are already flowing through China with 5G, helping to feed the data-hungry algorithms to foster learning. As China looks to proliferate Chinese-developed 5G technology across the globe as part of the Belt and Road Initiative, an ever-increasing stream of varied data will facilitate artificial intelligence expansion and provide access to a significant portion of the world's data. United States efforts to build partnerships with other nations might serve as a double-edged sword if those nations are also heavily reliant on Chinese telecommunications infrastructure. United States partners may unknowingly enable China to harvest and militarize data for malign influence and intelligent warfare purposes.



A specialized type of artificial Intelligence algorithm that imitates human vision. It can be used for applications involving facial recognition, image analyis, and change detection.[27] (Graphic by MIPB Staff)

With such large datasets made accessible as part of next-generation communications, Chinese artificial intelligence algorithms can develop at a much greater pace and, using military-civil fusion, enable integration into the military Internet of Things ecosystem more rapidly to support intelligent warfare efforts. Tactically, the employment of artificial intelligence in PLA weapon systems and C4ISR can aid in the analytic efforts necessary for targeting U.S. and allied forces. The targeting process is extraordinarily complex and requires a multilayered integration of data to understand the system capabilities of friendly weapon systems and a simultaneous vulnerability analysis of adversary systems to achieve the appropriate effect against a target. In multidomain large-scale combat operations, time is of the essence, requiring nearly instantaneous target identification and analysis of an appropriate effects solution to achieve the commander's objectives. Reliant on next-generation communications infrastructure and sophisticated artificial intelligence algorithms in both manned and unmanned platforms, the PLA will have the capability and capacity to quickly seize the initiative in large-scale combat operations, complicating or even preventing U.S. objectives.

While next-generation communications will enable greater connectivity for machine-to-machine communications, thereby vastly increasing the potential targets for intelligence collection, next-generation communications will present access and exploitation limitations to tactical collection capabilities. This will create a heavy reliance on theater and national intelligence collection capabilities, with an enhanced focus on collecting and targeting the crucial data links providing the connectivity for a PLA military Internet of Things. With greater numbers of connected devices in intelligence warfare, cyberspace will continue to be an increasingly important domain during artificial intelligence-accelerated competition and conflict, providing unique access and opportunities to achieve effects against artificial intelligence-enabled systems.

Photos courtesy of U.S. Air Force

Swarm intelligence or swarm combat offers insight into how the convergence of artificial intelligence and next-generation communications can facilitate tactical intelligent warfare. The TRADOC journal *OE Watch* published an excerpt from the PLA's official publication, *Jiefangjun Bao*, highlighting how the PLA might use massive numbers of unmanned drones for swarming operations, relying on collaboration by networked autonomous systems against an adversary. The drones would either simply overwhelm enemy capabilities through sheer numbers or assign roles to each drone, such as offensive, defensive, or ISR, depending on the mission requirements.[28] Another described method was "mother ship-launched" operations, whereby a centralized manned or unmanned platform serves as the command and control and mobilization effort for multidomain unmanned systems, providing a long-range and versatile coordination capability across multiple locations, and effectively conducting offensive rather than defensive maneuvers.[29]

Countering Chinese Technological Convergence

The question becomes how to counter Chinese artificial intelligence and next-generation communications convergence efforts. At the highest levels, the United States must employ a national strategy using all instruments of power to develop partnerships, incentivize, and build relations with Pacific nations. A whole-of-government effort is necessary to counter Chinese influence in the region and mitigate the expansion of Chinese next-generation communications infrastructure in partner nations to reduce the risk of data used for nefarious purposes. Domestically, the need exists for a greater emphasis on developing indigenous artificial intelligence algorithms to support U.S. military requirements. This requires a combination of military-civil fusion efforts with industry and academia to generate the knowledge and skills necessary in artificial intelligence-related fields like software engineering and data science.

In concert with efforts to integrate data science into the intelligence warfighting function, the Army has implemented initiatives to build literacy in data science and artificial intelligence.[30] One such program is the Army Futures Command "Software Factory," focused on teaching "Soldiers and Civilians how to solve Army problems with cloud technology and modern software, and to better prepare Soldiers for disconnected warfare in 2028 and beyond."[31] These skill-building initiatives scaled to the joint force and combined with insider knowledge of U.S. capabilities, doctrine, and systems will be crucial to integrating artificial intelligence algorithms dynamically to adapt to adversary capabilities in near real time. These efforts, combined with other whole-of-government initiatives, are necessary to counter Chinese artificial intelligence and next-generation communications-enabled threats and win the technology competition through 2035. Failure to act will allow China to realize technological convergence and attain overmatch against United States and allied forces in future multidomain large-scale combat operations.

Endnotes

1. Mallory Shelbourne, "SECDEF Nominee Austin Confirms Threat from China, Will 'Update' National Defense Strategy," USNI News, 19 January 2021, https://news.usni.org/2021/01/19/secdef-nominee-austin-affirms-threat-from-china-will-update-national-defense-strategy.

2. Andrew S. Erickson, "Full Text of 2019 Defense White Paper: 'China's National Defense in the New Era' (English and Chinese Versions)," Andrew Erickson (website), 24 July 2019, https://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions.

3. "199. 'Intelligentization' and a Chinese Vision of Future War," *Mad Scientist Laboratory blog*, U.S. Army Training and Doctrine Command (website), December 19, 2019, https://madsciblog.tradoc.army.mil/199-intelligentization-and-a-chinese-vision-of-future-war/.

4. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-92, *The Operational Environment and the Changing Character of Warfare* (Fort Eustis, VA: TRADOC, 7 October 2019), 13–15.

5. Office of the Secretary of Defense, *Military and Security Developments Involving the People's Republic of China 2020, Annual Report to Congress* (Washington, DC, 2020), 161.

6. Brett Grossfeld, "Deep learning vs. machine learning: a simple way to learn the difference," *Zendesk blog*, Zendesk, January 23, 2020 (updated November 22, 2021), https://www.zendesk.com/blog/machine-learning-and-deep-learning/; and Michael Middleton, "Deep Learning vs. Machine Learning—What's the Difference?" Flatiron School, February 8, 2021, https://flatironschool.com/blog/deep-learning-vs-machine-learning.

7. Elsa Kania, "AlphaGo and Beyond: The Chinese Military Looks to Future 'Intelligentized' Warfare," Lawfare, June 5, 2017, https://www.lawfareblog.com/alphago-and-beyond-chinese-military-looks-future-intelligentized-warfare.

8. Graham Webster, Rogier Creemers, Paul Triolo, and Elsa Kania, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' [2017]," *Cybersecurity Initiative* (blog), New America, August 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017.

9. Ibid.

10. Ibid.

11. Elsa B. Kania and Lorand Laskai, "Myths and Realities of China's Military-Civil Fusion Strategy," Center for a New American Security, January 28, 2021, https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy.

12. Christopher Moyer, "How Google's AlphaGo Beat a Go World Champion," *The Atlantic*, March 28, 2016, https://www.theatlantic.com/technology/archive/2016/03/the-invisible-opponent/475611/; and James Vincent, "Former Go champion beaten by DeepMind retires after declaring AI invincible," The Verge, November 27, 2019, https://www.theverge.com/2019/11/27/20985260/ai-go-alphago-lee-se-dol-retired-deepmind-defeat.

13. Timothy Thomas, *The Chinese Way of War: How Has it Changed?* (McLean, VA: MITRE Corporation, June 2020), 35–37, https://community.apan.org/cfs-file/__key/docpreview-s/00-00-16-68-30/20200611-China-Way-of-War-_2800_Timothy-Thomas_2900_.pdf.

14. Ibid., 32–34.

15. Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad Burke, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf.

16. Todd South, "New in 2021: The Army's Project Convergence scales up," *Army Times*, January 4, 2021, https://www.armytimes.com/news/your-army/2021/01/04/new-in-2021-the-armys-project-convergence-scales-up.

17. Elsa B. Kania, "Securing our 5G Future," Center for a New American Security, November 7, 2019, https://www.cnas.org/publications/reports/securing-our-5g-future.

18. Amy Nordrum and Kristen Clark, "Everything You Need to Know About 5G," IEEE Spectrum, 27 January 2017, https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g.

19. Ibid.

20. Ibid.

21. United States–China Economic and Security Review Commission, *2020 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC, 2020), 51, https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf.

22. Ibid., 212.

23. Ibid.

24. Robert Clark, "China 5G still immature, says think tank," Light Reading, January 7, 2021, https://www.lightreading.com/asia/china-5g-still-immature-says-think-tank/d/d-id/766457.

25. Kania and Laskai, "Myths and Realities."

26. Elsa B. Kania, " 'AI Weapons' in China's military innovation," *Brookings Institution*, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania.pdf.

27. Avijeet Biswal, "Convolutional Neural Network Tutorial," AI & Machine Learning, Simplilearn, last updated February 21, 2022, https://www.simplilearn.com/tutorials/deep-learning-tutorial/convolutional-neural-network.

28. Cindy Hurst, "China: 'New Concepts' in Unmanned Combat," *OE Watch* 10, no. 10 (October 2020): 37–38.

29. Ibid.

30. Jason Boslaugh and Zachary Kendrick, "The Application of Data Science in the Intelligence Warfighting Function," *Military Intelligence Professional Bulletin* 45, no. 4 (October–December 2019): 57–63.

31. Army Futures Command, "AFC Announces 'Software Factory' in Austin," Army.mil, July 14, 2020, https://www.army.mil/article/237265/afc_announces_software_factory_in_austin.

CW5 Jason Kinsey serves as the 352S, Signals Collection Technician, Warrant Officer Basic Course manager/instructor with the 304th Military Intelligence (MI) Battalion at Fort Huachuca, AZ. He was previously assigned to the 706th MI Group at Fort Gordon, GA, where he served as a division chief for the Emerging and Anticipatory Technologies office at the National Security Agency/Central Security Service Georgia. He has over 20 years of signals intelligence experience at a variety of assignments in the continental United States and overseas and holds a master of science in strategic intelligence from the National Intelligence University.

GRAPHIC INTELLIGENCE SUMMARIES: 5 PRINCIPLES FOR CLEAR, CONCISE, AND RELEVANT PRODUCTION

by Chief Warrant Officer 2 Andrew L. Chadwick, Ph.D.

Introduction

This article describes five principles that will help produce readable, analytically rigorous, and mission-relevant graphic intelligence summaries (GRINTSUMs). These principles are most relevant to Army all-source professionals who work in the analysis and control elements (ACEs) of a division or a corps that produce operational and strategic-level intelligence during the competition phase of conflict. During this phase, analysts generally have the time, resources, and connectivity to invest in creating detailed and analytically rigorous GRINTSUMs, whereas during the high operational tempo of large-scale combat operations, especially in tactical units, there is a demand for brevity and ease of transmissibility—features the standard GRINTSUM often lacks. Nevertheless, these five principles apply to many situations, such as a rotation to the Middle East or a deployment with a joint task force in a combat zone.

What is a GRINTSUM?

A GRINTSUM is an essential intelligence product that an intelligence staff uses to provide its unit with timely updates, usually daily, of key developments within an area of responsibility. Such information enables the commander and staff to make informed plans and judgments. Unlike the intelligence summary (INTSUM), the GRINTSUM displays these updates in graphical form using a combination of text overlaid or adjacent to maps, tables, operational graphics, storyboards, and other visualizations. Analysts and their customers often prefer the GRINTSUM to the INTSUM because of its ability to convey complex information visually. The incorporation of effective visual information is also one of the nine analytic tradecraft standards that the Office of the Director of National Intelligence established in ICD 203, *Analytic Standards*.[1]

Despite the GRINTSUM's importance and ubiquity, Army doctrine provides only generalized guidance on this particular intelligence product. What doctrine does provide has a tactical focus and does not address a GRINTSUM's different requirements in a competition environment dealing with operational and strategic-level concerns. For instance, the latest version of ATP 2-33.4, *Intelligence Analysis*, has a brief overview of a GRINTSUM's content; it includes a weather forecast and effects chart, situation template, rollup of reporting across all the intelligence disciplines, intelligence collection synchronization matrix, and list of current priority intelligence requirements (PIRs).[2]

The Five Principles

The following five principles aim to help fill the gap in doctrine with regard to GRINTSUMs:

- Mission relevance.
- Analytic rigor.
- Readability.
- Article types.
- Analytical responsibilities.

Principle 1: Mission Relevance

A GRINTSUM's content must be mission-relevant in that the information should directly relate to the unit's PIRs and current or anticipated decision points. GRINTSUMs that do not focus on PIRs and decision points risk becoming irrelevant because commanders and staff can simply ignore them with little to no consequence to mission accomplishment. The incentive to ignore the GRINTSUM is high among senior leaders because of their busy schedules and competing priorities. In short, an intelligence staff must battle for their customers' attention by ensuring a GRINTSUM's content directly ties to the PIRs and decision points.

To keep a customer's attention, an intelligence staff must also ensure the GRINTSUM is in the customer's preferred format. Some commanders want the GRINTSUM displayed on slides, whereas others prefer it in a text document with graphics. The best way to determine the preferred format is simply to ask the customer. Another way is to observe which products capture the customer's attention and which fall by the wayside during exercises and deployments.

It is tempting to focus the GRINTSUM entirely on the commander's needs, but it is important to keep in mind the needs of at least four other important audiences: other staff sections, subordinate units, adjacent units, and higher headquarters. These audiences will often require more specialized and detailed information. For instance, a downtrace

S-2 section may need detailed sourcing for information in the GRINTSUM, while collection managers—assuming the mission has a collection element to it—or others will require specifics on collection activities.

To meet these competing requirements and not overload the GRINTSUM, intelligence staffs can include highly technical details in another attachment, or they can simply place this information at the end of the product. They should also make sure any piece of specialized information, such as still frames of full motion video feeds, includes assessments or comments to provide context and to explain their relevance to PIRs and decision points.

Finally, units must ensure their GRINTSUMs include information that is relevant to their levels of command and span of influence. For example, an infantry battalion conducting force protection at a specific site should focus production on information that could directly affect its mission, rather than on larger strategic or peripheral items that may have little to no relevance to current and anticipated tasks. Instead, such information should fall under the purview of its higher headquarters or adjacent units. Additionally, if one's leadership wants that strategic or peripheral information, then the intelligence staff should pull GRINTSUMs or products produced by theater intelligence brigades, combatant command J-2s, or national-level agencies. Too often intelligence staffs chase the same stories while losing sight of their actual missions in the process.

Principle 2: Analytic Rigor

Perhaps the most difficult challenge regarding the Army GRINTSUM is ensuring it adheres to the nine analytic tradecraft standards in ICD 203. ATP 2-33.4 also incorporates these standards.[3]

- Properly describe the quality and credibility of all underlying sources, information, and methodologies.
- Properly express and explain uncertainties associated with major analytical judgments.
- Properly distinguish between underlying intelligence information and analysts' assumptions and judgments.
- Incorporate analysis of alternatives.
- Demonstrate customer relevance and address implications.
- Use clear and logical argumentation.
- Explain change to or consistency of analytical judgments.
- Make accurate judgments and assessments.
- Incorporate effective visual information where appropriate.

Most of the standards are relatively self-explanatory. Some, like "incorporate analysis of alternatives," are difficult to display in the GRINTSUM without confusing the audience or bogging down the GRINTSUM with too much information. Of course, analysts must consider alternatives to their assessments, but in most cases, the intelligence staff should keep this type of information internal. However, three of the standards require further explanation.

Properly describe the quality and credibility of all underlying sources, information, and methodologies. This standard calls for analysts to properly describe the quality and credibility of their sourcing—something analysts often fail to do in GRINTSUMs.[4] For example, some may write a significant activity (SIGACT) report based on a very low-quality source and in doing so fail to alert their audience to concerns with the sourcing. The audience, in turn, must assume the information in the product is entirely credible. The easy solution to this issue is to include source descriptors in the form of "according to" statements at the end of each SIGACT report or any summary of reporting.[5] For instance—

> As of 01 August, SAPA forces were planning an attack on FOB X-Ray, according to a detained SAPA member with direct access to the information.

If space is limited, which is often the case, the analyst can simplify the descriptor to something like "according to a detainee." Again, the reason for doing this is to ensure that commanders and staffs understand the quality and reliability of the data in the GRINTSUM.

Properly express and explain uncertainties associated with major analytical judgments. Properly distinguish between underlying intelligence information and analysts' assumptions and judgments. These two standards require the analysts to properly express and explain uncertainties with major analytic judgments while distinguishing between assessments, assumptions, and information. One way to do this is through expressions of likelihood, such as "likely" or "unlikely."[6] This is important for two reasons. First, it signals that the analyst is making an assessment—not a statement of fact—and second, it lets the audience know how likely it is that the analyst's judgments are accurate.

Estimative Language: Expressions of Likelihood[7]

Expressions of Likelihood	Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
	Remote	Highly Improbable	Improbable	Roughly Even Odds	Probable	Highly Probable	Nearly Certain
Probability	1–5%	5–20%	20–45%	45–55%	55–80%	80–90%	95–99%

Some commanders and staff may dislike the use of probabilistic language, thinking it is "wishy-washy," but it is the duty of the intelligence staff to enforce the analytic standards and explain their importance. After all, war is a social and political phenomenon. Thus, there is a considerable degree of uncertainty, especially since intelligence analysts do not have access to perfect information about the enemy and operational environment. Even if they did, they unconsciously filter their analysis through analytic lenses that may distort how they interpret the information.

In addition to describing the quality of sourcing, analysts must ensure they go beyond the initial report for a topic they are analyzing. This is especially true for complex developments for which there is ample reporting. For instance, one cannot gain a full and accurate sense of an adversary's warfighting capabilities based on a single report from one point in time. Such topics require analysts to look back into years of reporting to understand the evolution of those capabilities and the organization's performance in multiple contexts, be it in exercises or real-world operations. This type of in-depth research, however, is best suited for division-level and above staffs that generally have the time, space, and analytical expertise to conduct more extensive and intensive research.

When producing products on their specific problem sets, analysts must also avoid the tendency to simply copy and paste other organizations' finished intelligence products; rather, they should do their best to examine the original sources of information those organizations used. After all, one cannot assume those other organizations accurately characterized the information in the underlying source material, and when analysts write the report in their own words based on their own research, they will be more likely to fully understand the material.

There are, however, some instances when copying finished intelligence is preferable to original production, for example, when the information is highly technical and requires analysts with specialized experience and training. Additionally, it is advisable to take another organization's storyboard for a particular event they participated in or directly witnessed. When doing so, analysts should ensure they properly credit the originators, who will likely be happy to see that others have noticed their hard work. Sourcing the work to the originators will also ensure the audience has the proper points of contact for those organizations to ask questions about the original reports.

Principle 3: Readability

All this hard analytical work means little if the audience cannot easily read and understand the information. One of the most common ways to facilitate the audience's comprehension is to guide readers' eyes to the main points of each page of the GRINTSUM by using textboxes, colors, and bolded or italicized text. For instance, the assessments should be easily identifiable at the top or bottom of every slide/page using a standard format.

Meanwhile, the evidence analysts use to create their assessments should be in neat bullets consisting of short, clear sentences with no more than three to four lines of text. Having more than four lines creates large word blocks the average commander and staff officer do not have the time or the patience to navigate. Sentences should also follow simple, short structures. For example—

- **Standard Pattern:** Timeframe → subject → verb → direct object (when appropriate) → source descriptor (when appropriate).
- **Example:** On 01 March 2020, SAPA forces attacked FOB X-Ray, according to Atropian media reporting.

When possible, those sentences should be fewer than 40 words to improve their readability. Keeping sentences concise ensures the audience quickly reads, processes, and retains the information. Retention is essential because ultimately the purpose of all-source products like GRINTSUMs is to inform immediate- and long-term decision making.

Principle 4: Article Types

From an all-source perspective, the GRINTSUM normally comprises five types of products in addition to standard content like the weather forecast and effects chart and the PIR slides:

- SIGACTs.
- Intelligence highlights.
- Storyboards.
- Profiles (equipment, personnel, organizations, and processes).
- Historical background notes.

SIGACTs. The SIGACT should briefly summarize and assess a key development (or developments) that occurred since the publication of the last GRINTSUM. The summary generally includes the "5Ws": who, what, when, where, and why. The summary should follow the standard sentence format as described earlier in "Principle 3: Readability," starting with the timeframe and ending with the source descriptor. After that sentence, the analyst may provide one or two additional sentences, giving context for the SIGACT. Following the summary, the analyst should provide a one- to three-sentence assessment that identifies the "so what" for the SIGACT, with a focus on tailoring it to the needs and interests of one's command and staff. When possible, SIGACTs should also be arranged thematically (by country, topic, etc.) to enhance readability.

There are many ways to organize SIGACTs onto a page or slide. One of the most common and effective is to group them

by location or theme. Each SIGACT should be numbered and that number should also appear on a map to help the audience know where the event occurred in relation to friendly or enemy forces. Simple techniques like these will help the command and staff to visualize the operational environment by understanding where key events are happening in relation to organizations, areas of interest, and other events.

Intelligence Highlights. Intelligence highlights generally have three components: a short paragraph summarizing the main developments (the 5Ws), two to four bullets of evidence from reporting that supports the summary, and an assessment at the end. Alternatively, the first paragraph can contain the development and the assessment followed by two to four bullets of evidence. Ideally, the highlight will also have an associated graphic on the same slide/page, such as a table showing indicators and warnings for contingencies related to the highlight, or more simply, it can be a related picture or map depicting the information in the highlight. These graphics or images have the benefit of helping visual learners to more easily understand and retain the information in the highlight.

There is also the longer-form highlight that generally takes up an entire slide. The product has the same core features of the shorter version with some differences. In general, the summary is at the top of the article, usually in a textbox, and the assessment is at the bottom of the slide. The assessment often appears in a colored textbox in order to steer the audience to the most important information. On the right-hand side is the graphic, and on the left-hand side are bullets showing the evidence used to make the summary and assessment. However, instead of filling the entire page with bullets, the analyst should organize them into two or three groups with their own headers to set them apart, for example—

- Details about the development under examination elaborating on the 5Ws.
- Evidence for the causes/drivers behind the development.
- Identification of threats or opportunities for friendly forces.
- Several bullets projecting what may happen next in order of likelihood.

Storyboards, Profiles, and Historical Background Notes. In addition to SIGACTs and intelligence highlights, GRINTSUMs can have useful background information for the commander and staff. Such information includes storyboards summarizing key events; profiles; and backgrounds of a particular person, historical event, piece of equipment, and more. These types of products generally come at the end of the GRINTSUM and should link to a SIGACT or a highlight. For example, if one SIGACT deals with a particular piece of enemy equipment, then analysts could include a profile about that equipment.

Intelligence Highlights

Donovian Offensive Imminent

On 02 April, the Donovian 12th Combined Arms Army (CAA) deployed to attack positions along the line of contact with Farlandia. The 12th CAA consists of two motor rifle divisions and three armored divisions. Opposing the 12th CAA are three Farlandian motor infantry divisions.

- Between 20 and 30 March, the 12th CAA moved from mobilization depots to staging ground 10 km west of the line of control, according to press reporting and imagery.
- Between 30 March and 02 April, 12th CAA elements occupied attack positions along the line of contact, according to imagery.

Assessment: The Donovian 12th CAA likely will conduct offensive operations into Farlandia within the next 24 to 48 hours to seize control over the disrupted border zone.

Commercial satellite imagery showing elements of 12th CAA at staging areas near line of contact, 02 April 2021

Donovian Separatists Acquire SA-15 Battery

On 31 March, the Donovian government transferred one battery of SA-15s to Donovian separatists inside Donetsk. The SA-15 is a short-range surface-to-air missile system designed for destroying airplanes, helicopters, cruise missiles, precision guided munitions, unmanned aerial vehicles and short-range ballistic threats (anti-munitions).

- On 31 March, the Donovian Western Front commander authorized the transfer of one battery of SA-15s to separatists inside Donetsk, according to press reporting.
- As of 01 April, Donovian separatists are staging the newly acquired SA-15s—which they previously trained on in 2019—in defensive positions 10 km west of the line of contact, according to imagery.

Assessment: The SA-15 battery likely will enhance Donovian separatists' ability to detect and defeat Farlandian UAVs and helicopters operating along the line of contact.

Donovian SA-15 deployed near Donetsk, 01 April 2021.

Example of intelligence highlights

Roles and Responsibilities

Junior Analyst Key Responsibilities

Performs message traffic search to find reporting to answer intelligence questions and to identify any significant activities for the GRINTSUM.

Summarizes reporting accurately and performs basic analysis on significant activities and highlights.

Writes basic profiles and backgrounders on topics provided to them.

Mid-Level Analyst Key Responsibilities

Guides junior-level analysts' research based on weekly/daily production plans; typically serves as a team lead for a particular country/functional topic.

Is the subject matter expert for their particular country/functional area.

Serves as the first-line reviewer on GRINTSUM products before publication.

Ensures products have an assessment that provides a "so what?" linked to priority intelligence requirements.

Senior-Level Analyst Key Responsibilities

Sets the daily/weekly production plan and associated intelligence questions for the GRINTSUM.*

Synchronizes teams' production and coordinates with internal and external organizations.

Serves as an organization's overall subject matter expert on its particular area of responsibility.

Coordinates the integration of all-source production with single-source disciplines and open-source intelligence.

Serves as final reviewer on products within the GRINTSUM.

* A production plan outlines the topics that analysts will produce during a specified timeframe; the more time leadership gives them, the more in-depth they can go on their research.

Principle 5: Analytical Responsibilities

To manage the GRINTSUM production process, ACE and fusion chiefs can divide their all-source analysts into three basic job categories based on their experience and expertise. Doing so puts analysts, and the team as a whole, in a position to succeed. Moreover, these categories should not focus too heavily on rank because, in some cases, junior Soldiers are more experienced and capable of performing high-quality analysis on a particular topic than a more senior Soldier or a noncommissioned officer. This is especially true for the Army National Guard and Army Reserves because many privates first class (E-3) and specialists (E-4) work in the intelligence community, law enforcement, or a host of other fields requiring in-depth analytical expertise and experience. This division of labor can also serve as a basis for a product review chain, which is essential for making sure products are technically sound and adhere to the analytic standards in ICD 203.

Conclusion

There are, of course, no fixed rules for how to structure teams or how to employ any of the principles discussed in this article. Rather, I hope these five principles can provide a general framework others can adapt based on mission requirements and available capabilities. I also hope that as intelligence professionals adapt these principles, they can share their best practices on how to make Army GRINTSUMs more readable, analytically rigorous, and mission-relevant to enable decision advantage.

The process of assessing warfare and informing decision makers is a forever-changing art. Therefore, all-source professionals must constantly adapt products to meet these variable conditions; otherwise, analysts risk losing their ability to provide decision makers with credible, timely, and actionable information to inform decisions and plans.

Endnotes

1. Office of the Director of National Intelligence, Intelligence Community Directive 203, *Analytic Standards* (Washington, DC, 2 January 2015), 3–4.

2. Department of the Army, Army Techniques Publication (ATP) 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. Government Publishing Office, 10 January 2020), E-3, E-7–E-8.

3. Ibid., C-1–C-2.

4. Defense Intelligence Agency, Tradecraft Note 02-17, *Sourcing* (Washington, DC: Office of the Research Director, 2017).

5. Ibid.

6. Department of the Army, ATP 2-33.4, *Intelligence Analysis*, C-2.

7. This figure is a modified version of the original in Department of the Army, ATP 2-33.4, *Intelligence Analysis*, C-2.

CW2 Andrew Chadwick, Ph.D., is an all-source intelligence technician with the 29th Infantry Division, Maryland Army National Guard. As a civilian, he serves as an intelligence analyst with the Department of Defense. He wrote this article based on experiences and observations producing graphic intelligence summaries, intelligence summaries, and many other intelligence product types over the past decade while deployed to Afghanistan, during a rotation to Kuwait, as an intelligence analyst with the National Guard Bureau, and while working as a civilian for the Department of Defense.

EMBRACING BIG DATA
Analytical Techniques

by Colonel Jeremy Hartung and Major Eric Nolan

Introduction

Several recent articles in the *Military Intelligence Professional Bulletin* have argued for the importance of incorporating big data analysis into the military intelligence (MI) toolkit.[1] The consensus is that increasing amounts of information and sources of data are overwhelming both technical and cognitive capabilities within our intelligence sections. Proposed solutions to the gap in big data analysis tend to focus on support from industry experts or the purchase of new analytic software. While both of these are important aspects of improving the Army's big data capability, these solutions ignore innovative analytical techniques that MI professionals could employ today. Furthermore, methodologies like the Multi-INT Spatial Temporal (MIST) toolsuite, developed as part of the Fusion Analysis Development Effort (FADE) program, provide a sufficient platform to apply the principles of big data analysis without waiting for the perfect solution in a future system.

The 2016 textbook *Activity-Based Intelligence: Principles and Applications* provides a foundational analytic approach to big data analysis for MI professionals.[2] Activity-based intelligence, also known as ABI, can be applied at the brigade combat team (BCT) level immediately to leverage underutilized sources of data and fill intelligence gaps for the commander. This article will describe ABI's four main ideas, or pillars, with examples of their immediate utility at the BCT level.

What is Activity-Based Intelligence?

"ABI is an analysis methodology that rapidly integrates data from multiple sources to discover relevant patterns, determine and identify change, and characterize those patterns to drive collection and create decision advantage….ABI practitioners have advanced the concept of large-scale data filtering of events, entities, and transactions to develop understanding through spatial and temporal correlation across multiple data sets."[3]

The Development of Activity-Based Intelligence

ABI was born out of the Special Forces intelligence community during the height of the wars in Iraq and Afghanistan.[4] Targeting individuals in the modern interconnected world allowed the Special Forces to leverage more sources of data than ever before. However, as they did this, they became overwhelmed and developed ABI as an approach to work with big data. As the name implies, ABI starts with observed activity. All activity must happen at a defined time and place. If analysts can gain access to data sets of events, including locations and times, they can make spatiotemporal correlations between events that would otherwise seem to be unrelated or unimportant. This key insight led to the development of ABI and its four pillars:

- Georeference to discover.
- Integration before exploitation.
- Sequence neutrality.
- Data neutrality.[5]

A Summary of the Four Pillars[6]

- **Georeference to Discover:** Focusing on spatially and temporally correlating multi-intelligence (INT) data to discover key entities and events.
- **Integration before Exploitation:** Correlating data as early as possible, rather than relying on vetted, finished products (from single INT data), because seemingly insignificant events in a single INT may be important when integrated across multiple INTs.
- **Sequence Neutrality:** Understanding that we have the answers in the data collected at any time to many questions we do not yet know to ask.
- **Data Neutrality:** The premise that all data may be relevant regardless of the source from which it was obtained.

Georeference to Discover

Georeference to discover refers to the ability to add location and time information to data sets, allowing for geospatial and temporal correlations. The resulting correlations are "discovered" as a result of structuring the data to allow a quick comparison of the locations and times of these events. Using methodologies like the FADE program's MIST toolsuite, users can pull in many disparate data sets and perform geospatial discovery. The key is pulling in the right data and ensuring it is properly georeferenced.

The BCT offers many good examples of how to effectively employ georeference to discover. In fact, the BCT has tremendous advantages over higher echelons for analyzing georeferenced data because it has a narrow geographic focus. However, not all the data available at the BCT is readily georeferenced in databases. The georeferenced data is rarely in a format that allows machines to digest it easily and enable a geospatial discovery environment. This is due to a complex combination of problems with system interoperability and a systemic failure to train using mission command systems in accordance with their design. For example, most BCT tactical operations centers do not send reports using the United States message text format (USMTF) between mission command systems. Instead, they depend heavily on text chat programs like TransVerse, mIRC chat, or Joint Battle Command-Platform texts that machines do not automatically scrape for georeferenced data to include in databases. Soldiers have to read the chat message text line by line and relay relevant information to the rest of the BCT headquarters. However, some BCT S-2 sections have been using applications like Rip-It or ChatSurfer to scrape georeferences from text services.[7] These programs can read thousands of lines of text and provide an overlay with all the locations and times of events mentioned in the message traffic.

Georeferencing the text applications of tactical operations centers will allow intelligence analysts to easily ingest reports from subordinate units into their larger geospatial discovery environment. Automating the process through ChatSurfer will allow faster discovery of previously unknown correlations between subordinate unit reports and all other intelligence reports, making the brigade significantly more responsive to the environment. Scraping text applications is just one example of how to apply georeference to discover. Enterprising analysts across the Army are likely to find many more uses once they are aware of the concept.

Integration before Exploitation

The second pillar of ABI is integration before exploitation. Integration in this context is *fusion*, defined in ADP 2-0, *Intelligence*, as "consolidating, combining, and correlating information together."[8] Fusion occurs in the traditional intelligence process during the produce step after collection tasking, information collection, and information processing.[9] Preliminary exploitation and processing prioritize and limit the amount of information passed to all-source analysts for fusion. In the traditional intelligence process, limiting the information passed to all-source analysts for fusion is a positive feature because traditional information management techniques could easily overwhelm these analysts. However, the ability to perform geospatial discovery in ABI depends on having access to all the available data, not just the bits that single-source reports provide to answer priority intelligence requirements. Performing ABI requires analysts to have access to all data before making judgments about the information's relevance or importance.

The clearest example of integration before exploitation in the BCT is intelligence data that the integrated broadcast service provides from overhead collection systems. Analysts in the BCT can currently access the integrated broadcast service layer in near real time through the Joint Tactical Terminal on the Tactical Ground Station or through the MIST toolsuite on the SECRET Internet Protocol Router Network (SIPRNET) and Joint Worldwide Intelligence Communications System. S-2 sections often assign this data analysis to signals intelligence analysts and geospatial intelligence analysts because they are better suited to perform the analysis and provide a finished intelligence report. However, new programs like FADE and the MIST toolsuite require only a few hours of training and practice for most all-source analysts to learn how to manipulate the data. Then they can compare multi-INT reporting in a specific geographic area to discover previously unknown correlations. The MIST toolsuite provides intuitive geospatial discovery environments that make integration before exploitation possible. Rather than the data overwhelming analysts, ABI allows analysts to process more and more data efficiently to fill intelligence gaps for the commander.

> **"An ABI analyst correlating activities and resolving objects will enable real-time tipping and cueing of sensors, thereby driving collection, again, in ways that cannot be done today."[10]**

Sequence Neutrality

ABI's third pillar is sequence neutrality. Its basic premise is to recognize that establishing temporal causality is difficult when looking back at events that have already occurred. Performing discovery requires the analyst to be conscious

of the logical fallacy—*post hoc, ergo propter hoc* (in other words, after this, therefore because of it).[11] In layman's terms, this is a logical fallacy in which one might believe an event caused another event simply because it happened first. This fallacy serves as a warning to ABI analysts that they cannot be satisfied with simply establishing causality. When analysts believe they have discovered what caused an event, they may stop looking for other potential causes or indicators of it. Instead, they should seek all indicators of an event. More sources and types of data will provide more clarity on the various indicators of an event. The benefits of this analytical work might result in identifying new indicators of enemy activity that could be included in future priority intelligence requirements for collection tasking. It could contribute to building enemy doctrinal templates by adding nuance to the activities the enemy performs in certain circumstances. In current operations, it could result in targeting information that contains more detail.

Sequence neutrality has implications for the types of data that units need to access and store. The ABI analyst conducting geospatial discovery does not necessarily know what data will lead to actionable intelligence. Similarly, sequence neutrality suggests the ABI analyst needs access to data from a broad period of time. These requirements mean that the ABI analyst will depend on data from outside the BCT. Unfortunately, accessing external data depends on establishing robust primary, alternate, contingency, and emergency (PACE) plans. The BCT must overcome concerns about operating in denied, intermittent, and limited bandwidth environments using redundant PACE plans that have different transport layers. A BCT S-2 section today can gain access to the integrated broadcast service layer using three different types of transport: satellite communications over the Joint Tactical Terminal, tactical SIPRNET over the Warfighter Information Network-Tactical, and Tactical Data Network-1 through the TROJAN. This PACE plan will only improve with the future introduction of the Tactical Intelligence Targeting Access Node (TITAN) system. The crucial lesson from this pillar is that units need to recognize the absolute necessity to access data from echelons above brigade and then to prioritize, resource, and train their PACE plan to be successful in modern large-scale ground combat operations.

Data Neutrality

The fourth pillar of ABI is data neutrality. This pillar serves as a reminder that the best intelligence is not always highly classified. The best intelligence is simply that which provides timely and relevant support to the commander's decision making. Top secret information is not better than secret information. The sources and methods used to obtain the information are simply more sensitive, and we must protect them more carefully. With this in mind, data neutrality requires ABI analysts to fully understand the capabilities and limitations of MI systems, the systems of the other warfighting functions in the BCT, and even the systems in adjacent or supporting units to make sure they do not overlook valuable data. The modern battlefield is littered with sensors providing data for all sorts of varying purposes. Identifying opportunities to pull more data into the ABI geospatial discovery environment is a critical part of planning for any operation.

The BCT S-2's running estimate will often list the available organic collection platforms. It may also list the requested echelons above brigade support platforms. These running estimates must also include the Q-36 and Q-50 counter-battery radar systems—not just to note their presence in the BCT or to attempt tasking them as collection platforms but as a reminder to incorporate their data into the geospatial discovery environment. Supporting aircraft are another source of

data. Most have air defense threat warning systems that can report the locations of enemy air defense assets. Comparing aircraft threat warning data to data from echelons above brigade and overhead systems' sensors could result in enough target fidelity to enable the destruction of high-payoff targets. Pulling these sources of data into the geospatial discovery environment might be as simple as automating the text-scraping applications previously discussed or using USMTF messages between mission command systems to deliver machine-readable location data. Either way, the S-2 section must plan how it will receive the data and ensure the architecture supports the proposed plan. The S-2 section should seek out any data source that can provide the location and time of an event and pull it into the geospatial discovery environment.

Application of Activity-Based Intelligence in BCTs

BCTs today could employ the four pillars of ABI to improve analytic outcomes and fill gaps for the commander. The key component to being prepared to perform ABI on the battlefield is being able to train in data-rich environments. The National Training Center (NTC) has been leading the effort to build a modern data-rich intelligence training environment, enabling just such a training opportunity. Leaders at the NTC have recognized that BCTs are preparing to fight against highly technical systems with distinct signatures, yet training environments do not typically incorporate these signatures. Rather, finished reporting is often pumped directly into databases, denying intelligence sections the ability to do their own data analysis.

NTC is approaching this problem by hand-scripting data into the scenario, giving rotational training units the opportunity to "eat the data raw" rather than relying on external processing, exploitation, and dissemination support. The NTC is also experimenting with the automated production of raw reporting in order to create the vast volume of reporting that would be realistic in any future technology-enabled environment. In fact, units unprepared to deal with the overwhelming amount of data available at the NTC will struggle to gain a situational understanding of the operational environment.

Conclusion

Industry is offering advanced technical solutions, but the MI community cannot wait for the fielding of new systems to start developing new doctrinal approaches to analyzing big data. ABI offers an analytic approach that is ready to fill the current gap. The examples in this article are just a few ways BCTs could immediately employ ABI to help leverage underutilized sources of data.

Armed with the four pillars of ABI, analysts across the Army will discover untapped sources of data they could quickly georeference and pull into geospatial discovery environments for improved analytical outcomes. Big data is a reality on the battlefield now, and the MI community should embrace ABI to keep pace with that reality.

Endnotes

1. Jason Boslaugh and Zachary Kendrick, "The Application of Data Science in the Intelligence Warfighting Function," *Military Intelligence Professional Bulletin* 45, no. 4 (October–December 2019): 57–63; Iain J. Cruickshank, "On Data Science and Intelligence Analysis," *Military Intelligence Professional Bulletin* 45, no. 3 (July–September 2019): 29–32; and Garrett Hopp, Glenn Gleason, Nick Rife, and Ashley Muller, "Data Analytics to Win in a Complex World," *Military Intelligence Professional Bulletin* 44, no. 4 (October–December 2018): 59–61.

2. Patrick Biltgen and Stephen Ryan, *Activity-Based Intelligence: Principles and Applications* (Norwood, MA: Artech House, 2016).

3. Patrick Biltgen, Todd S. Bacastow, Thom Kaye, and Jeffrey M. Young, "Activity-Based Intelligence: Understanding Patterns-of-Life," United States Geospatial Intelligence Foundation, April 18, 2017, https://medium.com/the-state-and-future-of-geoint-2017-report/activity-based-intelligence-understanding-patterns-of-life-481c78b7d5ae.

4. Biltgen and Ryan, *Activity-Based Intelligence*, 23–25.

5. Ibid., 33–51.

6. Lauren Zabierek, "Enabling OSINT in Activity-Based Intelligence (ABI)," Recorded Future, August 31, 2016, https://www.recordedfuture.com/activity-based-intelligence/.

7. The 1-2 Stryker Brigade Combat Team (SBCT) S-2 section used Rip-It and ChatSurfer with some success during Joint Readiness Training Center rotation 21-02 with the 5th Security Force Assistance Brigade (SFAB). However, since the 5th SFAB was the rotational training unit, and the 1-2 SBCT was role-playing a host-nation force, the brigade had limited access to intelligence feeds that would have made creating a geospatial discovery environment possible.

8. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, 31 July 2019), Glossary-3.

9. Ibid., 3-2.

10. David Gauthier, "Activity-Based Intelligence Definition for the Intelligence Community," National Geospatial-Intelligence Agency, 2013, quoted in Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Force Quarterly* 77 (2nd Quarter, 2015): 26, https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/.

11. Biltgen and Ryan, *Activity-Based Intelligence*, 47–49.

COL Jeremy Hartung is the Senior Intelligence Officer at the National Training Center. He previously served as the 7th Infantry Division G-2 and as the S-2 for the 173rd Airborne Infantry Brigade Combat Team. He is a graduate of the Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance.

MAJ Eric Nolan is the Analysis and Control Element Chief for the 1st Multi-Domain Task Force at Joint Base Lewis–McChord, WA. He previously served as the S-2 for the 1-2 Stryker Brigade Combat Team and as the Deputy G-2 for the 7th Infantry Division. He holds a master of arts in strategic studies and international economics from Johns Hopkins University's School of Advanced International Studies.

Interested in an Intelligence Career with a Fort Bragg Special Missions Unit?

TRUST ▲ ADAPTABILITY ▲ COMMITMENT

THE Mission

Entrusted with the Nation's most critical tasks, we stay at the leading edge of operations that immediately impact global security.

National Crisis Response
Some problems require immediate action and application of unique skills where failure is not an option.

High Value Targeting
We specialize in capturing and eliminating the most influential threats to our Nation and the World.

Combat Development
Staying at the forefront of the modern combat environment requires continuous development of cutting edge tools and weapons, by individuals who operate at the highest levels.

Assignments for:

35A, 35D, 35F, 35G, 35L
35M, 35N, 35P, 35S, 35T
35X, 35Y, 18F

Apply in 4 Easy Steps

Step 1
Email your SRB/ORB to:

army.sof1-recruiter@mail.mil

and request an online application

Step 2
Complete and Submit an online application consisting of:

- Application
- Commander Evaluation
- Updated ORB/SRB
- All OER/NCOERs
- All 1059s
- Security Clearance (SF 86)

Step 3
Attend an assessment

Step 4
Those selected will PCS to Fort Bragg to begin training or start work in their new position

"THE RELENTLESS PURSUIT OF EXCELLENCE"

CALL **(910) 643-0699**

Contact & Article
Submission Information

This is your professional bulletin. We need your support by writing and submitting articles for publication.

When writing an article, select a topic relevant to Army MI professionals.

Our goals are to spark discussion and add to the professional knowledge of the MI Corps and the intelligence community. Articles about current operations, TTPs, and equipment and training are always welcome as are lessons learned, historical perspectives, problems and solutions, and short "quick tips" on better employment of equipment and personnel. Explain how your unit has broken new ground, give helpful advice on a specific topic, or discuss how new technology will change the way we operate.

When submitting articles to MIPB, please consider the following:

- Feature articles, in most cases, should be between 1,000 and 3,000 words, double-spaced with normal margins without embedded graphics.
- We cannot guarantee we will publish all submitted articles.
- Please do not send overly large and complicated or small print graphics/PowerPoint slides. What looks good as a PowerPoint presentation doesnt always translate well to an 8 1/2" x 11" article format.
- Please do not include any personally identifiable information (PII) in your article or biography.
- Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

What we need from you:

- Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.
- A cover letter/email with your work or home email, telephone number, and a comment stating your desire to have your article published.
- **(Outside of USAICoE)** A release signed by your unit's information security officer stating that your article and any accompanying graphics and photos are unclassified, not sensitive, and releasable in the public domain. A sample security release memorandum is available from the MIPB Staff. Contact us at the email address at the bottom of the page.
- **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297) for information on how to get a security release approved for your article. A critical part of the process is providing all of the source material for the article to the information security reviewer in order to get approval of the release.
- Article in Microsoft Word; do not use special document templates.
- Pictures, graphics, crests, or logos relevant to your topic. Include complete captions (the 5 Ws), and photographer credits. Please do not send copyrighted images. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg.** Photos must be at least 300 dpi. If relevant, note where graphics and photos should appear in the article. PowerPoint **(not in .tif/.jpg format)** is acceptable for graphs, figures, etc.
- The full name of each author in the byline and a short biography for each. Biographies should include authors' current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications.

We will edit the articles and put them in a style and format appropriate for MIPB. From time to time, we may contact you during the editing process to help us ensure a quality product. Please inform us of any changes in contact information.

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

MIPB (ATZS-DST-B)
DOTD, USAICoE
550 Cibeque St.
Fort Huachuca, AZ 85613-7017

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

PIN: 214953-000