MI Professional Bulletin

July - September 2018
PB 34-18-3

INSCOM

UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND

Enabling Readiness for the Intelligence Enterprise

Modernizing to Enable Greater Lethality | Setting the Theater

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

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

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

Our mailing address: MIPB (ATZS-DST-B), Dir. of Doctrine and Intel Sys Trng, USAICoE, 550 Cibeque St., Fort Huachuca, AZ 85613-70

Commanding General
MG Robert P. Walters, Jr.

Chief of Staff
COL Douglas R. Woodall

Chief Warrant Officer, MI Corps
CW5 Matthew R. Martin

Command Sergeant Major, MI Corps
CSM Warren K. Robinson

STAFF:

Editor
Tracey A. Remus
usarmy.huachuca.icoe.mbx.mipb@mail.mil

Associate Editor
Maria T. Eichmann

Design and Layout
Emma R. Morris

Cover Design
Robin H. Crawford
IAPA-INSCOM Public Affairs

Military Staff
CPT John P. Mones
CPT Emily R. Morrison

Purpose: The U.S. Army Intelligence Center of Excellence publishes the **Military Intelligence Professional Bulletin** (**MIPB**) quarterly under the provisions of **AR 25-30**. **MIPB** presents information designed to keep intelligence professionals informed of current and emerging developments within the field and provides an open forum in which ideas; concepts; tactics, techniques, and procedures; historical perspectives; problems and solutions, etc., can be exchanged and discussed for purposes of professional development

By order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

GERALD B. O'KEEFE
Administrative Assistant to the
to the Secretary of the Army
1814308

From the Editor

We would like to take this opportunity to acknowledge and thank INSCOM's CPT Andrew Harris for the significant contributions he made to the development of this issue. Other INSCOM contributors include Robin Crawford, COL Nichoel Brooks, CPT Gretchen Pace, and INSCOM's Public Affairs Office. Without the planning, coordination, support, and other key contributions of these dedicated professionals, this highly informative edition could not have been accomplished.

As always, articles from you, our reader, remain important to the success of MIPB as a professional bulletin. **We are currently looking for a few good articles to feature in our new recurring department—Know Your Enemies, Adversaries, and Threats.** The focus of these articles will be on specific countries and groups whose objectives may be at odds with the interests of the United States.

The following themes and deadlines are established:

January–March 2019, *Intelligence Support in Large-Scale Combat Operations*. This issue will focus on the challenges of intelligence support in a complex environment against a peer threat. Deadline for article submission is 4 October 2018.

April–June 2019, *Intelligence and Special Operations.* This issue will focus on how intelligence professionals provide support to special operations forces. Deadline for article submission is 17 December 2018.

July–September 2019, *Security Force Assistance Brigade S-2*. This issue will focus on the roles of the SFAB S-2 in conducting security cooperation activities. Deadline for article submission is 2 April 2019.

Please call or email me with any questions regarding article submissions or any other aspects of MIPB. We welcome your input and suggestions.

Tracey A. Remus
Editor

MI Professional Bulletin

July - September 2018
PB 34-18-3
Volume 44 Number 3

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

FEATURES

5 What is the Intelligence and Security Command For?
by MG Christopher S. Ballard, COL Nichoel E. Brooks, LTC Jarred M. Lang, MAJ Christopher D. Thornton, CPT Charles F. Nadd, CPT Gretchen L. Pace, and Mr. Thomas J. Stokowski

10 The U.S. Army Intelligence and Security Command at Four Decades Part I: Inception
by Mr. Michael E. Bigelow

12 Seeing the Elephant: INSCOM's Exercise of Mission Command
by LTC Ryan H. Beery

18 Intelligence and Security Command Mission Command
by Mr. Richard Harfst and Mr. Thomas Stokowski

–ENABLING READINESS FOR THE INTELLIGENCE ENTERPRISE–

25 The Army Intelligence Program of Analysis
by Ms. Rita McIntosh, Ms. Kelly Nelson, and Dr. Crisanna Shackelford

29 Setting the Theater: A Critical Intelligence Function
by MAJ James Chester

33 Efforts in Africa: The New Frontier
by CW5 David Bassili and CW3 James Macfarlane

38 The U.S. Army Intelligence and Security Command at Four Decades Part II: Winning the Cold War (1981 to 1989)
by Mr. Michael E. Bigelow

40 Return of the Technical Control and Analysis Elements for Theater Signals Intelligence Support
by Mr. Scott R. Hammon

43 How INSCOM Supports Intelligence Readiness in Europe
by Mr. Steve Hughes

–ENABLING READINESS IN THE KOREAN THEATER OF OPERATIONS–

48 The Stage: Land of Interrupted Calm
by COL Derrick S. Lee and MAJ Margaret Dervan Hughes

58 The U.S. Army Intelligence and Security Command at Four Decades Part III: Regional Conflicts and Drawdown (1989 to 2001)
by Mr. Michael E. Bigelow

–MODERNIZING FOR GREATER LETHALITY–

61 Innovation and Modernization: INSCOM's Aerial Intelligence, Surveillance, and Reconnaissance
by LTC Tony K. Verenna, LTC Keith A. Haskin, MAJ Trevis C. Isenberg, Mr. Stephen A. Gasparek, and Mr. Marco A. Garavito

65 OSINT: Increasing Readiness by Leveraging the Digital Environment
by Mr. Daniel Zieminski

69 The U.S. Army Intelligence and Security Command at Four Decades Part IV: Global War on Terrorism
by Mr. Michael E. Bigelow

71 The Road to the Data Strategy for Army Intelligence
by Mr. Kirk G. Brustman, Mr. Erik K. Christensen, Dr. Holly A. Russo, LTC Russel J. Edmiston, and Mr. Richard H. Saddler

78 Developing a Big Data Strategy: Where We Are and Where We Need to Go
by COL Ingrid Parker

83 Army Processing, Exploitation, and Dissemination Capabilities: Adapt, Evolve, Innovate
by CW3 Otis Griffin III

86 Building a Strong Europe Through Collaborative Intelligence
by COL David W. Pendall and LTC Christopher J. Heatherly

89 Joint Certification of Service Human Intelligence Collector Training and Professional Development
by CW5 Joseph P. Lancaster

90 MG Oliver W. Dillard Award by MAJ Jason Elphick

91 BG Roy M. Strom Award by MAJ Jason Elphick

109 A Tribute to Military Intelligence Legend Lieutenant General James Arthur Williams
by COL Nichoel E. Brooks and CPT Jessica A. Tarsa

DEPARTMENTS

2 Always Out Front
3 CSM Forum
4 Technical Perspective
92 Distinguished Members of the MI Corps/ MI Corps Hall of Fame
100 Doctrine Corner
102 USAICoE Lessons Learned
104 Culture Corner
106 Moments in MI History

Always Out Front

by Major General Robert P. Walters, Jr.
Commanding General
U.S. Army Intelligence Center of Excellence

In 1977, 10 years before the development of the Military Intelligence (MI) Corps, the Army established the U.S. Army Intelligence and Security Command (INSCOM). The need for INSCOM came during a time when numerous conflicts arose throughout the world: the Cambodian Campaign, the Vietnam War, and the Lebanese Civil War, along with Hutu genocides in Burundi and the Moro Rebellion of the Philippines. With a multitude of conflicts occurring within most every region of the world, the Army established INSCOM to integrate all intelligence disciplines under one command to meet the increasing demands for intelligence.

As the Army continues to change, so does Army intelligence and INSCOM. The Army G-2 recently created the Army Intelligence Plan to ensure intelligence readiness and modernization issues are synchronized and energized. Driven by recommendations from the Bottom Up Review and various other intelligence studies and strategies, this plan requires INSCOM and the U.S. Army Intelligence Center of Excellence (USAICoE) to collaborate; ensuring the G-2's concept of "One Vision, One Vector, One Voice" is achieved. The plan calls for cooperation and communication between INSCOM, USAICoE, and the G-2 staff.

The Army Intelligence Plan is separated into near-, mid- and far-term objectives culminating with an end state that delivers an Army intelligence team capable of supporting organizations at the tactical and operational levels regardless of the threat or operational environment. Near-term objectives focus on enhancing the capabilities and capacity at the brigade combat team, division, and corps echelons with the existing systems and force structure that are available today. Mid-term objectives concentrate on identifying capability gaps to optimize current sensors, while far-term objectives emphasize developing future sensors on upgraded platforms.

Since INSCOM is a critical component of all future intelligence operations, I decided to dedicate this quarter's MIPB to INSCOM. As you read this issue of MIPB, you will find perspectives from MG Ballard and his team who composed articles on the history, organizational design, and intricate relationships INSCOM has with the combatant commands. This issue of MIPB is a comprehensive guide to INSCOM and is a must-read for the Army's intelligence professionals seeking to understand and leverage national to tactical intelligence in support of tactical, operational, and strategic level operations. Take this opportunity to continue to learn about the many different aspects of our MI Corps and the ways that intelligence drives operations.

Always Out Front!

CSM FORUM

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

This is my first article as your Military Intelligence (MI) Corps Command Sergeant Major. Humbled and excited are the best words to describe my feelings at the opportunity to continue to serve our great Nation and Soldiers in this capacity. I am very appreciative of all the leaders and Soldiers who made the Army the great organization it is today through their amazing work and accomplishments over the years. It has truly been a team effort. Some of our key goals going forward are to validate MI force structure design, relook how we accomplish talent management, strengthen our Noncommissioned Officer (NCO) Corps through training and education, and develop more proficient and disciplined MI Soldiers who are ready to fight tonight. Meeting these goals will require teamwork, transparency, and collaboration with leaders across the Army intelligence community. Although mission accomplishment is always first, taking care of our Soldiers and their families is as important as any other task we undertake. The focus of this quarter's publication, the U.S. Army Intelligence and Security Command (INSCOM), plays a vital role in MI mission accomplishment.

INSCOM provides intelligence support to Army commanders worldwide by conducting multidiscipline intelligence operations to deliver comprehensive, collaborative intelligence to decision makers from national to tactical levels. INSCOM remains at the cutting edge of technologies; cyberspace and information operations; and tactics, techniques, and procedures (TTPs) that enable and enhance the Army's strategic roles in a complex world. INSCOM reaches across multiple components to ensure all commanders receive premiere intelligence support.

Additionally, INSCOM provides essential intelligence training focused on Forces Command units and Soldiers that are deploying. Much of the training is conducted through Foundry Intelligence Training Program sites collocated within our division footprints. The Foundry program enables MI Soldiers to sustain intelligence skills pertinent to their unit's mission and to improve their individual and collective technical and analytical skills. Certified subject matter experts provide relevant and realistic training to Soldiers of all ranks that is consistent with the various current operational environments. Foundry training ensures the necessary skillsets and proficiency levels that are invaluable to mission accomplishment are present within our tactical formations.

After many years focused on contingency and counterterrorism operations, our focus must now shift to the difficult task of providing an Army that is trained and ready to face the challenges of large-scale combat operations against a peer threat in a multi-domain environment. As the Army's operational arm for intelligence, INSCOM will be more important than ever to ensuring commanders receive predictive intelligence from numerous platforms. This creates a clear and contextual picture.

INSCOM also plays a critical role in the development of our NCO Corps. From a senior NCO's perspective, an assignment to an INSCOM unit provides commanders with well-trained Soldiers at all levels for a variety of tasks. The opportunity to conduct real-world intelligence operations within INSCOM units places Soldiers in a position to see immediate or near-term outcomes of their efforts to support decision makers ranging from the warfighter to key leaders at the national level. New technologies and TTPs provide flexible capabilities and tools that allow Soldiers to increase their skills to meet the ever-changing requirements. INSCOM units provide new opportunities for Soldiers to develop their operational and leadership skills. This is an integral part of leader development at the operational level. Through this type of assignment, we help build a stronger MI Corps as these skills will eventually move to other formations and assist other commanders with their intelligence missions.

Always Out Front!

Technical Perspective

by Chief Warrant Officer 5 Matthew R. Martin
Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence

The Army remains heavily engaged around the globe with more than 187,500 Soldiers allocated to combatant commanders in support of eight named contingency operations, various exercises, and theater security cooperation activities. The ever-increasing complexity of the operational environment, combined with the need to rapidly deploy, fight, and defeat a peer threat, creates new challenges for the intelligence warfighting function. Peer threats are capable of employing both conventional and irregular warfare capabilities, which requires the Army to have a trained and ready intelligence warfighting function that is innovative, adaptive, and highly skilled. In order to accomplish this, we must remain focused on continually improving our most precious commodity—our intelligence professionals.

The U.S. Army Intelligence and Security Command (INSCOM) contains 19 major subordinate commands and nearly 18,000 Soldiers, Department of the Army Civilians, and contractors that are "Always Out Front." Serving as the largest intelligence formation in the Army, INSCOM units are operationally employed across 180 locations and 45 countries, providing global intelligence reach. Our INSCOM intelligence professionals serve as irreplaceable force multipliers, often working shoulder to shoulder with their U.S. Army Forces Command (FORSCOM) and U.S. Army Special Operations Command (USASOC) partners. These professionals provide multidiscipline intelligence, security, and linguistic support to Army, joint, and coalition commanders in an effort to answer their priority intelligence requirements. These Soldiers offer unique skills and capabilities that are a critical component in helping to ensure the intelligence warfighting function accurately describes and visualizes the operational environment in support of commanders' decision-making process.

Since 1977, INSCOM has been a cornerstone of intelligence support for Army commanders and senior decision makers during every major conflict and contingency operation the U.S. Army has engaged in. INSCOM's ability to adapt and grow its capabilities to meet requirements has become vitally important given the fiscal environment and force constraints we currently face. The ability to leverage highly skilled specialists with physics, computer science, and engineering backgrounds enhances our understanding of the ever-changing operational environment. This support ensures we maintain a decisive advantage by leveraging technology within the cloud environment to provide rapid and agile intelligence support to the warfighter.

This is my final article as your Chief Warrant Officer of the Military Intelligence (MI) Branch. I am extremely proud of the work we have done over the last 4 years, as we have made significant improvements in many areas—the MI warrant officer force structure, talent management, education, capability and integration of the Distributed Common Ground System-Army family of systems, and cohort communications and collaboration. While much remains to be done, I am confident that our warrant officer cohort is on the right path, and will continue to mature and grow its technical competence under the leadership of the next Chief Warrant Officer of the MI Branch, CW5 Dave Bassili.

Never fail to recognize that we are at our best when we work as a team to develop and execute a common vision for the future of our warrant officer cohort. Much of what I accomplished in the past 4 years was only possible because of the strong partnership I developed with CW5 Andrew Maykovich (FORSCOM Senior Warrant Officer Advisor), CW5 Kevin Boughton (INSCOM Command Chief Warrant Officer), and CW5 Jess Ohle (USASOC G-2 Senior Warrant Officer Advisor).

Thank you for your service, sacrifices, and continued support to the Army, the MI Corps, and the cohort!

Always Out Front!

What is the Intelligence and Security Command For?

by Major General Christopher S. Ballard, Colonel Nichoel E. Brooks, Lieutenant Colonel Jarred M. Lang, Major Christopher D. Thornton, Captain Charles F. Nadd, Captain Gretchen L. Pace, and Mr. Thomas J. Stokowski

Introduction

MG Robert Walters, Jr.'s team at the U.S. Army Intelligence Center of Excellence in Fort Huachuca, Arizona, has dedicated the July-September 2018 issue of the *Military Intelligence Professional Bulletin* as the Intelligence and Security Command (INSCOM) edition. As part of an effort to educate the force about INSCOM's mission, the Soldiers and Civilians of the command have written a series of articles that describe how INSCOM functions as the operational headquarters for the Army intelligence enterprise, working to build intelligence combat power, achieve readiness, and modernize as we prepare for tomorrow's war. The intent is that through these articles you are empowered as an intelligence professional to leverage INSCOM and all the capabilities it brings to bear.

To put this into context, as the former U.S. Army Training and Doctrine Command Commanding General, retired GEN David Perkins, explained, "You need to understand what you are for before you understand what you need to do… Leaders have to capitalize on the environment or organization they are in. In other words, they need to understand the big picture. It falls uniquely on leaders' shoulders."[1] Understanding the purpose of an organization, no matter how small or large, goes beyond a mission statement—it requires a thorough analysis of the history, structure, and resourcing of the organization.

Evolution of Army Intelligence

Throughout the 243-year history of the U.S. Army, intelligence superiority has been decisive to victory. Commanders in every century have recognized the imperative for accurate, timely, and integrated intelligence, including GEN George Washington with his network of scouts and spies spread across the American colonies; President Abraham Lincoln and the Union's use of balloon reconnaissance in the Civil War; and GEN Dwight D. Eisenhower who relied on the vital work of cryptologists and Japanese-American linguists during World War II. Today's Army obtains intelligence superiority through a multitude of organizations and operations (from tactical to national). INSCOM resources and synchronizes a majority of these activities to reinforce and deliver that superiority.

The Army established INSCOM in 1977 as a way to meet the challenges of modern warfare. Through building an intelligence command that housed all the intelligence disciplines with the necessary authorities, INSCOM could fulfill a significant charter—unify various echelons above corps intelligence organizations that, until 1977, had narrowly focused on single intelligence disciplines or functions, as shown in Figure 1. This role as the unifier of Army intelligence activities provides INSCOM with unique flexibility and adaptability to deliver the results expected of an operational headquarters—yet it introduces a complexity that can frustrate those who lose sight of the purpose of this organization.

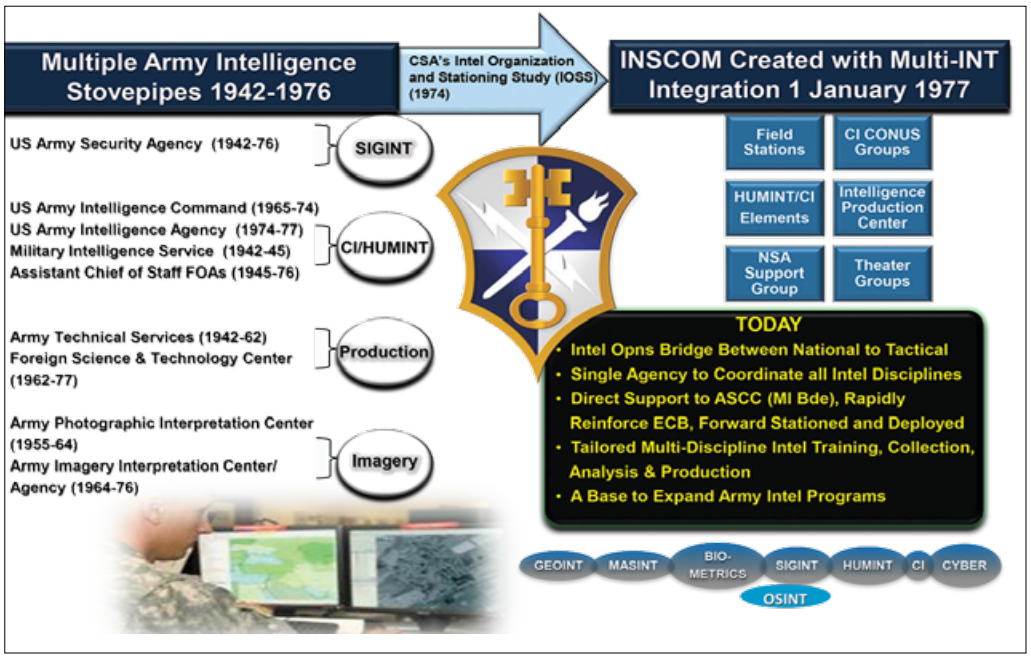


Figure 1. Evolution of Army Intelligence

INSCOM's Role

INSCOM is the operational-level headquarters that manages echelons above corps Army intelligence assets and provides the downward support necessary to give tactical commanders the additional capability needed for the tactical fight. The operational level of war is described as the planning, conduct, and sustainment of large units to obtain strategic goals within a theater. History has proven that failure at the operational level of war will yield an inability to achieve strategic objectives, despite tactical successes. Operational commanders determine the sequence of actions over time and space that will produce the conditions necessary to achieve strategic objectives. To do this, the commander must constantly interact with the strategic level as he or she assesses the adversary and determines how best to employ tactical forces. It is this interaction between strategy and tactics that delineates the operational level of war. As the operational-level headquarters for the Army's intelligence enterprise, INSCOM synchronizes, shapes, resources, and reinforces intelligence efforts from the tactical fight to the strategic echelon.

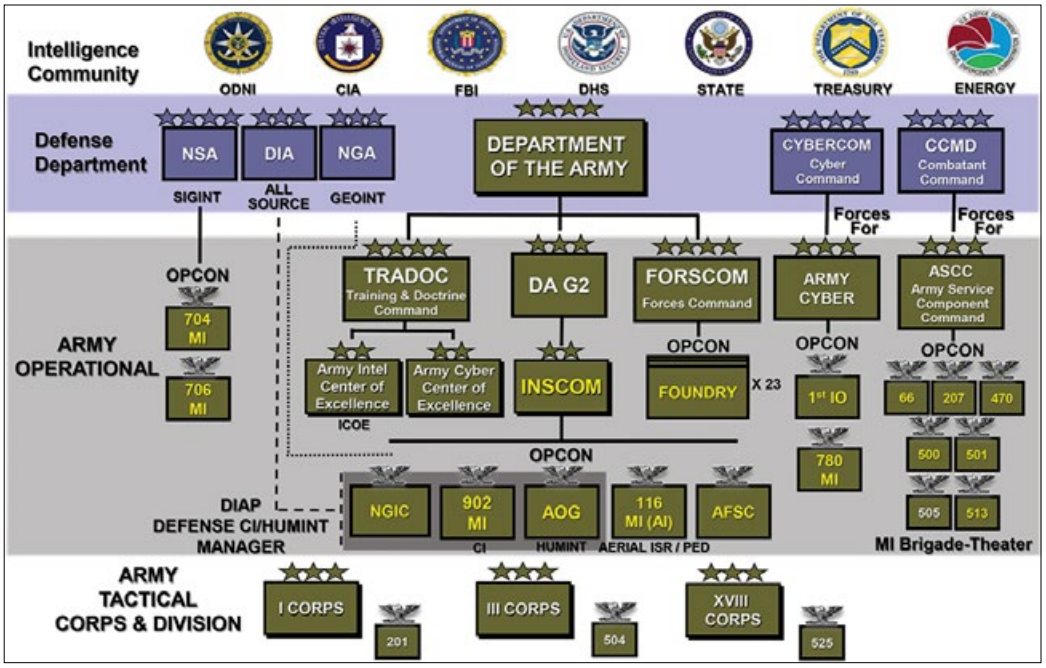


Figure 2. The Intelligence Enterprise—Where INSCOM Fits

As a direct reporting unit (DRU) to the Deputy Chief of Staff, G-2, INSCOM is uniquely positioned to provide operational support to the Army's regional and expeditionary activities, the institutional Army, the joint force, and the U.S. intelligence community. INSCOM—

- Exercises mission command of multidiscipline intelligence and security forces.
- Delivers linguist support.
- Provides advanced intelligence skills training through Foundry.
- Coordinates the acquisition, logistics, communications, and other specialized capabilities that enable the enterprise to function.

INSCOM has a general support relationship with the entire Army by virtue of its DRU designation, providing the operational support functions that are not otherwise available. In other words, INSCOM synchronizes several Army and Department of Defense (DoD)-level activities (such as the Contract Linguist and Intelligence Program) and the capabilities of its brigades on behalf of the broader intelligence enterprise to support maneuver commander requirements.

Figure 2 shows how INSCOM enables multi-domain operations by serving as a bridge within the intelligence enterprise, from capabilities resident in national defense agencies, while supporting laterally and downward across the Army.

Figure 3, on the next page, depicts the tasks, functions, and missions INSCOM conducts and synchronizes on behalf of the broader enterprise.

Organization to Support the Broader Enterprise

INSCOM consists of 17 major subordinate commands (MSCs). All of INSCOM's MSCs are organic to INSCOM for the purposes of Army force structure management. INSCOM exercises a specific type of command authority over them all, commonly referred to as administrative control (ADCON), which encompasses the responsibility to man, train, and equip these units.

Figure 4, on page 8, shows the breakout of INSCOM's subordinate commands that are operational control (OPCON) to other commands/organizations and those subordinate commands for which INSCOM retains OPCON. The light blue icons represent non-INSCOM, echelons above corps, Reserve Component, and National Guard military intelligence (MI) units for which INSCOM supports the U.S. Army Forces Command (FORSCOM) in enabling their readiness.

Ten of INSCOM's MSCs are assigned to U.S. combatant commands or have been placed under the OPCON of other commands or organizations. Six of these units are the military intelligence brigades-theater (MIB–Ts).[2] Each MIB–T is

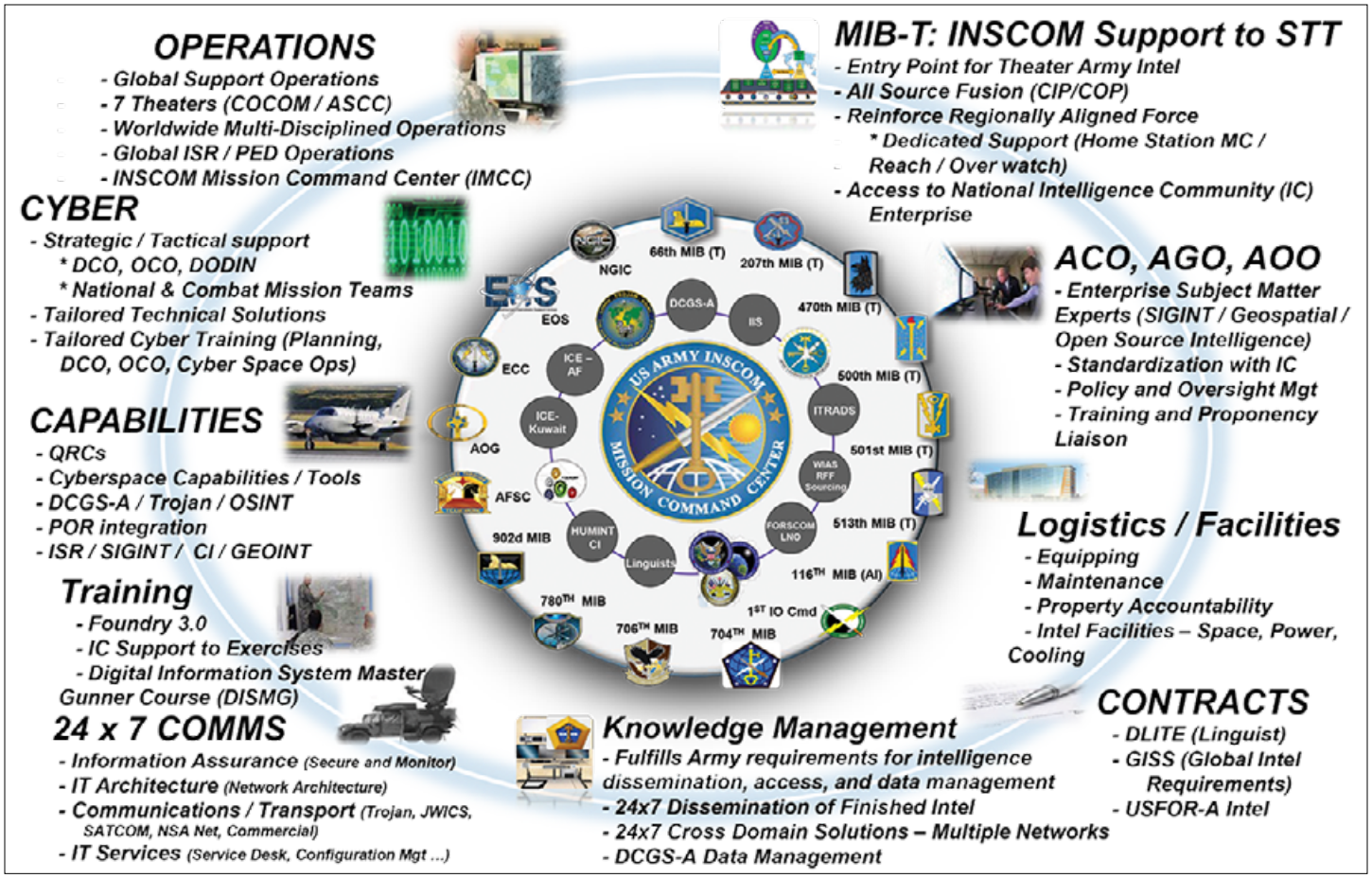


Figure 3. INSCOM Enterprise Support

unique in its organization, capabilities, and capacities—tailored to its theater's enduring requirements and relative prioritization within the Defense Planning Guidance. Their mission is to set the theater through phase 0 and phase 1 intelligence activities. They provide regionally focused collection and analysis in support of the theater army's daily operations requirements and specific joint operations in their respective ground component commander's area of responsibility (AOR). By tying the brigade to a geographic area, the MIB–T serves as the subject matter expert for that region and possesses capabilities specific to that AOR. Where regionally aligned forces or a maneuver unit may be new to the mission or theater due to changes in the Global Force Management Allocation Plan, the aligned MIB–T will have been part of the theater mission for a long time and can serve as an "anchor point" to support, train, and integrate FORSCOM intelligence units into the theater.

INSCOM's two signals intelligence (SIGINT) brigades, the 704th and 706th MI Brigades, are the Army's contribution to the National Security Agency (NSA)-Washington and NSA-Georgia, respectively. Combined they perform a variety of tasks on behalf of the Army such as technical SIGINT collection, reporting, and analysis, and language dialect training. The European Cryptologic Center and Expeditionary Operations Support Group provide vital SIGINT support to global operations. Additionally, INSCOM's 780th MI Brigade serves as the U.S. Army Cyber Command's action arm, creating operational effects in and through cyberspace. The 1st Information Operations (IO) Command provides IO and cyberspace operations through deployable teams, planning, analysis, and special training in order to support freedom of action in the information environment and denies the same to adversaries.

In addition to the 10 ADCON brigades, INSCOM has 5 functional brigades:

- National Ground Intelligence Center (NGIC).
- 116th Aerial Intelligence Brigade.
- 902nd Military Intelligence Group.
- Army Operations Group (AOG).
- Army Field Support Center (AFSC).

Each functional brigade performs tasks, functions, and missions that no other Army intelligence unit performs in general support to the Army, intelligence community, and joint task force. These brigades provide unique capabilities.

NGIC is the DoD center for foreign ground forces analysis, managing a variety of functions that directly support

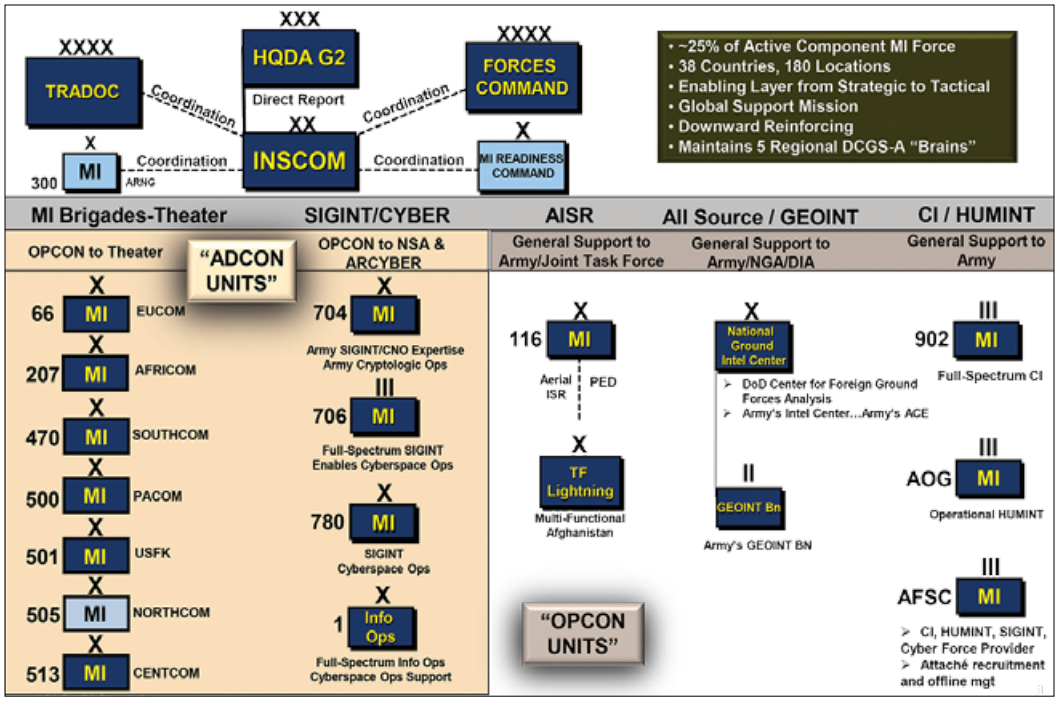


Figure 4. INSCOM's Organization

the warfighter. Its Army foreign materiel program, chartered to acquire and exploit all foreign ground weapon systems and rotary-wing helicopters, primarily conducts threat assessments and countermeasure development to help maintain our technological advantage on the battlefield.

The 116th is the Army's only aerial-intelligence, surveillance, and reconnaissance brigade, equipped to provide real-time processing, exploitation, and dissemination (PED) in support of ground operations. The 902nd is the Army's lead to protect our forces and technologies from insider threats and foreign intelligence exploitation; it is also the Army's only action arm equipped to conduct unique operations in the cyberspace domain that routinely produce actionable intelligence for ground forces. AOG produces human intelligence required to answer the Chief of Staff of the Army's priority intelligence requirements, and AFSC serves as a force provider and manager of many of these specialized capabilities. In essence, the functional brigades answer specific intelligence gaps—unaddressed by others within the intelligence community—to produce vital intelligence that enables ground operations.

Integration of Capabilities

The INSCOM headquarters brings all of these intelligence capabilities to bear in an integrated manner to provide agile trained and ready capabilities to respond to the Army's requirements. INSCOM serves as the Army's only intelligence organization postured to perform functions that military intelligence units and staffs at echelon cannot do effectively by themselves due to limited resources. This allows the INSCOM staff to bridge intelligence-related capability gaps, giving commanders at echelon a tailored set of capabilities at the right time to set conditions for success across operational environments.

For example, before deployment, the INSCOM staff sustains and administers advanced skills training via geographically dispersed Foundry platforms to intelligence Soldiers in INSCOM and FORSCOM units. The G-6 and the Ground Intelligence Support Activity provision the Joint Worldwide Intelligence Communications System, the military intelligence SECRET Internet Protocol Router Network, and the Nonsecure Internet Protocol Router Network domains, as well as the TROJAN family of capabilities that connect warfighters to intelligence databases, products, and tools. At Combat Training Center rotations or equivalent certifications, INSCOM may augment rotational units with specialized collection assets to enhance training—many of which are capabilities and technologies that the INSCOM G-7 team has developed.

During deployments, INSCOM headquarters manages echelons above corps intelligence personnel, equipment, architecture, and aircraft to support the DoD Global Force Management Allocation Plan. To enable capabilities such as on-site and intelligence reach PED, members from across the staff provision necessary architectures while the G-4 staff plans, sustains, and maintains Army operational intelligence systems and facilities. INSCOM maintains the agility to fill the ranks of deployed forces to ensure that expeditionary-MI brigade, brigade combat team, or joint task force personnel requirements are met with capable and trained intelligence Soldiers at a moment's notice.

Upon redeployment of a combat unit, the MIB–Ts remain on mission, prepared to support the next deploying unit. To maintain its readiness, the INSCOM staff administers "set the theater" exercises to validate brigades' abilities to execute shape and prevent intelligence tasks, which set conditions for prevailing in large-scale combat operations and consolidating gains. These exercises help refine the intelligence warfighting function support to regional

operation plans, and identify doctrine, organization, training, materiel, leadership and education, personnel, and facilities requirements, which will contribute to modernization efforts. Throughout deployment cycles, the INSCOM Mission Command Center operates continuously to maintain situational awareness of the global landscape so that we can ensure the Army's regional and expeditionary activities, the institutional Army, and the joint force are adequately equipped with the intelligence capabilities needed to meet current and projected requirements in the ever-changing threat environment. The command's ability to execute cross-boundary mission command is a critical capability we deliver, maintaining the resources, authorities, and agility to react to emerging demands that cannot be performed elsewhere.

Conclusion

INSCOM headquarters and its brigades synchronize, shape, resource, and reinforce finite intelligence resources with a set of highly skilled, trained intelligence professionals who offer direct and reinforcing support to commanders at all levels. INSCOM is a force fully engaged from the tactical to the national level. With more than 11,000 Soldiers, Civilians, and contractors committed to the combatant commands supporting contingency and combat operations, INSCOM formations are always ready and always vigilant. We maintain constant readiness to meet the challenges our Nation and Army will face in the future.

Endnotes

1. Bonnie Heater, "TRADOC general talks of changes," *U.S. Army Worldwide News,* February 26, 2016, https://www.army.mil/article/163074/tradoc_general_talks_of_changes.

2. The 505th Military Intelligence Brigade is the Army's seventh military intelligence brigade-theater, which falls within the U.S. Army Reserve Military Intelligence Readiness Command under the U.S. Army Reserve Command and U.S. Army Forces Command.

MG Christopher S. Ballard became the Commanding General, U.S. Army Intelligence and Security Command (INSCOM), on 27 June 2016. MG Ballard has commanded at the company, battalion, and brigade levels with combat tours in Iraq and Afghanistan as a battalion commander and combined/joint principal intelligence staff officer. His commands include Headquarters Company, 125th Military Intelligence Battalion; 312th Military Intelligence Battalion and Operation Iraqi Freedom; and 500th Military Intelligence Brigade. The Chief of Staff of the Army recently selected MG Ballard to become the Deputy Director, Signals Intelligence Directorate, National Security Agency, at Fort Meade, MD. MG Ballard holds a bachelor's degree in political science and German from Furman University, a master's degree in international relations from Indiana University, and a master's degree in National Security and Strategic Studies from the National War College.

COL Nichoel E. Brooks is the Director of the Commander's Action Group at INSCOM. She entered the Military Intelligence Corps after earning her commission through the Officer Candidate Program, where she graduated as the distinguished military graduate. Before joining INSCOM, she served as the Director of Intelligence (J-2), Special Operations Joint Task Force-Afghanistan. Her previous command positions include Deputy Commander, INSCOM; Commander, National Ground Intelligence Center; Commander, 310th Military Intelligence Battalion; Intelligence Company Commander, 3rd Armored Cavalry Regiment; Detachment Commander, 308th Military Intelligence Battalion, 902nd Military Intelligence Group; and Counterintelligence Platoon Leader, A Company, 163rd Military Intelligence Battalion, 504th Military Intelligence Brigade.

LTC Jarred M. Lang, a fixed-wing Army aviator, is the Commander of the 206th Military Intelligence Battalion (AE) and is currently serving as the Commander of Headquarters, Task Force Observe, Detect, Identify, and Neutralize (ODIN) in Afghanistan. He has deployed six times to the U.S. Central Command (CENTCOM) area of responsibility (AOR), three times in leadership roles in Task Force ODIN in Iraq or Afghanistan.

MAJ Christopher D. Thornton is a military intelligence officer serving as the Executive Officer for the 206th Military Intelligence Battalion (AE), operating in Afghanistan as Headquarters, Task Force ODIN. He previously served in a variety of intelligence assignments, including Detachment S-3 (FWD) for Army Joint Surveillance Target Attack Radar System in the CENTCOM AOR. He is currently on his fifth deployment.

CPT Charles F. Nadd entered active duty in 2011 upon graduation from the U.S. Military Academy. His first assignment after flight school was with the 3rd Battalion, 10th Combat Aviation Brigade, where he served as Battalion Assistant S-3, Forward Battalion Battle Captain (Afghanistan), and UH-60 Flight Platoon Leader. Following completion of the Military Intelligence Captain's Career Course, he was assigned to the 204th Military Intelligence Battalion (Aerial Reconnaissance) and served as the Battalion S-4. He has completed a tour in Afghanistan supporting Operation Enduring Freedom. CPT Nadd has a bachelor of science with honors in political science and history.

CPT Gretchen L. Pace is the Deputy Director of the Commander's Action Group at INSCOM. She attended the University of Virginia where she participated in the Reserve Officer Training Program and commissioned as a military intelligence officer in 2011. Upon completion of the Basic Officer's Leaders Course, she served as a Signals Intelligence Platoon Leader in the 1st Brigade Special Troops Battalion, 1st Armored Brigade Combat Team, at Camp Hovey, Korea. Her additional assignments include Military Intelligence Company Executive Officer, 1st Infantry Division; and Joint Intelligence Support Element Targeting Officer, Special Operations Joint Task Force-Afghanistan.

Mr. Thomas J. Stokowski has been a senior planner on the INSCOM staff since 2006. Before that, he served for more than 23 years as an Army intelligence officer with a dual specialty in all-source and signals intelligence with assignments in the 82nd Airborne Division, 6th Infantry Division, U.S. Army Europe Headquarters, U.S. Army Training and Doctrine Command, and Army G-2 Staff.

The U.S. Army Intelligence and Security Command at Four Decades

1977 Part I: Inception 2018

by Mr. Michael E. Bigelow, INSCOM Command Historian

Established in 1977, the U.S. Army Intelligence and Security Command (INSCOM) emerged from a radical reorganization of Army intelligence. INSCOM continued the functions of its predecessor, the Army Security Agency (ASA), by exercising centralized control over a worldwide organization. Multidiscipline military intelligence (MI) brigades or groups remain INSCOM's primary means to support theater commanders. INSCOM provides tailored intelligence forces with specific, often unique, training and equipment to meet national and tactical requirements. INSCOM remains a fluid organization to allow its subordinate groups and brigades to deliver intelligence support to the Army in the field and provide a critical bridge between national agencies and theater forces.

In the aftermath of the Vietnam War, the U.S. Army reorganized almost its entire institutional and training headquarters to streamline important administrative functions while improving operational effectiveness. In late 1974, the Army cast its eyes on Army intelligence to see if it was effectively organized and efficiently managed. The instrument of this scrutiny was the Intelligence Organization and Stationing Study (IOSS), a panel of senior officers headed by MG James J. Ursano. Released in mid-1975, the IOSS report recommended that the Army break up existing intelligence organizations and reassemble them into a new configuration. These recommendations led to the most sweeping reorganization of Army intelligence in a generation.

At the center of this transformation, the Army established a single intelligence command to control an integrated, worldwide structure that provided multi-intelligence support to the Army theater commanders. ASA, the Army's signals intelligence (SIGINT) organization, was the cornerstone of this new command. To better align itself to the new Army structure, ASA transferred its training, development resources, and logistics organization to other Army commands. In addition, ASA's tactical SIGINT units were reassigned to the divisions or corps they supported.

On 1 January 1977, ASA was redesignated as INSCOM. The new command merged ASA's remaining SIGINT assets with counterintelligence (CI) and human intelligence (HUMINT) assets of the U.S. Army Intelligence Agency, and was formally established as a multidisciplined intelligence organization on 1 October 1977 with its headquarters at Arlington Hall Station, Virginia. With MG William I. Rolya as its first commanding general, it provided the Army with multidiscipline intelligence and security at the echelons above corps and controlled diverse assets around the world.

U.S. Army photo courtesy of INSCOM Public Affairs Office

Arlington Hall

To support the Army's overseas theaters, INSCOM relied on multidiscipline MI groups stationed abroad that were tailored to meet theater-specific requirements, with each group varying in size and composition. By mid-1978, INSCOM had four such units:

- The relatively small 470th MI Group in Panama, supporting U.S. Army South and its infantry brigade.
- The large 66th MI Group in West Germany, supporting U.S. Army Europe and its two corps.
- The 501st MI Group in South Korea, supporting the U.S. Eighth Army, included INSCOM's only aerial exploitation unit, the 146th ASA Company.
- The 500th MI Group in Japan, which focused primarily on HUMINT.

Photo courtesy of Roger Corman

MG William I. Rolya

Through these four units, INSCOM furnished intelligence resources and support to Army field commanders.

INSCOM offered general support to the Army with three single-discipline MI groups in the United States. The 902nd MI Group handled both CI and signal-security support missions throughout the continental United States (CONUS). The CONUS MI Group commanded the Soldiers who worked with the National Security Agency and administered a readiness program, which allowed SIGINT Soldiers to train technical skills against real-world threat targets. The last of these stateside groups was the Army Operational Group, which coordinated HUMINT collection and supported the overseas MI groups.

To meet national requirements, INSCOM controlled a number of fixed field stations. These stations were located around the world: two in West Germany (Augsburg and Berlin), two in Japan (Okinawa and Misawa), one in Turkey (Sinop), and one in South Korea. Two sites were in CONUS (Key West, Florida, and San Antonio, Texas). In late 1980, INSCOM established a new field station, the first since the Vietnam War, in Kunia, Hawaii. All the field stations varied in size and mission, but all used sophisticated equipment to monitor current and potential threats.

INSCOM steadily expanded and acquired new missions. With the production assets it had gained, INSCOM established a unified production element, the Intelligence and Threat Analysis Center, on 1 January 1978. Later, it assumed control over the U.S. Army Russian Institute in West Germany. When MG Rolya changed command, INSCOM had established a framework for elements of the Army's intelligence system to cross-cue one another, resulting in a collective, enterprise-like effort. The command had become the centerpiece of the Army's intelligence organization.

Mr. Michael E. Bigelow has served as the Command Historian for the U.S. Army Intelligence and Security Command (INSCOM) since 2006. He received a bachelor of arts in history from Colorado State University and a master of arts in military history from Temple University. He has written numerous articles for military publications such as Military Review *and* Military Intelligence Professional Bulletin. *Before becoming INSCOM's Command Historian, he served as an active duty military intelligence officer for 22 years.*

Seeing the Elephant: INSCOM's Exercise of Mission Command

by Lieutenant Colonel Ryan H. Beery

Introduction

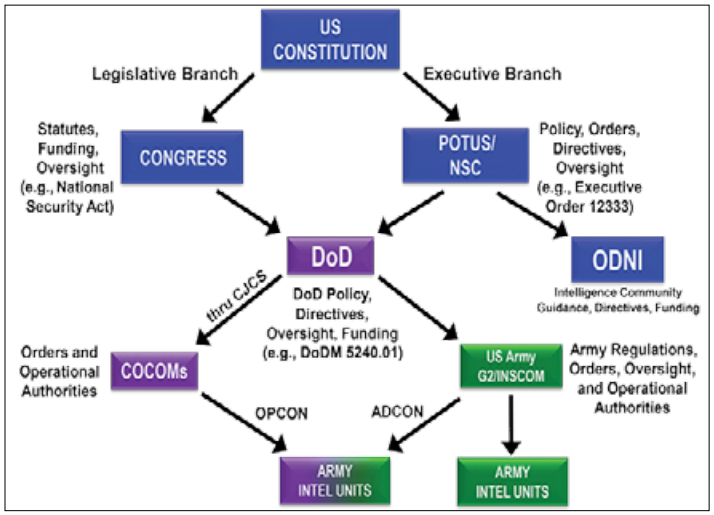
In the parable of the blind men and the elephant,[1] a group of blind men encounter an elephant for the first time and ask, "What is this creature?" Each man touches a different part of the elephant—the trunk, tusks, feet, tail, and ears—and then describes the elephant based on his experience. Their search for consensus quickly devolves into argument, with each going his separate way in frustration. No one understood that, although different, each individual impression was accurate, and together the impressions described a complex creature.

Like the elephant in the parable, few can see the whole of the U.S. Army Intelligence and Security Command (INSCOM) because most are only acquainted with a part of it, which may bear little resemblance to its other parts. Some may describe INSCOM as the blind men did, taking a portion for the whole, leading to a misunderstanding about the purpose and strength of INSCOM.

In order to execute its Army, Department of Defense (DoD), and intelligence community responsibilities, INSCOM exercises a variety of command, administrative, and support relationships across the Army intelligence enterprise. Since each relationship is predicated on a specific INSCOM function or responsibility, these relationships may seem like the description of a distinct part of an elephant. But, by taking a step back, one can see how INSCOM leverages and synergizes the network of relationships and authorities into a single powerful, composite organization.

What is INSCOM?

To understand INSCOM's purpose, one must understand the source of the organization's authorities:



Intelligence Authorities

Executive Order 12333, *United States Intelligence Activities*

Authorizes the Secretary of the Army (SECARMY) to collect (including through clandestine means), produce, analyze, and disseminate defense and defense-related intelligence and counterintelligence (CI) to support departmental requirements, and, as appropriate, national requirements; and to conduct CI activities. Through the 381-series of Army Regulations (ARs) and AR 10-87, *Army Commands, Army Service Component Commands, and Direct Reporting Units*, the SECARMY established a framework for executing these Executive Order (EO) 12333 responsibilities.

This framework distinguishes the differences in scope and responsibility for various Army organizations. The SECARMY directs INSCOM as a direct reporting unit of the Deputy Chief of Staff of the Army, G-2 (DCS, G-2). Direct reporting units provide broad, general support to the Army in a normally single, unique discipline not otherwise available in the Army.

AR 10-87, *Army Commands, Army Service Component Commands, and Direct Reporting Units*

AR 10-87 specifies INSCOM's mission:

- Execute mission command of operational intelligence and security forces.
- Conduct and synchronize worldwide multidiscipline and all-source intelligence and security operations.
- Deliver linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities in support of Army, joint, and coalition commands and the U.S. intelligence community.
- Provide National Intelligence Program support to the intelligence community, combatant commands (CCMDs), and Army organizations.

To fulfill this mission, the regulation tasks INSCOM with 28 distinct functions, many of which require multiple subtasks to execute. These tasks are wide-ranging and include—

- Carrying out Army responsibilities for training, supplying, and equipping.
- Serving as a force provider to CCMDs.

- Executing service intelligence authorities.
- Accomplishing security support functions for the Army.
- Operating and sustaining military intelligence information technology for the Army and the interorganizational and multinational partners.

Overview of Command Relationships and Authorities

INSCOM exercises command relationships in accordance with joint doctrine[2] and exercises administrative control (ADCON) on behalf of the SECARMY. INSCOM also routinely enters into coordination and support relationships with other Army commands, DoD agencies, and intelligence community members. These coordination relationships exist through a combination of direct liaisons and memoranda of agreement (MOAs) or memoranda of understanding (MOUs). INSCOM also has service-derived "operational" intelligence authorities that do not fit into traditional doctrinal lines between service authorities and CCMD authorities.

Administrative Control (Army Authority and Responsibilities)

INSCOM, under the supervision of the Army DCS, G-2, is responsible to the SECARMY for the execution of assigned responsibilities contained in Title 10 of the United States Code (U.S.C.) section 3013(b) in support of INSCOM forces worldwide. Commonly referred to as Title 10, service, or ADCON responsibilities, 10 U.S.C. section 3013(b) provides the SECARMY with authority to execute the responsibilities and functions of the Department of the Army, to include equipping, training, servicing, maintaining, administering, and organizing the Army.

Shared Administrative Control

Under AR 10-87, shared ADCON is the internal allocation of 10 U.S.C. section 3013(b) responsibilities and functions between Army organizations over Army personnel and units. INSCOM, for example, shares ADCON responsibilities over its military intelligence brigades-theater (MIB–Ts) with Army service support commands and/or installation and garrison commands. Both mission and geography influence the specific division of shared ADCON responsibilities.

Combatant Command Authority

The combatant command (command authority) (COCOM) is a nontransferable command authority of a combatant commander (CCDR) to perform those functions of command over assigned forces that involve—

- Organizing and employing commands and forces.
- Assigning tasks.
- Designating objectives.
- Giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command.

Operational Control

Inherent in COCOM is operational control (OPCON), the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. A CCDR can delegate OPCON to commanders of subordinate organizations (i.e., those units assigned to the CCMD). Although INSCOM does not possess COCOM or OPCON authorities, it is a force provider of Army intelligence forces that operate under the COCOM authority of the CCDRs and, as delegated, the OPCON of the Army Service component commands (ASCCs), with whom it shares ADCON responsibility.

Service Intelligence Authorities

In EO 12333, the President directed the intelligence and CI elements of the Army to—

- Collect, produce, analyze, and disseminate defense and defense-related intelligence and CI to support Army requirements, and, as appropriate, national requirements.
- Conduct CI activities.
- Monitor the development, procurement, and management of tactical intelligence systems and equipment and conduct related research, development, and test and evaluation activities.
- Conduct military intelligence liaison relations and military intelligence exchange programs with selected foreign defense establishments and international organizations.

Under DoD Instruction 5240.10, *Counterintelligence (CI) in the Combatant Commands and Other DoD Components,* the military services alone have the authority to conduct CI investigations, while the CCMDs and defense agencies are prohibited from conducting such investigations.

These service intelligence responsibilities are executed by what is colloquially described as "service OPCON" (technically a type of ADCON because it is the exercise of SECARMY authorities, provided by the President to SECARMY in EO 12333). However, since the execution of these responsibilities appears more akin to operational mission command, i.e., OPCON, it is helpful to describe it as "service OPCON" to distinguish it from the traditional "man, train, and equip" ADCON responsibilities.

Under these service intelligence authorities, executed on behalf of SECARMY and DCS, G-2, INSCOM provides worldwide operational oversight, synchronization, coordination, and technical authority of all Army CI and human intelligence (HUMINT) activities.

Support Relationships

Support is a command authority established by a common superior commander between subordinate commanders when one organization is directed to aid, protect, complement, or sustain another force. Within the Army, INSCOM has been directed to provide support to multiple organizations. INSCOM, for instance, is in support relationships with a number of DoD agencies, including the National Security Agency/Central Security Service (NSA/CSS).

Direct Liaison Authorized

Direct liaison authorized (DIRLAUTH) is the authority to directly consult or coordinate an action with another command or agency. DIRLAUTH is a coordination relationship, not an authority, through which command may be exercised. Under AR 10-87, INSCOM has broad DIRLAUTH, allowing it to coordinate directly with Army commands; ASCCs; other direct reporting unit commanders; Headquarters, Department of the Army; other DoD headquarters and agencies; and other foreign and domestic government departments. Since INSCOM supports a multitude of these commands and agencies, DIRLAUTH is critical to accomplishing INSCOM's broad and diverse mission sets.

Memoranda of Agreement or Understanding

Like DIRLAUTH, MOAs and MOUs[3] do not create command relationships or authorities; they only detail how each party will exercise its responsibilities in relation to the other. INSCOM makes extensive use of MOAs and MOUs with other Army commands, DoD agencies, intelligence community partners, and other government agencies. Common subject matters for MOAs and MOUs between organizations are the delineation of ADCON responsibilities and financial reimbursement.

Relationships within the Army

INSCOM has relationships within the Army to support operations in the areas of CI, HUMINT, open-source intelligence (OSINT), and multiple intelligence projects.

Department of Army CI Operations

The Army and the CCMDs both exercise CI authorities; however, the Army exercises some CI authorities exclusively (i.e., investigation authority) in support of both the Army and the designated DoD components.[4]

Through the 902nd Military Intelligence Group (MIG), INSCOM provides CI support globally and domestically to the Army and to designated DoD components. Support includes counterespionage; support to force protection; support to research, development, and acquisition activities; and cyberspace CI. The 902nd MIG's primary functions include investigations, operations, collection and reporting, analysis, production, and other activities.

These CI support responsibilities require INSCOM to coordinate across the Army and with the supported DoD components. INSCOM must also maintain close liaison relationships with the Federal Bureau of Investigation (FBI), other service CI agencies, Army Criminal Investigation Command, and local U.S. Attorneys' offices to ensure proper information sharing, operational coordination, and determination of investigative responsibility for Army CI cases. These liaison relationships support joint investigations with the FBI and potentially criminal prosecution through the local U.S. Attorney. Thus, INSCOM's ability to conduct direct liaison with these commands and agencies on both a recurring and a specific basis is essential to providing timely and effective CI support across the Army and DoD.

Department of Army HUMINT Source Operations

Army HUMINT overt and clandestine source operations are executed through INSCOM by the Army Operations Group. While Army HUMINT primarily focuses on collecting information against validated Army collection requirements, Army HUMINT collectors are not prohibited from collection against other intelligence requirements, including national intelligence requirements. This permissive mission set requires coordinating relationships with multiple intelligence organizations in the DoD and intelligence community, formalized in MOAs and MOUs or by direct liaison.

Project Manager

INSCOM manages multiple intelligence projects, including Army HUMINT support to the NSA/CSS, the Army Cover Program, the Intelligence Polygraph Program, the Force Protection Detachment Program, the Technical Surveillance Countermeasures Program, the Army CI Cyber Program, and the Joint Terrorism Task Force Program. These projects require INSCOM to establish relationships, pursue acquisition solutions, and manage each project within the Army, DoD, and intelligence community.

Program Manager

INSCOM serves as the Army program manager for four major intelligence programs. All four programs are essential to Army intelligence and CCMD operations, and support users down to the tactical level. Given this breadth in both scope and user base, these programs bring INSCOM into relationships with commands and agencies across the Army and DoD.

- **DoD Executive Agency for Linguist Support**. For DoD, INSCOM administers the multibillion-dollar DoD Language Interpretation and Translation Enterprise Contract portfolio to fulfill the Army's executive agent responsibilities for providing contract linguist support services to all DoD components. The INSCOM Contract Linguist and Intelligence Program Support Office (CLIPSO) serves as the single point of entry for all contract linguist requirements validated and resourced under executive agent authorities. CLIPSO and INSCOM are routinely involved in discussions with DoD, CCMDs, ASCCs, and joint task forces on linguist support requirements.
- **Military Intelligence Information Technology.** INSCOM operates, sustains, and secures the military intelligence information technology operational platform in support of Army and joint, interorganizational, and multinational mission partners. This includes managing and coordinating all ground intelligence support activities worldwide, and maintaining the information technology backbone for classified network systems. INSCOM's information technology responsibilities require enduring relationships with Army Cyber Command (ARCYBER) and its subordinate Army Network Command; the Army Chief Information Officer, G-6; the NSA/CSS; and the Defense Information Systems Agency.

- **TROJAN Program.** At the direction of the DCS, G-2, INSCOM executes the TROJAN Program that provides communications support and collection capabilities for the intelligence warfighting function down to the tactical level. INSCOM's responsibility for TROJAN includes worldwide logistics sustainment support to all non-program of record TROJAN users.
- **Army Sensitive Compartmented Information Oversight.** INSCOM provides centralized sensitive compartmented information (SCI) contract security oversight and support to senior intelligence officers across the Army enterprise and at unified commands in the execution of SCI contract actions. It also supports the development of Armywide SCI industrial security policy and training programs.

Capability Development

INSCOM is an Army capability developer for operational-level and expeditionary intelligence systems, including measurement and signatures intelligence, offensive cyberspace, and special-purpose electronic attack systems. INSCOM represents the Army's equities in national signals intelligence (SIGINT) systems development. As such, INSCOM coordinates with pertinent commands, agencies, acquisition organizations, and industry partners to execute its capability development functions.

Training

Beyond its inherent ADCON training responsibilities for Army intelligence personnel, INSCOM executes the Army's Foundry Intelligence Training Program. Management of the Foundry Program requires coordination with U.S. Army Forces Command (FORSCOM), Training and Doctrine Command, ASCCs, and U.S. Army Reserve and National Guard intelligence units that train under the Foundry Program.

Army Open-Source Intelligence Office

Under Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities*, INSCOM established the Army Open-Source Intelligence Office (AOO) to fulfill its Armywide responsibility as the operational proponent for OSINT, including training and equipping all Army OSINT users. As trainer and equipper, INSCOM supports commands throughout the Army. To fulfill its development responsibilities, the AOO must maintain close relationships with the Defense Intelligence Agency, the ASCCs, the special operations community, and the intelligence community.

Security

Despite centralization of adjudication responsibilities for personnel security clearances at the DoD Central Clearance Facility, INSCOM still oversees Army submissions of personal background investigations for security clearance, Federal employment, and common access card credentialing decisions. INSCOM also has growing security responsibilities for the Army in operating the Army Security Vetting Enterprise and supporting the Army's Insider Threat Program:

- **Army Security Vetting Enterprise.** This vetting enterprise identifies potential insider threats connected to terrorist organizations or foreign intelligence services that attempt to gain access to Army personnel, facilities, or information systems. The Army's demands on this enterprise have been growing, requiring relationships with multiple Army commands needing this support, and coordination within DoD and other government agencies to perform vetting functions.
- **Army's Insider Threat Program.** INSCOM's role in the Army's Insider Threat Program is another area of recent growth. The INSCOM Security Operations Center (ISOC) is a spoke in the Army's insider threat hub, supporting command responses to security-related insider threat triggers, providing training to the Army community, and providing potential CI leads to the Army Counterintelligence Coordination Authority for CI investigation. The ISOC helps train and support local security managers across the Army. This emerging role is creating new relationships between INSCOM and the rest of the Army—from enduring training relationships with other commands to direct liaison between the ISOC and a command's security manager in identifying and responding to potential security issues under that command's purview.

Information Operations Support

INSCOM maintains ADCON over the 1st Information Operations Command (1st IO CMD). Through 1st IO CMD, INSCOM provides intelligence and intelligence-related support to information operations (IO) support teams, IO vulnerability assessments, IO-related training, and the Army operations security support element. In fulfilling these responsibilities, 1st IO CMD maintains relationships with the combat training centers, ARCYBER, and other Army commands.

Army Cyber Command Support

Beyond cyberspace-tool capability development, INSCOM maintains a relationship with ARCYBER to operate, sustain, and secure the top secret/SCI portion of the military intelligence information technology operational platform in support of Army and joint mission partners.

U.S. Army Forces Command and U.S. Army Reserve

INSCOM maintains a coordinating relationship with the U.S. Army Reserve Military Intelligence Readiness Command (MIRC). Since MIRC is a major subordinate command of U.S. Army Reserve Command, which is itself subordinate to FORSCOM, INSCOM must maintain relationships with all three organizations. The goal of these relationships is to ensure shared intelligence readiness responsibilities for those MIRC service-retained military intelligence units that functionally align to provide Reserve Component capacity to like-type INSCOM subordinate commands. INSCOM also maintains a coordinating relationship with FORSCOM to integrate MIRC units into the Army intelligence enterprise, ensuring readiness to meet Army and COCOM requirements.

Relationships with Combatant Commands

Due to multiple support responsibilities to the CCMDs and other DoD agencies, INSCOM and its major subordinate commands maintain command relationships with the COCOM and multiple DoD agencies. Since CCMDs also have HUMINT and limited CI authorities, INSCOM must coordinate, synchronize, and de-conflict both operational activities and collection management for Army HUMINT and CI with CCMDs, ASCCs, other military departments, and the intelligence community.

Force Provider to Combatant Commands

Through the Global Force Management Implementation Guidance (GFMIG), INSCOM's MIB–Ts are assigned to each geographic CCMD, except the U.S. Northern Command. INSCOM also provides U.S. Cyber Command with a large part of its assigned cyber mission force, through the 780th MIB-Cyber. These brigades serve as the "anchor points" for INSCOM, providing Army intelligence capabilities to support the CCMD and ASCC. The brigades are under the OPCON of their higher ASCC and COCOM of their GFMIG-assigned CCMD. These units operate under CCMD intelligence authorities and oversight to meet the CCMD's intelligence requirements.

Under AR 10-87, INSCOM maintains shared ADCON of all Army forces' GFMIG assigned to CCMDs. Depending on geography, the ADCON relationship for the MIB–Ts may be shared by two or more Army commands. For example, a MIB–T may have ADCON relationships with INSCOM, their assigned ASCC, and for some functions, a theater support command or installation senior commander. For geographically dispersed units, this may involve even more relationships. The specifics of ADCON functions vary based upon geography; thus, the ADCON relationships for the MIB–Ts are not uniform.

For example, 500th MIB–T, the INSCOM brigade that supports U.S. Army Pacific (USARPAC), has an OPCON relationship (through the U.S. Pacific Command's COCOM) and a shared ADCON relationship with USARPAC, as well as a shared ADCON relationship for Uniform Code of Military Justice (UCMJ) and adverse administrative actions with 8th Theater Support Command. And since one battalion is located in Japan, 500th MIB–T also has a shared ADCON relationship (including UCMJ) with U.S. Army Japan for that battalion.

Although AR 10-87 contemplates MOAs and MOUs specifying shared ADCON responsibilities, historical practice among the commands has been more informal, but formal documents are used for monetary support, services, or reimbursement issues. In general, INSCOM has responsibility over its intelligence units for personnel management functions such as awards, evaluations, assignments, and reliefs for cause. UCMJ actions are typically executed under the local General Courts-Martial Convening Authority with the MIB–T commander designated as the Special-Courts Martial Convening Authority. Investigations and adverse administrative actions can flow through either ADCON chain, but INSCOM typically handles matters relating to the execution of command- and intelligence-related matters. Most shared ADCON matters can be handled at the staff level without the need for command involvement. Agreements that are more formal are sometimes used to address contentious, novel, or recurring issues.

Aerial Intelligence

Through the 116th Aerial Intelligence Brigade, INSCOM coordinates, provisions, synchronizes, and executes the operational-level aerial intelligence, surveillance, and reconnaissance support to ASCCs and CCMDs. This relationship involves training and qualifying pilots of both manned and unmanned aircraft, along with logistical support and equipping of the aircraft.

INSCOM's support function goes far beyond being a force provider for Army aerial intelligence resources. INSCOM also coordinates, provisions, and synchronizes capabilities that enable the Army to meet expeditionary and home-station mission command, predominantly through the processing, exploitation, and dissemination (for the ASCCs and CCMDs) of intelligence gathered by INSCOM aircraft. With INSCOM as the mission command hub for Army aerial intelligence, it can surge both the collection and the analytical capability across CCMDs to meet emerging and dynamic aerial intelligence requirements.

Counterintelligence Support to DoD

DoD Instruction 5240.10 tasks Army CI as the supporting CI organization for multiple defense agencies, CCMDs, and field activity headquarters. INSCOM provides forces and executes mission command of Army CI capabilities to support the CI requirements of these organizations. The details of these support relationships are typically captured in an MOU or a support agreement between INSCOM and the supported DoD agency, activity, or command.

Relationships with the DoD Intelligence Community

Relationships with the DoD intelligence community extend to the NSA/CSS and the National Ground Intelligence Center (NGIC).

National Security Agency/Central Security Service

NSA/CSS is the lead U.S. Government agency for cryptology, including both SIGINT and information assurance.[5] INSCOM maintains a significant direct support relationship with NSA/CSS. Although NSA/CSS does not have command authorities like a CCMD, INSCOM's relationship with NSA/CSS is similar to that of an MIB–T with a CCMD, albeit with some important distinctions.

- **Mission Control.** The INSCOM Commanding General is the principal advisor to the Director, NSA/CSS, for U.S. Army cryptologic activities, and subordinate to the Director, NSA/CSS, for U.S. Army cryptologic activities in accordance with DoD Directive 5100.20, *National Security Agency/Central Security Service (NSA/CSS)*, and SIGINT directives. Since INSCOM is subordinate to NSA/CSS based upon these SIGINT directives, NSA/CSS exercises an OPCON-like authority, colloquially called mission control, over Army SIGINT and information assurance activities. The NSA/CSS is not a combatant or DoD command, so mission control is not technically COCOM or OPCON authority over INSCOM personnel. However, this mission control includes the authority to assign tasks, designate objectives, and give authoritative direction over training and all aspects of the NSA/CSS mission. Therefore, while not doctrinally OPCON, INSCOM conducts cryptologic activities under the mission control, direction, and authority of NSA/CSS.
- **Army Cryptologic Mission Command and Oversight.** The Commander, INSCOM, is designated as the Army Service Cryptologic Component commander, serving as the principal U.S. Army authority for all U.S. Army cryptologic activities, and retaining management oversight for cryptologic activities performed by the U.S. Army. The Commander, INSCOM, is also responsible for intelligence oversight of all Army SIGINT activities on behalf of the DCS, G–2. The Army Cryptologic Office (ACO) executes these responsibilities on behalf of the Commander, INSCOM, which requires ACO to maintain a close liaison relationship with NSA/CSS.

- **Force Provider.** INSCOM's 700-series brigades provide Army cryptologic personnel to NSA/CSS. However, since NSA/CSS is not a command, it does not exercise ADCON over INSCOM personnel. Thus, while these Army personnel work under NSA/CSS direction and authorities, INSCOM is solely responsible for ADCON responsibilities. This non-doctrinal relationship requires MOUs or MOAs to clarify roles and responsibilities between NSA/CSS and INSCOM, and continued liaison between the organizations.

National Ground Intelligence Center

INSCOM commands NGIC, the Army's Service Intelligence Center, which produces and disseminates all-source intelligence on conventional and irregular foreign ground forces' identities, networks, and ground-related weapon systems technologies. In performing this mission, NGIC supports multiple agencies in the DoD and national intelligence community, requiring INSCOM to establish relationships and partnerships with multiple agencies within the Army, DoD, and national intelligence community. These relationships include—

- Having a federated partnership with the Defense Intelligence Agency.
- Commanding the Army Geospatial Intelligence Battalion that supports the National Geospatial-Intelligence Agency.
- Leading the Army Program of Analysis that develops methodologies and standards to ensure Army intelligence products meet the needs of the Army, DoD, and national intelligence community.
- Managing the Army's Foreign Materiel Program.

NGIC also manages the national biometrically enabled watchlist, requiring relationships within the intelligence community and other Federal agencies.

Conclusion

As describing the parts of an elephant is the first step in understanding the elephant, describing INSCOM's functions and relationships is the first step in understanding INSCOM. Similar to the parable, the strength of INSCOM can only be understood when it is viewed as an interconnected organization, not as disparate entities.

INSCOM's numerous relationships should not be viewed as a checklist of unrelated tasks assigned by the SECARMY, but instead as the culmination of decades of building synergy and executing mission command across the Army intelligence enterprise. The combination of worldwide ADCON of INSCOM forces, oversight and "service OPCON" of Army intelligence authorities, and ability to conduct direct liaison and coordinate across the Army, DoD, and intelligence community enables INSCOM to command and synchronize Army intelligence forces. Understanding not just the parts but also how they join together is essential to understanding why INSCOM exists.

Endnotes

1. "Blind men and an elephant," Wikimedia Foundation, last modified 23 March 2018, at 23:18, https://en.wikipedia.org/wiki/Blind_men_and_an_elephant.

2. Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: U.S. Government Publishing Office [GPO], 25 March 2013). Change 1 was issued on 12 July 2017.

3. Department of Defense Instruction 4000.19, *Support Agreements* (Washington, DC: U.S. GPO, April 25, 2013). Change 1 was issued on November 30, 2017.

4. Department of Defense Instruction 5240.10, *Counterintelligence (CI) in the Combatant Commands and Other DoD Components* (Washington, DC: U.S. GPO, October 5, 2011). Change 1 was issued on October 15, 2013. This document provides a complete delineation of CI responsibilities between combatant commands and the Military Departments.

5. Department of Defense Directive 5100.20, *National Security Agency/Central Security Service (NSA/CSS)* (Washington, DC: U.S. GPO, January 26, 2010).

Thank you to COL Jonathan Howard, INSCOM SJA; Mr. Michael Wilding, INSCOM G-7; and Mr. Michael Banks, 704th MI Brigade, for their expertise in helping write this article.

LTC Ryan H. Beery was assigned to the U.S. Army Intelligence and Security Command, Office of the Staff Judge Advocate, in 2015 and currently serves as the Deputy Staff Judge Advocate. He was previously the Deputy Director of the Center for Law and Military Operations at The Judge Advocate General's Legal Center and School; and the Brigade Judge Advocate, 1st Brigade, 1st Armored Division. He is expected to report to U.S. Central Command in mid-2018 to be an operational legal advisor.

Intelligence and Security Command Mission Command

by Mr. Richard Harfst and Mr. Thomas Stokowski

Introduction

ADP 6-0, *Mission Command,* defines mission command as "the exercise of authority and direction by the commander," and that the exercise of mission command is "based on mutual trust, shared understanding, and purpose."[1] The U.S. Army Intelligence and Security Command (INSCOM), which executes mission command of the Army's operational intelligence force, applies these doctrinal tenets through authorities, associated responsibilities, resources, and organizational design.

INSCOM's structure consists of three categories of subordinate elements: the military intelligence (MI) brigades (MIBs), single-function units, and intelligence community support units; it synchronizes the elements' operations through staff organizations, functions, and facilities. It resources those elements through legal authorities prescribed in U.S. law and command relationships prescribed in Army regulations.

INSCOM uses the military intelligence brigade-theater (MIB–T) to distribute Army intelligence support to geographic combatant commands (GCCs), Army Service component commands (ASCCs), and regionally aligned forces. INSCOM uses functional intelligence commands and brigades aligned with national agencies to provide reinforcing, specialized expertise to warfighters and to deliver capabilities that underpin and empower the Army intelligence enterprise.

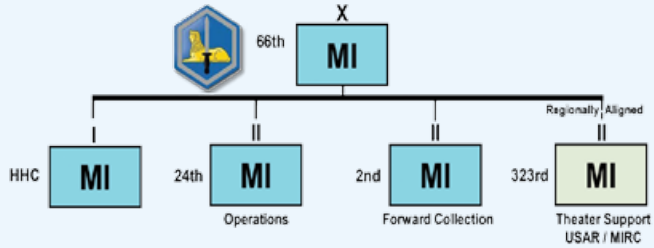
Military Intelligence Brigades-Theater

The MIB–Ts provide regionally focused collection and analysis in support of theater-level daily operations requirements and specific joint operations in the GCCs' areas of responsibility (AORs). Though tailored to the unique circumstances of their theaters of assignment, MIB–Ts share a common baseline design:

- A multicomponent brigade headquarters (composed of Regular Army and U.S. Army Reserve [USAR]).
- An operations battalion that serves as the ASCC G-2's analysis and control element (ACE) or ground intelligence center. The ASCC might also direct this battalion to send forward a task-organized deployable intelligence support element (DISE) as part of a theater command post or to support other theater land forces.
- A forward-collection battalion that may possess counterintelligence (CI), human intelligence (HUMINT), and ground signals intelligence (SIGINT) capabilities.
- A regionally aligned USAR MI battalion (theater support) from the Military Intelligence Readiness Command that is designed to provide surge capability to the MIB–T or other theater land force requirements.

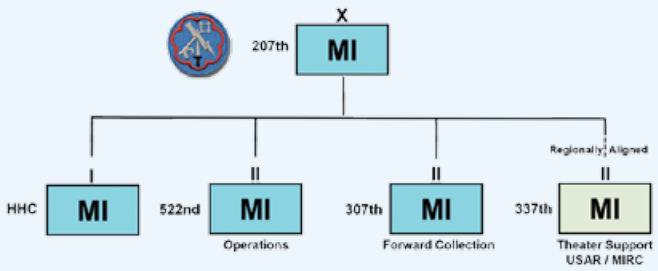
As the theaters' permanently assigned Army intelligence organization, the MIB–Ts provide the ASCCs with their foundational capacities to conduct phase 0 (Shape) and phase 1 (Deter) intelligence activities to set the theaters for the intelligence warfighting function. MIB–Ts serve as anchor points for land forces deploying to, operating in, or supporting the theaters via intelligence reach operations. They do this by supporting the ASCC G-2s in synchronizing and coordinating intelligence activities in their AORs. This includes providing enabling support and services that help units gain access to theater-specific data and integrate into the theater's intelligence architecture. It also assists in coordination of intelligence sharing and interoperability with allies and partner nations.

66th Military Intelligence Brigade



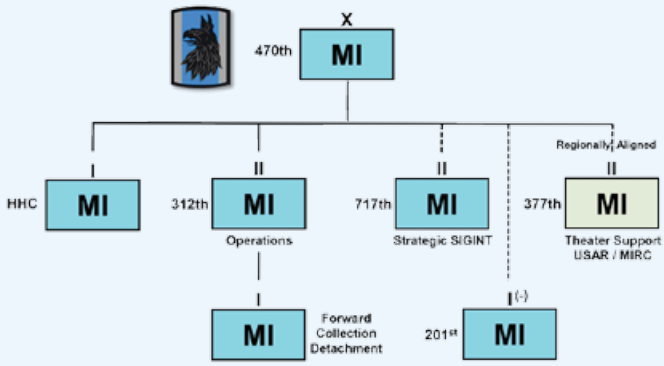
The 66th MIB–T conducts multidiscipline intelligence collection and analysis in the U.S. European Command (EUCOM) AOR in support of U.S. Army Europe (USAREUR) in order to protect U.S. forces, enable the North Atlantic Treaty Organization alliance, and set conditions for theater-level decision and action. The 66th MIB–T's active component elements are entirely forward-stationed in the European theater, and the brigade is organized according to the standard MIB–T design. Its 24th MI Battalion serves as the USAREUR G-2's ACE and can provide a task-organized DISE for USAREUR missions. The brigade's 2nd MI Battalion conducts theater-level multidiscipline (SIGINT, CI, and HUMINT) forward collection and exploitation in support of USAREUR and EUCOM requirements; on order, it deploys tailored expeditionary forces in support of USAREUR, EUCOM, and other combatant command unified land operations. The 2nd MI Battalion's CI support operations include staffing resident and day offices in 15 countries across EUCOM's AOR. The brigade's regionally aligned USAR MI battalion-theater support is located at Fort Meade, Maryland. The brigade also staffs and operates USAREUR's Foundry Platform.

207th Military Intelligence Brigade



The 207th MIB–T conducts full-spectrum intelligence in support of U.S. Army Africa (USARAF) and U.S. Africa Command (USAFRICOM) in order to set the intelligence architecture for the theater, disrupt trans-national and trans-regional threats, and promote regional stability in Africa while building and maintaining intelligence readiness. The 207th MIB–T is INSCOM's newest subordinate command, activated in March 2016. Its active component elements are forward-stationed in Europe, and its headquarters are colocated with USARAF headquarters. Though the brigade is organized according to the standard MIB–T design, it is still in the process of building the capacity to support USARAF and USAFRICOM operations. Its 522nd MI Battalion serves as the USARAF G-2's ACE. The brigade's 307th MI Battalion conducts theater-level multi-discipline (SIGINT, CI, and HUMINT) forward collection and exploitation in support of USARAF and USAFRICOM requirements, and it includes the brigade's two DISEs. The brigade's regionally aligned USAR MI battalion-theater support is located at Fort Sheridan, Illinois.

470th Military Intelligence Brigade

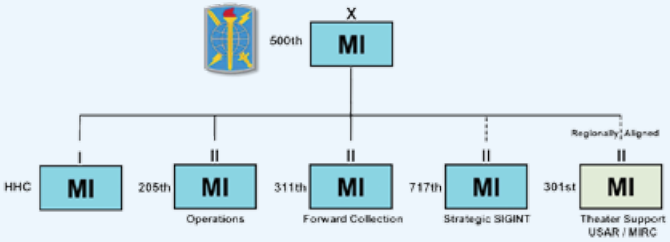


The 470th MIB–T provides mission command of assigned and attached intelligence activities to conduct intelligence operations; intelligence, surveillance, and reconnaissance (ISR) operations; and intelligence analysis for full-spectrum unified land operations in the U.S. Southern Command (SOUTHCOM) AOR. The brigade—

- ✦ Supports regional security and counters trans-regional threat networks in defense of the homeland.
- ✦ Trains and certifies the Army's five total force theater interrogation battalions to respond to global requirements.
- ✦ Sustains Army intelligence warfighting function readiness through multidiscipline individual and collective training at the INSCOM Detention Training Facility.
- ✦ Sustains intelligence enterprise and foundation layer readiness in support of total force MI units assigned to Joint Base San Antonio.

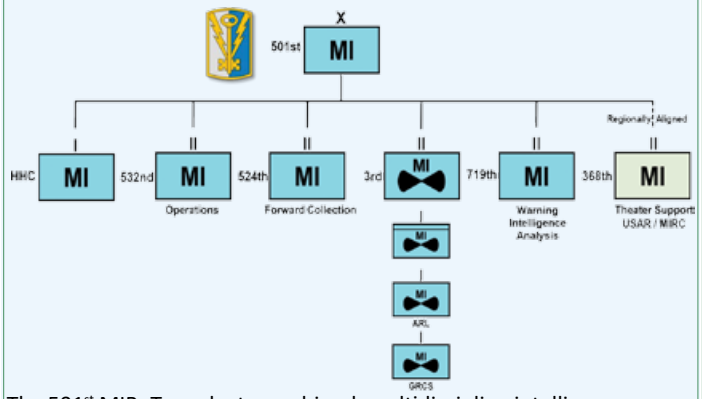
On order, the 470th MIB–T deploys tailored intelligence capabilities to global contingency operations. The 470th MIB–T is colocated with U.S. Army South (USARSO) at Fort Sam Houston, Texas. Its 312th MI Battalion serves as the USARSO's Theater Ground Intelligence Center. The brigade has a forward-collection detachment rather than a full battalion. The brigade is the administrative control (ADCON) headquarters for the 717th MI Battalion, which provides Army personnel to the National Security Agency's (NSA's) facility in Texas. The 470th is the Army unit of assignment for eight Force Protection Detachments (FPDs) forward-stationed in U.S. embassies in the SOUTHCOM AOR, for which the Army has been assigned the executive agency. FPDs exist to provide current and actionable force protection information for military personnel and resources transiting a GCC's AOR. The 470th was previously the ADCON headquarters for two interrogation battalions, the last of which deactivated in 2016. The brigade retains a company (minus) as a residual element of expertise for interrogation operations, and it continues to serve as the host for the INSCOM Detention Training Facility at Camp Bullis, Texas. The facility provides a platform for collective intelligence training and mission rehearsal and certification exercises for MI units from across the total force. The brigade's regionally aligned USAR MI battalion-theater support is located at Fort Sam Houston, Texas.

500th Military Intelligence Brigade



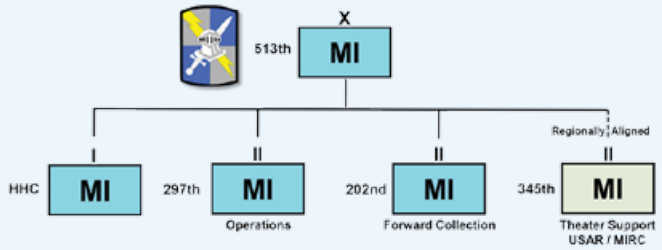
The 500th MIB–T conducts continuous, multidiscipline ISR operations to support commanders with timely, predictive, and actionable intelligence. On order, the brigade deploys tailored intelligence forces in support of U.S. Army Pacific (USARPAC) and globally in support of unified land operations. The 500th MIB–T's active component elements are entirely forward-stationed in the Pacific theater. Its headquarters and two of its battalions are in Hawaii, and one battalion is in Japan. The brigade has task-organized its assets in a way that somewhat varies from the doctrinal MIB–T organization, in order to accommodate the long-term stationing and force structure circumstances that have evolved over the course of the unit's existence. The 205th MI Battalion located in Hawaii has two companies. One company serves as the USARPAC G-2's ACE and can provide a task-organized DISE for USARPAC missions. The other company is a CI and HUMINT operations company, which includes CI resident offices in Alaska. The brigade also has a strategic SIGINT battalion that exists to provide Army personnel to NSA's facility in Hawaii, and the brigade has placed its expeditionary SIGINT collection elements in this battalion. In 2018, the 311th MI Battalion activated in Japan and inherited its mission and structure from the 441st MI Battalion, which was its provisional predecessor. The 311th MI Battalion includes a Headquarters and Operations Company, the Asian Studies Detachment, the Pacific Liaison Detachment (all located in Japan), and several CI resident and field offices in the U.S. Pacific Command AOR. The 500th is also the Army unit of assignment for three FPDs forward-stationed in U.S. embassies for which the Army has been assigned executive agency. The brigade's regionally aligned USAR 301st MI battalion-theater support is located in Phoenix, Arizona, but has a company forward-stationed in Hawaii. The brigade also mans and operates USARPAC's Foundry Platform.

501st Military Intelligence Brigade



The 501st MIB–T conducts combined, multidiscipline intelligence operations in support of Combined Forces Command (CFC) in order to provide warning intelligence and to determine the intent of North Korea's provocations and aggression through asymmetrical and conventional means. On order, the brigade transitions to wartime operations that answer the GCC and CFC commander's priority intelligence requirements in order to enable the defeat of North Korea's asymmetric and conventional threats. The active component units of the 501st MIB–T are entirely forward-stationed on the Korean Peninsula. The brigade's command and support relationships, and therefore its task organization and operations, are governed by the unique circumstances and command structures resulting from the military armistice of the Korean conflict, which has been in force for more than 70 years. Owing to this, the 501st MIB–T not only supports U.S. Army forces in Korea (Eighth Army) but also has significant elements of its operations battalion structure committed to the U.S. Forces Korea J-2 and to the U.S. and Republic of Korea CFC. The CFC organization, in which 501st MIB–T analysts work alongside their Korean allies, is designated as the Ground Component Command-Combined Analysis and Coordination Center. As with the other MIB–Ts, the brigade's operations battalion can deploy an intelligence support element (DISE) for theater missions. To increase the theater's CI and HUMINT capacity, the brigade's forward-collection battalion was reestablished in 2017, after having been drawn down and inactivated for several years. To meet the requirements for warning intelligence against the North Korean threat, the 501st MIB–T has an aerial exploitation battalion, the 3rd MI Battalion, with Guardrail Common Sensor and Airborne Reconnaissance Low aircraft that fly missions along the Korean demilitarized zone. The brigade also has an additional battalion, the 719th MI Battalion, which in an integrated effort with our Republic of Korea allies provides specialized (warning intelligence) capabilities. The brigade's regionally aligned USAR 368th MI battalion-theater support is located at Camp Parks, California.

513th Military Intelligence Brigade

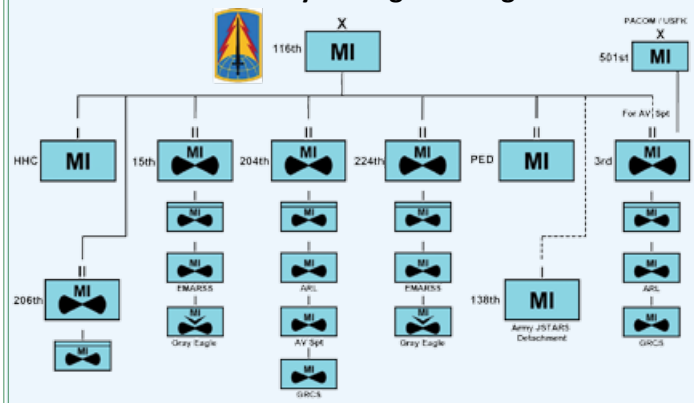


The 513th MIB–T provides tailored, multidiscipline intelligence and intelligence capabilities in support of U.S. Army Central (ARCENT) and other commands' execution of unified land operations in the U.S. Central Command (CENTCOM) AOR. The 513th MIB–T is organized according to the doctrinal MIB–T design. Its headquarters and subordinate battalions are stationed at Fort Gordon, Georgia, but it conducts enduring intelligence reach support and continuously has elements forward deployed in support of CENTCOM/ARCENT. The 297th MI Battalion provides ARCENT's Theater Ground Intelligence Center operating from Fort Gordon, though it also has a detachment located with ARCENT Headquarters at Shaw Air Force Base, South Carolina, and an element deployed with ARCENT's forward command post in the CENTCOM AOR. The brigade frequently deploys task-organized intelligence support elements (DISEs) for ARCENT exercises and operations. The 202nd MI Battalion, the brigade's forward-collection battalion, also has detachments forward deployed to conduct enduring operations. The brigade's regionally aligned USAR 345th MI battalion-theater support is located at Fort Gordon.

Functional, Signals Intelligence, and Cyber Brigades

The functional, SIGINT, and cyber brigades contain the Army's subject matter expertise for analysis, HUMINT, CI, SIGINT, and cyberspace operations. These organizations enjoy close relationships with other intelligence community organizations, such as the Defense Intelligence Agency, and sometimes work in the same buildings. Each of these organizations yields two major benefits for the Army: they collect operational intelligence for the Army, and they can serve as a linkage to ensure that the Army benefits from national-level intelligence operations.

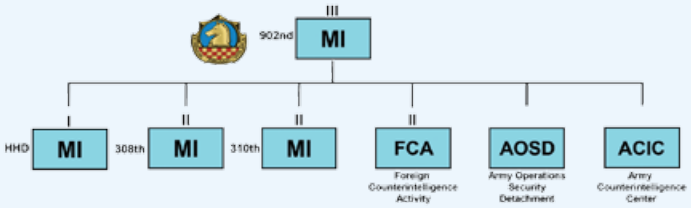
116th Military Intelligence Brigade



The 116th MIB (Aerial) conducts worldwide expeditionary and remote aerial reconnaissance, surveillance, and target acquisition; ISR; and associated tasking, collection, processing, exploitation, dissemination, and feedback of collected intelligence in support of Army unified land operations and joint requirements. The 116th MIB (Aerial) was established in September 2014 in order to unify mission command of the Army's medium-altitude aerial ISR aircraft fleet. The creation of this aerial ISR brigade resulted from lessons learned over more than a decade of sustained worldwide expeditionary operations: the effectiveness and efficiency of missions and force generation would be optimized by consolidating aerial exploitation and aerial reconnaissance battalions into a single Army service-retained formation. The 116th MIB headquarters and its processing, exploitation, and dissemination battalion are located at Fort Gordon, Georgia, with the subordinate battalions located at Fort Hood, Texas (15th MI Battalion and 206th MI Battalion); Fort Stewart/Hunter Army Airfield, Georgia (224th MI Battalion); and Fort Bliss, Texas (204th MI Battalion). The 3rd MI Battalion (Aerial Recon) in Korea remains assigned to the 501st MIB–T, but the 116th has a

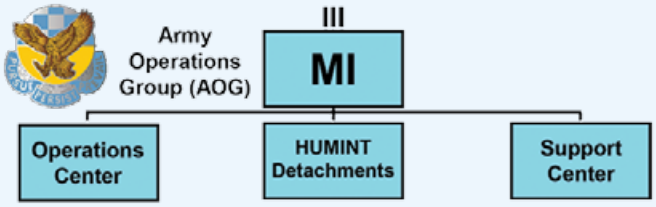
supporting relationship with the battalion to enable its aviation operations readiness. The 116th MIB also serves as the ADCON headquarters for the 138th MI Company, which provides the Army crew members who fly aboard U.S. Air Force Joint Surveillance and Target Acquisition Radar System aircraft. The 15th MI Battalion and the 224th MI Battalion each have one company of Enhanced Medium Altitude Reconnaissance and Surveillance System aircraft and one company of Gray Eagle unmanned aircraft systems. The 204th MI Battalion has one company of Airborne Reconnaissance Low aircraft and one company of Guardrail Common Sensor aircraft. The 206th MI Battalion has no organic aircraft but is a mission command headquarters that provides additional capacity for rotational expeditionary missions.

902nd Military Intelligence Group



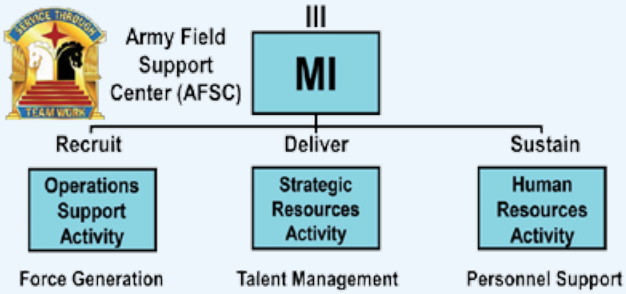
The 902nd MI Group (MIG) conducts CI to identify, neutralize, or exploit foreign intelligence entities, international terrorist organizations, and insider threats to protect Army and designated Department of Defense (DoD) forces, information, and technologies worldwide. The 902nd MIG is an Army service-retained functional command assigned to INSCOM. It consists of a Headquarters and Headquarters Detachment, four operational elements, and the Army Counterintelligence Center, which is an analytical element that produces CI-related assessments. The group's operational elements are the 308th MI Battalion, the 310th MI Battalion, the Foreign Counterintelligence Activity, and the Army Operations Security Detachment. The 902nd MIG headquarters and the headquarters of its subordinate elements are located at Fort Meade, Maryland, but group Soldiers and Civilians are spread across 43 field offices, detachments, and team locations across the continental United States (CONUS), and provide Army liaisons at 16 Federal Bureau of Investigation Joint Terrorism Task Force locations. The 902nd MIG conducts the full range of CI functions (operations, investigations, collection, analysis and production, and technical services and support activities) in direct and general support of the Army and selected DoD and joint activities in CONUS. The group conducts CI operations worldwide on a general support basis and provides a full range of CI capability, especially technical CI and functional services, and general support reinforcement through INSCOM's MIB–Ts to theater ASCCs. The 902nd MIG also deploys tailored capability packages in support of Army and joint expeditionary operations.

U.S. Army Operations Group



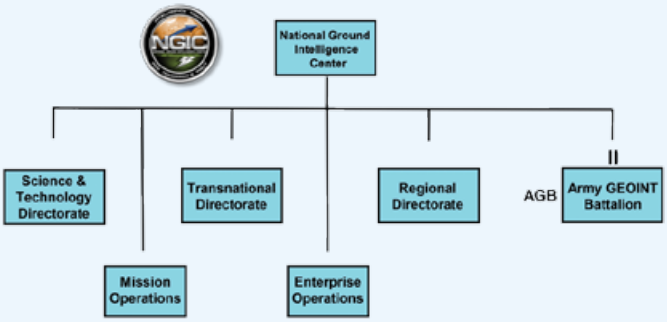
The U.S. Army Operations Group (AOG) conducts and enables global and contingency full-spectrum HUMINT operations in support of U.S. Army intelligence and operational requirements. AOG enhances and sustains U.S. Army HUMINT skillsets as the Army's functional HUMINT Foundry lead. The AOG headquarters is located at Fort Meade, Maryland, and its coordinating staff sections are task-organized into two functional elements: an operations center and a support center. The group has five regional collection detachments and a functional collection detachment. AOG provides general support HUMINT to answer information and intelligence requirements for all echelons, though with primarily a strategic and operational-level focus. As the HUMINT functional lead for the Army Foundry Program, AOG oversees certification of the Foundry site HUMINT cadre and maintains Foundry's program of instruction and classroom curricula for advanced HUMINT training.

U.S. Army Field Support Center



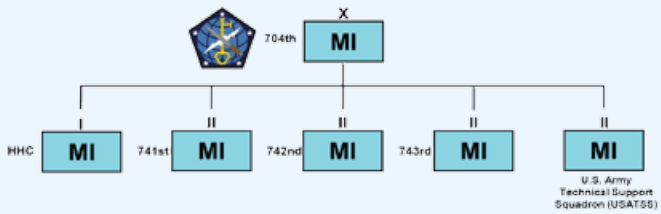
The U.S. Army Field Support Center (AFSC) provides specialized operational, administrative, and personnel management support to Army and other DoD services and agencies. AFSC recruits, delivers, and sustains personnel in the CI, HUMINT, SIGINT, and cyberspace career fields whose duty assignments require unique support not generally offered by standard administrative processes and organizations. To perform this mission, AFSC is organized into three activities. Each activity is dedicated to a different aspect of the AFSC mission to ensure a readiness pool of suitably qualified experts to meet Army and DoD specialized requirements.

National Ground Intelligence Center



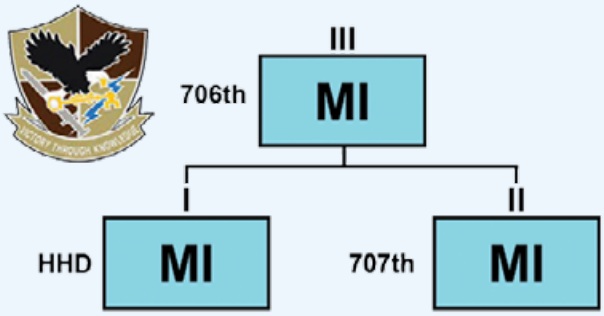
The National Ground Intelligence Center (NGIC) provides all-source and geospatial intelligence on foreign ground force capabilities and related military technologies while integrating with mission partners to ensure the U.S. Army, DoD, joint, and national-level leaders maintain decision advantage to protect U.S. interests at home and abroad. The NGIC, located at Rivana Station in Charlottesville, Virginia, is an INSCOM subordinate command and is the Army's service intelligence center. As a member of the federated Defense Intelligence Analysis Program, NGIC is DoD's primary producer of ground forces intelligence. It provides general MI covering foreign conventional and irregular ground forces order-of-battle; doctrine; tactics, techniques, and procedures; training; maintenance; and logistics. NGIC's staff also includes highly skilled specialists (physicists, chemists, computer scientists, mathematicians, and modeling and simulation experts) who analyze foreign ground forces' weapons, equipment, and operating systems to provide scientific, technical data, and assessments on current and emerging military capabilities. The Army Geospatial Intelligence Battalion, located with the National Geospatial-Intelligence Agency at Fort Belvoir, Virginia, is an NGIC subordinate unit.

704th Military Intelligence Brigade



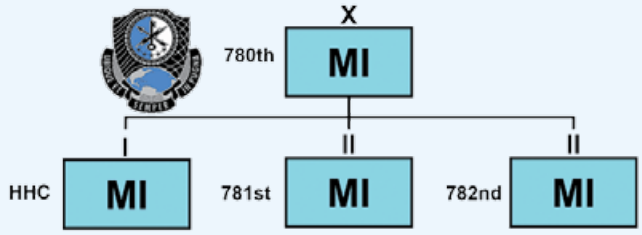
The 704th MIB conducts global cryptologic operations in support of strategic, operational, tactical, joint, and interagency commanders' intelligence and training requirements to enable decisive advantage in the multi-domain battle. As the Army's SIGINT functional brigade, the 704th is responsible for meeting national to tactical SIGINT requirements. In this role, the 704th MIB operates across a broad spectrum of support ranging from U.S. Government policy makers to tactical forces, ensuring that each are supplied with timely SIGINT reporting, training, and access to databases relevant to their missions. The 704th is the Army's largest intelligence brigade with a strength of more than 1,700 Soldiers and 80 Army Civilians, comprised of 50 plus military occupational specialties and with linguists for 25 different languages. The brigade headquarters and three of its battalions (741st, 742nd, U.S. Army Technical Support Squadron) are located at Fort Meade, Maryland, providing the Army's manning to NSA-Washington. The 743rd MI Battalion is located at Buckley Air Force Base, Colorado, and provides Army personnel for NSA-Colorado. The 704th MI Soldiers operate from NSA's fixed sites and deploy globally for the NSA, joint, and Army expeditionary missions. Though the brigade predominantly operates under the operations control (OPCON) of NSA, it also has elements dedicated to supporting the Army. The Army technical control and analysis element leverages its position within the NSA enterprise to enhance the operations of the Army's tactical SIGINT force. The 704th MIB is also the functional lead for SIGINT training at Foundry sites and for Army SIGINT professionalization programs.

706th Military Intelligence Group



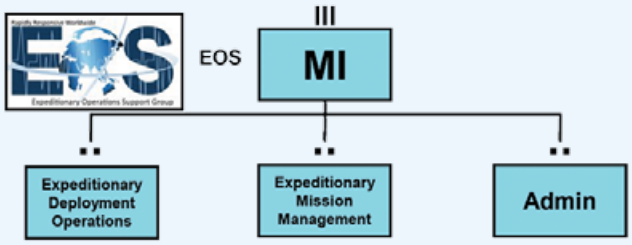
The 706th MIG provides trained and ready Soldiers in order to enable NSA/Central Security Service (CSS)–Georgia cryptologic operations supporting regional intelligence activities and globally deployed U.S. forces with accurate and timely SIGINT. The 706th MIG provides the Army's manning to NSA-Georgia at Fort Gordon. The 706th MIG commander also serves as the Director of NSA-Georgia and is responsible for leading that facility's multi-service military and civilian workforce. While the Soldiers of the 706th MIG are embedded in a national intelligence site, their daily mission serves to support operations from the strategic to tactical level in support of U.S. military operations worldwide. The 706th also partners with other INSCOM units at Fort Gordon (513th MIB and 116th MIB) and with U.S. Army Forces Command to leverage NSA programs that provide training and professionalization opportunities for Army SIGINT Soldiers and cryptologic linguists.

780th Military Intelligence Brigade



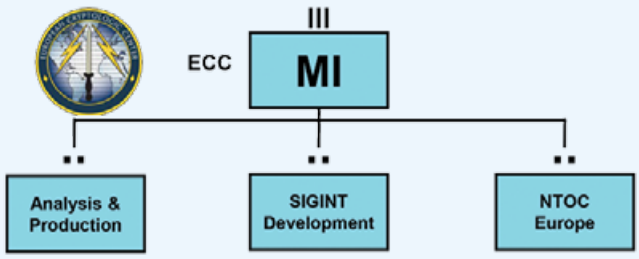
The 780th MIB conducts SIGINT and cyberspace operations to create operational effects in and through the cyberspace domain. These operations gain and maintain freedom of action required to support Army and joint requirements while denying the same to adversaries. While INSCOM has ADCON (man-train-equip-readiness responsibility/authority) of the 780th MIB, it is assigned to U.S. Strategic Command, which has further delegated OPCON of the brigade to U.S. Cyber Command and Army Cyber Command. The brigade comprises Soldiers and Civilians in a blend of the cyberspace operations (CMF 17) and intelligence career fields (CMF 35). The 780th MIB headquarters and its 781st MI Battalion are located at Fort Meade, Maryland, and the 782nd MI Battalion is located at Fort Gordon, Georgia. The 781st MI Battalion provides the mission teams, support teams, and cyberspace protection teams, which are the Army's contribution to the Joint National Cyber Mission Force. The 782nd MI Battalion provides combat mission teams and the combat support teams that support the GCCs.

Expeditionary Operations Support Group

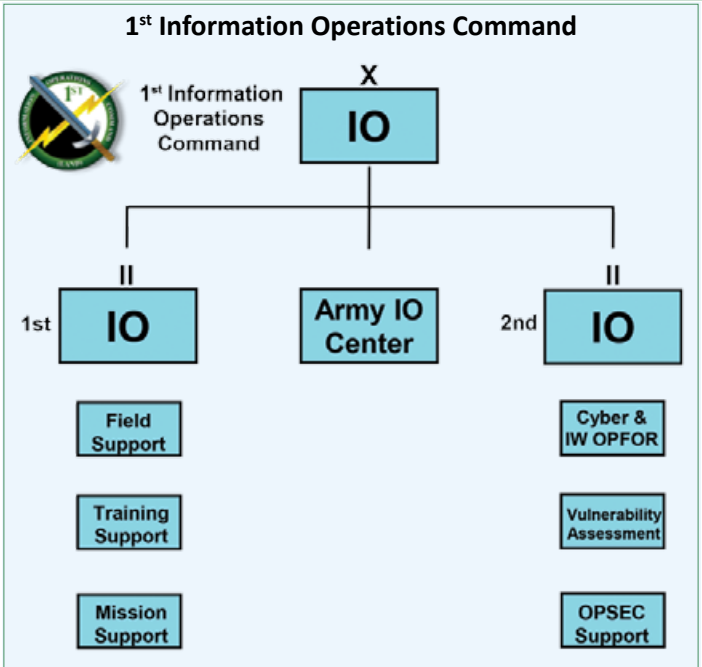


The Expeditionary Operations Support Group (EOSG) enables the NSA's Directorate of Operations expeditionary cryptologic support to current operations and leads expeditionary planning for crisis, contingency, and campaign operations worldwide. EOSG is a subordinate element of NSA's Directorate of Operations that comprises a mix of military members from all services and NSA civilians. EOSG provides and manages NSA's expeditionary capabilities in support of global operations.

European Cryptologic Center



The European Cryptologic Center (ECC) analyzes, produces, and disseminates SIGINT in support of the intelligence community, the EUCOM and USAFRICOM commanders, and national decision makers in order to defend against threats to the U.S. homeland and protect U.S. and allied national interests. ECC supports NSA/CSS partners with discovery, analytics, cyberspace defense, and tradecraft.



The 1st Information Operations (IO) Command (Land) provides IO and cyberspace operations support to the Army and other military forces through deployable teams, reachback planning and analysis, and specialized training in order to support freedom of action in the information environment and to deny the same to adversaries. The 1st IO Command is the Army's only Active Component IO organization. It is an INSCOM subordinate command and is under the OPCON of the U.S. Army Cyber Command. The 1st IO Command is a multicomponent, brigade-level organization, and consists of a Headquarters and Headquarters Detachment and two battalions. The 1st IO Command deploys mission-tailored IO field support teams and IO vulnerability assessment teams configured to meet the supported command's requirements. Its Army Information Operations Center provides the Army's only IO-focused reachback planning support, intelligence analysis, and technical assistance to deployed 1st IO Command teams and other military units, agencies, and departments requesting support. The 1st IO Battalion is responsible for the training and global deployment of multiple expeditionary IO teams from the Active Duty and Reserve Component to synchronize information-related capabilities in support of the Army, joint task forces, and combatant commands. Using publicly available information, 1st IO Battalion provides social media analysis to enable force protection and operational security in support of deployed forces. The 2nd IO Battalion deploys multifunctional IO teams worldwide while maintaining close and remote network access to employ a full range of IO capabilities that improve the readiness and ability of U.S. military forces to operate decisively in a contested information environment.

Endnote

1. Department of the Army, Army Doctrine Publication 6-0, *Mission Command* (Washington, DC: U.S. Government Publishing Office, 17 May 2012), 1-2. Change 1 was issued on 10 September 2012. Change 2 was issued on 12 March 2014.

Mr. Richard Harfst works in the U.S. Army Intelligence and Security Command (INSCOM) G-3/5 Directorate of Strategic Planning, Analysis, and Integration.

Mr. Thomas Stokowski has been a senior planner on the INSCOM staff since 2006. Before that, he served for more than 23 years as an Army intelligence officer with a dual specialty in all-source and signals intelligence with assignments in the 82nd Airborne Division, 6th Infantry Division, U.S. Army Europe Headquarters, U.S. Army Training and Doctrine Command, and Army G-2 Staff.

We mortgage our future if we don't prepare for future readiness.
—GEN Mark Milley, Chief of Staff of the Army

Military leadership has prioritized readiness so that troops can continue to meet the current and future demands of the complex global security environment. The *2018 National Defense Strategy* cautions that "without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people." Secretary of the Army, Dr. Mark Esper, demands "we stop doing things at home station…that inhibits our readiness and lethality." In order to ensure the U.S. Army Intelligence and Security Command (INSCOM) remains ready to provide accurate, relevant, and timely intelligence at the speed of mission command, INSCOM has outlined in its strategic vision four lines of effort:

- Build an effective and secure network architecture.
- Drive operational intelligence collection and production.
- Implement echelons above corps intelligence readiness strategy.
- Drive Civilian workforce professional development.

The readiness line of effort, in combination with U.S. Army Intelligence Center of Excellence initiatives, will enable the intelligence warfighting function to better measure and articulate readiness. The current commander's unit status report does not sufficiently capture intelligence readiness. AR 525-30 defines unit readiness as the ability of a unit to perform its mission in accordance with its modified table of organization and equipment (MTOE). Many INSCOM units do not operate with the same configurations described in their MTOEs. To overcome this challenge, INSCOM developed the *Unit of Action* to depict more accurately the organization of intelligence capabilities for operations. This framework will enable the command to provide a true understanding of the unit's capacities and capabilities to meet any mission requirement.

The INSCOM strategic vision provides focus so that the command can ultimately deliver critical functions required to improve Total Army Readiness. INSCOM provides network access in the most austere of locations, penetrates and exploits the toughest adversaries, provides trained and ready intelligence capabilities, and develops professional intelligence personnel in support of the Army, the joint force, and the U.S. intelligence community. With the lives of our Soldiers, the success of our Army, and the fate of our Nation in mind, INSCOM pursues readiness in all that it does.

The Army Intelligence Program of Analysis

by Ms. Rita McIntosh, Ms. Kelly Nelson, and Dr. Crisanna Shackelford

Army forces and the Army acquisition community depend on exceptional foundational analysis and production intelligence support from across the Army Intelligence Enterprise and its partners. In an era of competing resources and growing demand, the need to coordinate Army Intelligence Enterprise efforts becomes increasingly critical to the Army mission.
—LTG Robert P. Ashley, Jr., Director of the Defense Intelligence Agency

Army intelligence organizations and the customers they support face complex situations and fluid environments. The multifaceted regional and transregional issues and prominent actors in this dynamic environment result in numerous intelligence demands competing for scarce analytic resources. To address this challenge across the intelligence community, the Office of the Director of National Intelligence (ODNI) directed a Program of Analysis (POA) to change how the intelligence community collectively prioritizes intelligence planning and production. To meet the challenges of competing demands and priorities against a broad range of threats, the Army intelligence enterprise developed the Army Intelligence Program of Analysis (AIPOA) under the direction of the Office of the Deputy Chief of Staff (ODCS) for Intelligence, G-2. The AIPOA addresses the imperative to identify and prioritize evolving requirements and drives a more effective intelligence production plan.

History of the Army Intelligence Program of Analysis

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and the National Commission on Terrorist Attacks upon the United States both identified the need for greater information sharing and collaboration. The commission reports identified informational and functional stovepipes, lack of coordination, and duplicative efforts as areas for improvement. The commissions' findings illuminated the need for an overarching intelligence framework, and the years following their publications saw many reforms. The Bush Administration formed the ODNI and signed into law the Intelligence Reform and Terrorism Prevention Act of 2004, restructuring the intelligence community and its activities. Additionally, the National Intelligence Analysis and Production Board transitioned to the National Intelligence Analysis Board, allowing for the transparent coordination between agencies for increased efficiency, reduction in duplication, and greater focus on analysis.

What is the Army Intelligence Program of Analysis?

The AIPOA is a document that describes the intelligence community's most pressing intelligence needs, and it is the basis for de-confliction and coordination of analytic efforts. It enables the Army intelligence enterprise to build, coordinate, and share organizational-level requirements and production with consumers and producers of finished intelligence.

Now in its fourth year of executing the AIPOA, the National Ground Intelligence Center (NGIC)[1] continues to evolve methodologies to coordinate, synchronize, and integrate the Army intelligence enterprise with the broader intelligence community, academic, and industry collaborators and allied production partners. The AIPOA complies with the ODNI requirement that all intelligence community components develop and execute an annual POA. As the Army's service intelligence center and the intelligence community's lead for all-source ground force production, NGIC is the ODCS, G-2's executor for the AIPOA.

Role of the Army Intelligence Program of Analysis

COL James Wilmeth IV, the Director for ODCS, G-2's Foreign Intelligence Directorate, identifies the critical role of the AIPOA in addressing threat intelligence requirements: "The AIPOA drives current intelligence production across the whole of the Army intelligence enterprise while also shaping and aligning the Army's intelligence capabilities to respond to emerging worldwide threats."

The AIPOA identifies and prioritizes Armywide intelligence requirements that commanders and staffs need to understand adversaries and operational environments. The AIPOA addresses consumers' key intelligence questions, which are detailed and complex questions that the Army (through NGIC) has decided it must answer in order to fulfill its missions. These questions are derived from a variety of sources. They reflect an individual question about a strategic focus area for intelligence research, analysis, and production. The question is specific in scope but does not detail every individual subcomponent of a question. The answers to key intelligence questions will provide essential

information that helps military personnel and government officials make timely decisions.

Quality intelligence products require a deep understanding of complex and interwoven issues and an ability to see both a system of problems and its discrete components. The identification and development of key intelligence questions refine intelligence analysis, and the prioritization of key intelligence questions ensures NGIC resources and production capabilities allocate sufficient efforts to the most important requirements. For example, framing intelligence information in a narrative format guides analysts' production foci. Key intelligence questions provide the means to identify Army intelligence enterprise producers and partners with capacity and capability to provide the components of the narrative required to complete a whole story.

In accordance with ODNI guidance, the AIPOA process provides the means to evaluate previous products, assess current production progress, and forecast future intelligence production needs. The AIPOA, which sets key intelligence question priorities, resource allocations, and planned production, allows decision makers, senior leaders, and managers to identify capability and capacity gaps, technology needs, and indicators of duplicated effort. The AIPOA ensures that the Army intelligence enterprise meets relevant and timely demands for tailored, focused intelligence production.

Development of the FY 2019 Army Intelligence Program of Analysis

The NGIC Mission Operations Directorate recently hosted its first community-wide operational planning meeting of the year. The event marked the first time partner agencies converged to synchronize, integrate, and coordinate efforts toward meeting Army requirements. When preparing for the event, Patrick Walsh, NGIC Director of Mission Operations, stated that "this effort…will set coordination and synchronization of Army requirements for years to come."

"By bringing together a broad range of customers and producers in one forum, the Army enterprise is afforded the opportunity to cross-reference and shape prioritization to best array capacity against priority key intelligence questions," say Dr. Crisanna Shackelford and LTC Aaron Newcomer, the leads for POA integration. Routinely, the center's chief analyst, chief scientist, and senior intelligence officers engage in a continual dialogue with customers, subject matter experts, and military personnel across the Army intelligence enterprise to obtain accurate, timely, and relevant information.

NGIC's chief scientist oversees the scientific and technical intelligence portion of the AIPOA and ensures the unique needs of the Army requirements and acquisition communities are met. This role includes understanding the strategic and tactical needs of the science, technology, and acquisition organizations and processes of the Department of Defense (DoD). The POA process helps frame key intelligence questions for warfighters, policymakers, and force developers; it facilitates analysis and production that is executed from the customer's point of view. The chief scientist ensures focus expands to include the science and technology integration communities.

The chief scientist works in concert with the chief analyst to lead a cadre of senior intelligence officers that are subject matter expert stewards of AIPOA's content. They are charged with representing the NGIC and the Army across an assigned portfolio of intelligence missions. NGIC senior intelligence officers draw on relationships with Army customers, intelligence community partners, academia, industry, and allied production partners. Senior intelligence officers and analysts across the Army intelligence enterprise continue the dialogue required to ensure that current and focused efforts contribute to mission requirements.

Ralph Edwards, NGIC chief analyst, provides oversight and guidance to the senior intelligence officer structure and ensures that analytical programs remain oriented on NGIC's core mission of scientific and technical intelligence. According to Edwards, "the senior intelligence officers' relationships, and those of the analysts across the Center and throughout the Army intelligence enterprise, connect the intelligence user community. Their deep expertise and collegial approach are vital components in getting to the right key questions, at the right priority, at the right time."

Dr. Andrea Zechman, a long-time NGIC senior intelligence officer adds, "The AIPOA provides the strategic framework that then enables deliberate, integrated production planning to address the critical intelligence needs of a range of customers. The POA provides a holistic, integrated, synchronized, and coordinated body of evidence for policy makers, analysts, and customers alike."

Program of Analysis Construct

"Intelligence requirements are aligned both geographically and functionally to best serve customer needs from the Soldier downrange to decision makers at the White House," Edwards said. "We support the DoD mission—with oversight of the ODNI—and that's why getting intelligence right is vital to our unique customer sets. The work our senior intelligence officers and analyst teams do each day saves lives. The POA framework helps to keep our efforts focused on the most important and relevant intelligence questions."

Each agency of the intelligence community develops a POA. Planners and analysts use these documents to identify joint requirements and opportunities for joint analysis and production, reducing duplication and resource burdens. In addition, the development of the POAs reveals dependencies and collaboration opportunities, ensuring efficiency and focus on significant problem areas.

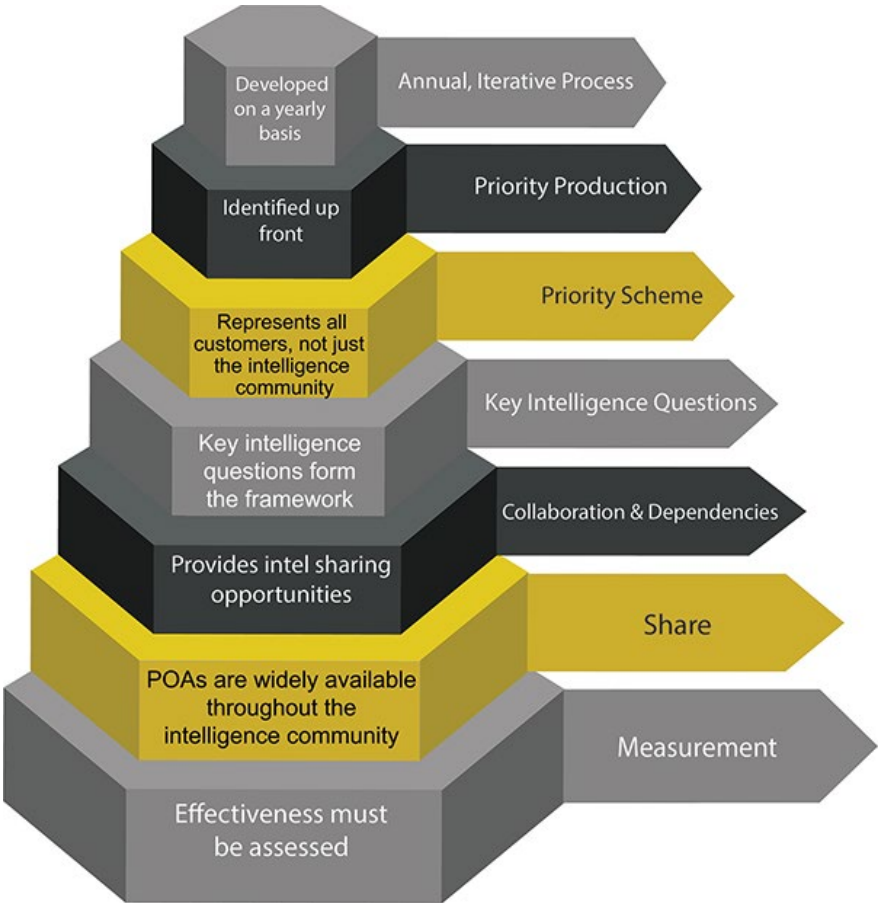


Figure 1. NGIC Program of Analysis Construct

To ensure effectiveness, POAs address seven key principles.

- POAs are living documents, and agencies must develop, compile, and publish them on an annual basis. POA contributors continually provide input and new requirements to the document as they evolve.
- The document must provide adequate representation of all priority production. The POA identifies all production requirements, but the construct ensures identification of priority production first. This gives intelligence producers confidence that their efforts are meeting real needs that support operations, acquisition, and policy.
- The POA includes a priority scheme that supports priorities from all Army intelligence consumers, not just the intelligence community. Priorities help planners understand the true scope of the work required and resourcing needs.
- Key intelligence questions are the foundation of the POA. Key intelligence questions provide a strategic focus for research, analysis, and production. The key intelligence question forces consumers and analysts alike to look at a problem from a perspective that is neither too broad nor too specific, and it helps mitigate analytical bias.
- The POA should enable expertise sharing and identify collaboration and dependencies. Enhanced collaboration allows for intelligence-sharing opportunities, transforming a stovepiped community to one of collaboration among intelligence providers. The POA identifies intelligence production requirements that can only be met via a shared responsibility across military services, governmental agencies, and others.
- The POA is shared widely across the Army via the POA conference; published by the ODCS, G-2; and circulated throughout the intelligence community.
- The Army must self-assess the effectiveness of the POA. Feedback from analysis consumers across the intelligence community provides NGIC with measures of effectiveness that allow teams to improve their processes and procedures. The POA process has evolved several times, and customer satisfaction has improved as a result. The process measures more than the number of intelligence products written—it measures effectiveness from a consumer's perspective. The framework requires increased consumer and producer interaction.

Impact of the Army Intelligence Program of Analysis

The AIPOA broadens the community of contributors for the analytic process, supports existing policy, and enhances intelligence analysis tradecraft. The method and process used to develop the POA creates a body of knowledge and a framework that defines prioritization for the next fiscal year's production. The AIPOA process has yielded better processes, technology development, and innovation. The "story arc" is one such innovation, developed in part from a joint-duty collaboration effort between the Defense Intelligence Agency and NGIC. The story arc is a powerful tool in the analysis process. It guides analysts in the telling

of an intelligence story and calls out the need for identifying new trends/developments, current impacts, future outlooks, implications, and opportunities. This framework removes information barriers and empowers analysts to contribute to the complete arc of an analytical narrative.

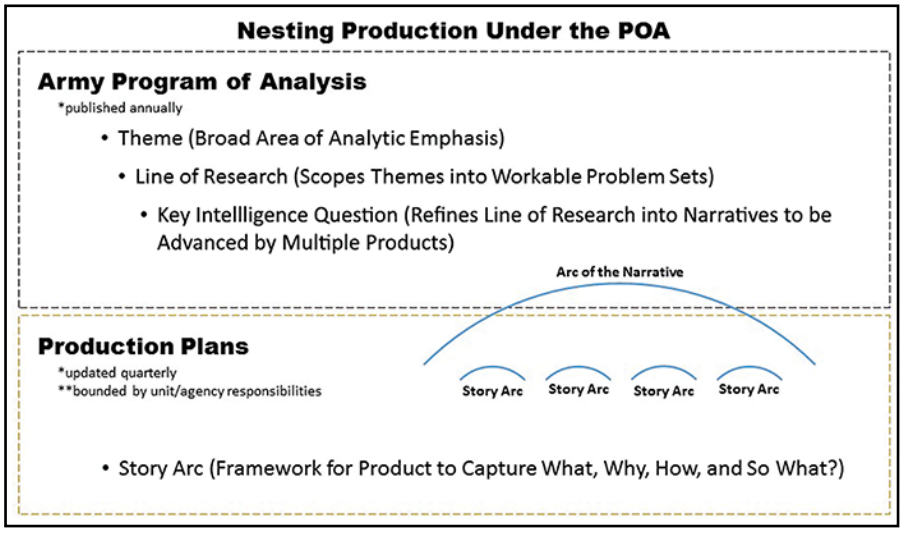


Figure 2. Impact of Army Intelligence Program of Analysis

The AIPOA also meets internal intelligence community standards that require the inclusion of subject matter experts and cross-organization analytic collaboration. The AIPOA provides a necessary and valuable communications and planning mechanism that connects those at the strategic level to individuals at the tactical level. It also drives acquisition requirements across the defense spectrum and provides the "how to" guide for meeting intelligence policy.

Endnote

All in-text quotations are the result of unpublished interviews or personal communications with the authors.

1. The National Ground Intelligence Center, a major subordinate command of the U.S. Army Intelligence and Security Command, provides all-source and geospatial intelligence on foreign ground force capabilities and related military technologies while integrating with mission partners to ensure the U.S. Army, Department of Defense, joint, and national-level decision makers maintain decision advantage to protect U.S. interests at home and abroad.

Ms. Rita McIntosh is a public affairs specialist with the Department of the Army. She holds a master of arts in journalism from the University of Missouri-Columbia and a master of arts in business and organizational security management.

Ms. Kelly Nelson has supported Army intelligence efforts for more than 20 years as a signals analyst, order of battle analyst, and information technology specialist. She currently leads knowledge management efforts for the National Ground Intelligence Center, focusing on policy and business process improvements.

Dr. Crisanna Shackelford's background and expertise, which span program management, futures warfare, systems thinking, and analytic frameworks, helped to inform the methodology required to develop the Army's Program of Analysis (POA). She has worked across the Army intelligence enterprise, gaining insights and buy-in needed to ensure the Army intelligence POA meets the Army's future challenges. Dr. Shackelford has supported the POA development process since its inception, continuing to provide valuable contributions to this important Army effort.

Setting the Theater: A Critical Intelligence Function

by Major James Chester

Editor's Note: Setting the Theater: A Critical Intelligence Function by James Chester is reprinted from Small Wars Journal per the Creative Commons license granted upon its original publication. (http://smallwarsjournal.com).

Introduction

Setting a theater is often considered the responsibility of logisticians; an entire issue of *Army Sustainment* was dedicated to the concept in 2015.[1] While the sustainment warfighting function does play a large and essential role in the process, setting an operational theater requires input from all warfighting functions, and the U.S. Army Intelligence and Security Command (INSCOM) has an important role in these actions. Most Soldiers who deployed in support of Operations Enduring Freedom and Iraqi Freedom, and their follow-on operations, deployed into mature, established theaters where setting and opening a theater had ceased to be a concern. Likely future operations will be conducted in far different operational environments. The advances in adversary capabilities that underpin the multi-domain battle concepts require the Army to be ready to rapidly deploy into theaters dramatically different from late-stage Iraq and Afghanistan.[2]

Defining Responsibilities

ADRP 4-0, *Sustainment*, published in 2012, defines setting the theater as "all activities directed at establishing favorable conditions for conducting military operations in the theater, generally driven by the support requirements of specific operation plans and other requirements established in the geographic combatant command's (GCC) theater campaign plan."[3] A more recent, but non-doctrinal definition suggested in 2015 would define setting the theater as "the broad range of actions conducted to shape the operational environment, deter aggression, and establish the conditions in a theater of operations for the execution of strategic plans."[4] Either definition has clear implications for intelligence warfighting function responsibilities. Setting the theater is a way of thinking about the activities that suppport operations to shape and about other actions during operations to prevent. Throughout the world every day, a wide range of organizations are setting operational theaters, including INSCOM, working in support of theater army requirements.

One of the key tasks for a theater army is to set the theater, briefly described in FM 3-94, *Theater Army, Corps, and Division Operations*, as a task to "set conditions in the theater for the employment of landpower."[5] INSCOM's military intelligence brigades-theater (MIB–Ts) support theater-setting requirements from Army Service component commands (ASCCs), GCCs, and aligned commanders in a variety of ways.[6] This includes conducting distributed intelligence operations; supporting joint, interagency, and multinational integration and intelligence and communications architecture development; and performing specific missions in the theater opening process.

Distributed Intelligence Operations

Ongoing intelligence, surveillance, and reconnaissance operations; intelligence analysis; partner nation training exercises; and a range of other operations and activities provide the theater-specific expertise necessary for MIB–Ts to support ASCC requirements in setting a theater. This expertise allows MIB–T personnel to inform ASCC actions, to improve aligned force and senior leader situational awareness, and to understand and request appropriate, high-payoff support from other INSCOM organizations and the broader intelligence community. In fact, ongoing distributed intelligence operations throughout a given GCC's area of responsibility underpin all aspects of MIB–T readiness to set an operational theater. Without this regional and warfighting function-specific knowledge, INSCOM would be less effective in conducting theater-setting tasks.

Each MIB–T conducts distinct operations based on a range of GCC authorities and requirements as specified by the respective ASCC. This operational expertise serves other theater-setting requirements beyond just creating groups of discipline-specific, regionally informed subject matter experts. Distributed operations also help to set the conditions for future success by demonstrating an active regional commitment to allies, partners, local populations, and adversaries. This demonstrated resolve can help to deter potential adversaries attempting to evaluate likely U.S. responses to actions counter to U.S. interests. These operations also can help to improve partner nation capability, giving our allies additional tools as they improve their own readiness to

conduct operations. Improving U.S. and partner nation individual capabilities can then provide opportunities to improve even further through joint, interagency, and multinational integration.

Joint, Interagency, and Multinational Integration

Close integration with joint, interagency, and multinational partners is essential when establishing the conditions for potential operations in a theater. Joint teammates provide capabilities that the Army lacks and can provide perspectives that Army personnel might not have considered. The same is true for civilian interagency organizations. In U.S. Southern Command, for example, some law enforcement agencies have decades of experience conducting operations throughout the region and provide a depth of knowledge on theater-specific information unmatched anywhere else. Integration with these partners, balanced with careful recognition of differing authorities and responsibilities, allows both organizations to improve the performance of ongoing operations and to improve readiness for future operations.

Multinational partners also provide essential perspectives and capabilities. In some regions, one or two partners can be mission essential to the conduct of any operations in that theater. In other regions, input from a wide range of partner nations is necessary to achieve the shared understanding that enables effective action. Partner nation ground intelligence forces and the expertise of U.S. joint and interagency partnerships with their own multinational counterparts all provide indispensable functions. The regional expertise and distinct capabilities of these counterpart professionals often provide knowledge and opportunities that other U.S. Army, joint service, or interagency organizations cannot match. More importantly, based on the status of forces and other agreements signed between the United States and international partners, some operations may be illegal without host nation approval. Setting the theater consequently requires that primary effort take place before the outbreak of hostilities or the beginning of a contingency operation. Wartime authorities, if granted, could be insufficient to permit the entire range of actions necessary to set an operational theater. The opening period of a named operation is likely too late to begin setting the conditions for mission success, making host and partner nation integration essential in any theater.

Intelligence and Communications Architecture Development

Modern advances in communications technology and intelligence systems have led to continual improvements in collection, analysis, and dissemination of intelligence data. These advances require a corresponding effort to ensure the systems architectures are in place to share data and provide mission command for distributed elements. The work that MIB–Ts, functional intelligence brigades, and other INSCOM organizations put into building this architecture not only enables current operations but also serves as the foundation for the systems architecture that arriving forces will require in a newly opened operational theater. By testing ideas and improving capabilities, INSCOM allows potential future inbound forces to focus more time on the content of intelligence and communications data and less on its transmission, receipt, storage, and access.

U.S. Army photo by SGT Jon Heinrich

The 8th Theater Sustainment Command hosted Perspicuous Provider 17 from May 29 to June 17 at Schofield Barracks, Hawaii. Perspicuous Provider is a joint exercise designed to increase sustainment-centric intelligence through a Humanitarian Aid/ Disaster Relief scenario within the Pacific theater.

Architecture development is not limited to physical systems and hardware. Database management, managing data flow to and from the broader intelligence enterprise, reporting prioritization, and a range of other architecture and data management functions provided by MIB–Ts establish a baseline that deploying units will need. Units arriving into a theater will deploy with their own intelligence and communications systems, but they can and should expect the resident theater ground intelligence experts to provide an effective systems framework that enables success.

Theater Opening

While preparing and executing shaping operations in the joint phasing construct is an essential part of setting a theater, deliberate actions supporting the execution of a named operation are also necessary. All doctrinal sources define *theater opening* more narrowly than *setting the theater. Theater opening* is defined in ADP 4-0 as "the ability to establish and operate ports of debarkation (air, sea, and rail), to establish a distribution system, and to facilitate throughput for the reception, staging, and onward movement of forces within a theater of operations."[7] It is designated in ADRP 4-0 as the responsibility of the theater sustainment command.[8] This somewhat narrow and sustainment-focused definition fails to account for the

required actions performed by other warfighting functions during the initial flow of forces into an underdeveloped theater. No amount of broad regional conditions setting will prevent the need to rapidly expand force-flow capabilities into an emerging operational theater, meaning that *theater opening* actions are a requisite, regardless of success in broader theater-setting tasks.

A better definition of *theater opening* for the non-sustainment warfighting functions would be "the establishment and operation of processes, systems, and facilities that facilitate reception, staging, onward movement, and integration of forces within a theater of operations." Under this definition, MIB–Ts help to meet intelligence requirements in several ways.

In early stages of a potential conflict or other contingency operation, a MIB–T will likely deploy an intelligence support element, potentially in conjunction with the ASCC's theater army headquarters. This element will not only provide a better understanding of the operational environment to commanders, but it may also serve as one of the first intelligence organizations in a new operational theater. As such, they will provide an integration point for intelligence organizations first arriving in a new area of operations. As more robust force levels are established, the MIB–T will need to synchronize with the ASCC G-2 and theater army staff to help receive arriving intelligence organizations and to ensure that they are appropriately connected to theater intelligence architectures. Depending on operational requirements, this reception and integration will involve pulling units not only into theater intelligence systems and processes but also incorporating a wide range of potential augmentation directly into the brigade itself.

The Way Forward

INSCOM organizations continuously work to set operational theaters every day and to refine their practices to this end. Support to theater exercises in every GCC allows intelligence professionals to improve condition-setting operations. Specific "set the theater" exercises allow INSCOM brigades to discern capability gaps and establish solutions that use the capabilities and expertise of the entire intelligence community. Additionally, examinations of essential tasks and functions to account for unique theater-setting requirements will help ensure units remain ready to perform these functions in the future.

INSCOM can improve its support posture with a greater emphasis on logistical readiness for the intelligence warfighting function. The use of Army pre-positioned stocks and other pre-positioned unit sets allows for the rapid deployment of units into potential conflict zones. The presence of these stocks serves as a credible deterrent for adversaries considering actions that might provoke a U.S. military response. Army pre-positioned stocks and other pre-positioned unit sets should continue to maintain intelligence systems and equipment that would allow INSCOM and other intelligence organizations to rapidly deploy into a range of potential theaters.

Integration with sustainment counterparts is also necessary. Subject matter experts from the sustainment and intelligence warfighting functions should collaborate across echelons to evaluate and improve intelligence operations while shaping the operational environment and deterring conflict. INSCOM, ASCC G-2, and GCC J-2 personnel must also ensure that intelligence organizations exercise and evaluate during theater exercises their ability to set the conditions necessary to enable further mission accomplishment, including their ability to perform reception, staging, onward movement, and integration functions during a theater opening.

U.S. Army photo by SPC Angelica Mendez

U.S. Army Africa Soldiers participate in an early entry command post exercise to maintain joint task force capabilities on Caserma Ederle in Vicenza, Italy, Jan. 29, 2018.

Conclusion

Adversaries are ceaselessly watching, assessing, and responding to U.S. actions and inaction. Readiness in setting a theater through effective performance of and support to

ongoing operations and effective preparation for potential contingency operations can help to deter conflict. If deterrence fails, or if circumstances require a military response short of armed conflict, then INSCOM's ability to set an operational theater will be critical in the success or failure of arriving forces in supporting the combatant commanders' missions.

Endnotes

1. "Setting the Theater, Planning Today Provides Options for Tomorrow," *Army Sustainment* 47, no. 6 (November-December 2015), http://www.alu.army.mil/alog/2015/novdec15/pdf/novdec2015.pdf.

2. GEN Robert B. Brown and GEN David G. Perkins, "Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight," *War on the Rocks* (Texas National Security Network), 18 August 2017, https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/.

3. Department of the Army, Army Doctrine Reference Publication (ADRP) 4-0, *Sustainment* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2012), 2-1–2-2.

4. Kenneth R. Gaines and Dr. Reginald L. Snell, "Setting and Supporting the Theater," *U.S. Army Worldwide News,* November 2, 2015, https://www.army.mil/article/157230/setting_and_supporting_the_theater.

5. Department of the Army, Field Manual 3-94, *Theater Army, Corps, and Division Operations* (Washington, DC: U.S. GPO, 21 April 2014), 2-3.

6. Thomas Stokowski, "The MI Brigade (Theater) as an Intelligence Anchor Point for Regionally Aligned and Global Response Forces," *Military Intelligence Professional Bulletin* 42, no. 2 (April-June 2016): 5-7.

7. Department of the Army, Army Doctrine Publication 4-0, *Sustainment* (Washington, DC: U.S. GPO, 31 July 2012), 12.

8. ADRP 4-0, 2-2.

MAJ James Chester currently serves as the Plans and Exercises Officer for the 470th Military Intelligence Brigade-Theater. Previous assignments include service as an assignment officer and account manager at U.S. Army Human Resources Command, as a tactical military intelligence company commander in Korea, and as a battalion S-2 in Germany and Operation Iraqi Freedom. He holds a bachelor's degree in geography from the University of Nebraska–Lincoln and a master's degree in public policy and management from the University of Pittsburgh.

by Chief Warrant Officer 5 David Bassili and Chief Warrant Officer 3 James Macfarlane

The recent release of the updated FM 3-0, *Operations*, emphasizes increased Armywide awareness and focus on the early phases of the joint operational planning construct.[1] Ensuring readiness for operations to "shape" and "prevent (deter)" arguably fails to elicit the same levels of motivation and excitement among ground force commanders as do operations focused on large-scale combat. However, each U.S. Army Intelligence and Security Command (INSCOM) military intelligence brigade-theater (MIB–T) is manned, trained, and equipped specifically for that purpose. As such, the term "setting the theater" is uniquely applicable to the capabilities, expected operations, and activities that MIB–Ts will execute on behalf of their Army Service component command (ASCC) and combatant command.

According to FM 3-94, *Theater Army, Corps, and Division Operations,* the primary mission of an ASCC or theater army is to set the conditions for the employment of land power in contingencies and campaigns—or "setting the theater."[2] The latter is not well defined or codified within doctrine, specifically the "how" of setting the theater. FM 3-0 describes Army shaping activities as those that help assure operational access for crisis response and contingency operations despite the changing U.S. overseas defense posture and the growth of antiaccess and area denial capabilities around the globe.[3] Shaping activities involving Army forces in support of the ground component commander (GCC) to promote favorable access include—

- Key leader engagements.
- Bilateral and multinational exercises to improve multinational interoperability and operations.
- Missions to train, advise, and equip foreign forces.
- Negotiations to secure basing and transit rights, establish relationships, and formalize support agreements.
- The use of grants and contracts to improve relationships with, and strengthen, partner nations.
- Designing interoperability into acquisition programs.
- Electromagnetic spectrum mapping of adversary capabilities.

The theater army also plays a critical role for the GCC in gaining operational access and positions of relative advantage throughout the area of responsibility (AOR). This involves analyzing the intent and capabilities of current and potential future adversaries.

Military Intelligence Brigade-Theater

As designed and described in FM 3-0, each combatant command is assigned an MIB–T that provides regionally focused collection and analysis in support of daily operational requirements and specific joint operations throughout the assigned AOR.[4] Specifically, the MIB–T develops threat characteristic databases, intelligence estimates, and all-source intelligence products to support theater army planning requirements against campaign, operation, and contingency planning efforts. Because of their regional focus, MIB–Ts provide continuity within the theater by developing cultural and linguistic skills that enable it to collect, analyze, and track threat and partner nation capabilities, doctrine, and tactics over many years.

During Army operations to shape, the most important role of intelligence is to provide timely and accurate warning analysis of threat capabilities, strengths, weakness, and changes in intent that enable commanders and senior government officials to make timely, informed decisions that ensure operational and strategic success. As the intelligence anchor points for the AOR, MIB–Ts provide regionally focused collection and analysis to support regionally aligned, assigned, and other specified forces. They provide the linkages to the theater intelligence architecture and the greater intelligence community.

Not all MIB–Ts possess the same capabilities; some have assigned aerial exploitation battalions that provide aerial intelligence, surveillance, and reconnaissance and signals intelligence (SIGINT) battalions to meet theater and national requirements. At a minimum, each MIB–T has two assigned active duty battalions. The forward collection battalion executes intelligence collection operations to satisfy commander's critical information requirements while the operations battalion provides all-source intelligence, single-source intelligence, and warnings intelligence analysis throughout the operational environment (OE) specifically to support operations to shape and prevent.

Additionally, all MIB–Ts have aligned Army Reserve theater support battalions that provide multidiscipline operational and tactical collection, analysis, and dissemination in support of their aligned ASCC's and combatant command's requirements. The MIB–T can employ organic counterintelligence (CI), human intelligence (HUMINT), and ground-based SIGINT capabilities. In the event of a crisis (beyond shaping operations), the MIB–T can be augmented with additional intelligence capabilities by INSCOM functional intelligence brigades or other theater requested forces.

Africa—Setting the Theater

U.S. Army Africa (USARAF) currently defines setting the theater as a continuous process of activities that enable joint, combined, and Army forces to deploy required resources to execute operations. It is nested within the U.S. Africa Command (USAFRICOM) theater campaign plan and the USARAF mission statement.[5] Based on this definition, USARAF's line of effort 6 (set the theater) hedges on three critical elements:

- Understand conditions and challenges in the OE.
- Shape the OE to incrementally improve conditions for the employment of land forces.
- (and ultimately) Respond to contingencies and/or open and close the joint operations area.

To inform these elements, USARAF created an assessment framework of five categories that is applicable to any country and any operation—access, mission command, intelligence, protection, and sustainment. Specifically for intelligence, the category includes 22 subcategories across the intelligence disciplines of SIGINT, geospatial intelligence, CI and HUMINT, and open-source intelligence. These subcategories focus on the availability of the authorities, capability, and capacity to conduct intelligence operations that "set the theater."

USARAF also supports other initiatives such as the cooperative security locations and regionally aligned forces that enable and reinforce set the theater efforts and operations throughout Africa. Cooperative security locations are "made up of host-nation facilities and have few permanent U.S. personnel" that "contain pre-positioned equipment and serve to enhance support contracts, blanket purchase agreements, security cooperation activities, and contingency access."[6] These sites can sustain up to 300 Soldiers for 30 days and provide an effective staging location for USARAF, regionally aligned forces, and 207th forces. They enable rapid responses to crises in the region.

Africa—Setting the Intelligence Theater

Since its activation in March 2016, the 207th MIB–T has supported USARAF's understanding of the conditions and challenges of the African OE through warning intelligence, all-source intelligence production, and specific shaping operations. It has done this using intelligence theater security cooperation training events with partner nations, multinational training exercises, briefings and debriefings of deploying personnel supporting these activities, and CI support to force protection. With the development of USARAF's set the theater framework, the 207th MIB–T focuses toward executing intelligence operations with assigned collection capabilities to satisfy USARAF commander's critical intelligence requirements.

U.S. Marine Corps photo by 1st Lt. Jack Lowder

U.S. Marine Corps 1st Lt. Jack Lowder addresses an audience on intelligence practices alongside U.S. Army COL David Jones, the chief of J29 engagements, and Royal Moroccan Armed Forces General Benlovali during the Basic Intelligence Course at the Moroccan Southern Zone Headquarters.

Under the USARAF set the theater construct, the 207th MIB–T uses the phrase "setting the intelligence theater" to describe its operations and other intelligence missions. In order to build and maintain intelligence readiness for these missions, the 207th MIB–T training strategy maximizes every opportunity to participate in USAFRICOM and USARAF exercises and create its own exercises. The 207th MIB–T trains using the INSCOM military intelligence training strategy (MITS), which employs doctrine-based training and evaluation outlines of individual and collective tasks through its four tiered levels. The 207th MIB–T has designed a MITS for its deployable intelligence support element-theater (DISE–T) based on the brigade combat team military intelligence company MITS (formerly Military Intelligence (MI) Gunnery). The DISE–T is designed to support contingency response operations in the USAFRICOM AOR, providing tactical level, all-source fusion, analysis, and secure communications to the supported element during expeditionary contingency operations.

In addition to providing contingency support via the DISE–T, the 207th MIB–T is establishing a semi-permanent,

rotational collection and analysis capacity in Africa to support the GCC, ASCC, and other Army forces conducting shaping operations. The 207th MIB–T will more effectively support situational understanding of the OE through the collection and analysis of threat and host nation capabilities, vulnerabilities, and doctrine that support shaping operations. In contingencies, the brigade will be positioned to enable and support ground force commanders and tactical MI enablers with a common intelligence picture of threat dispositions and capabilities, liaise with host nation security forces, and access the theater intelligence architecture. As the 207th MIB–T intelligence architecture matures, the unit will require additional capacity to enable processing, exploitation, and dissemination (PED) of theater aerial intelligence, surveillance, and reconnaissance assets.

Africa—Intelligence Systems Architecture

An essential component of setting the intelligence theater is establishing the intelligence systems architecture in order to enable the collection and production of intelligence products and the publication of the common intelligence picture. ADRP 2-0, *Intelligence*, defines the intelligence communications architecture as the backbone of the intelligence enterprise that "transmits intelligence and information to and from various collection elements, units, and agencies by means of different technologies and systems."[7] For the 207th MIB–T, the intelligence architecture focuses on establishing and maintaining intelligence systems and communication platforms that support the collection, transport, and hosting/sharing of data and information supporting USAFRICOM, USARAF, and U.S. Special Operations Command Africa missions. This architecture will also provide a reachback or "anchor point" of intelligence data and information for the USARAF/USAFRICOM area of operations.

Within the 207th MIB–T, the Distributed Common Ground System-Army (DCGS–A) Intelligence Processing Center or "Brain" serves as the master repository for all intelligence data from Africa. This DCGS–A system provides the reachback capability for the 207th MIB–T intelligence architecture, making intelligence data and information discoverable to all supported organizations. Like most Army organizations and systems that operate in a reachback environment, the regional hub node provided by the regionally assigned network command provides a consistent and reliable transport for the DCGS–A Brain and its supporting systems to communicate and host or share data and information.

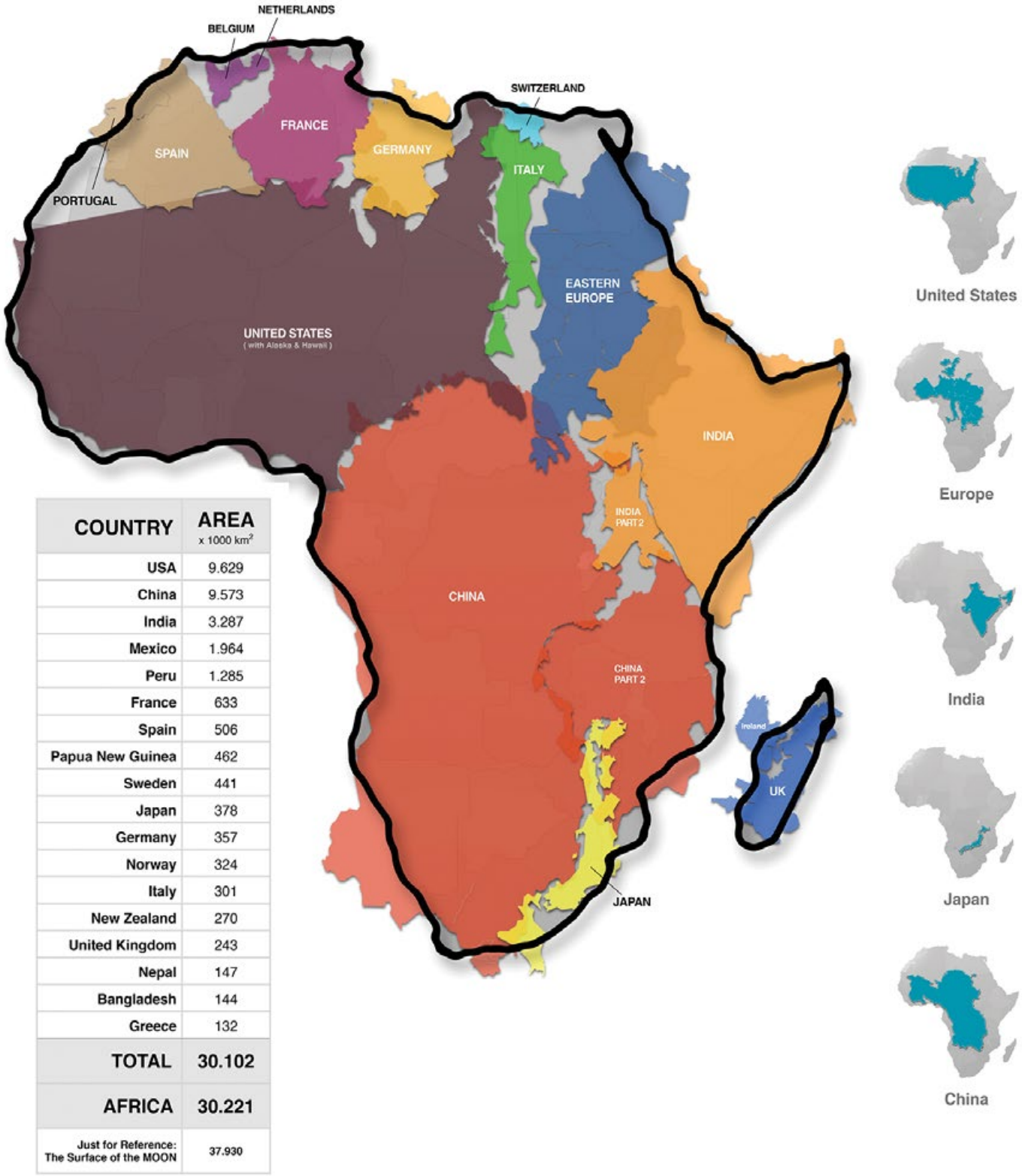
In addition to the Brain, several DCGS–A components, such as the Cross-Domain Solution Suite, directly support anchor point functionality. The Cross-Domain Solution Suite provides a timely means of moving classified data and information between different levels of classification. In addition, the Intelligence Fusion Server, Fixed Multi-Functional Workstations, and Portable Multi-Functional Workstations provide intelligence personnel with a means to interface, input, manage, and query data and information to satisfy analytical and fusion production requirements that answer the commander's priority intelligence requirements.

Another important component of the 207th MIB–T's intelligence architecture is the establishment and employment of PED enablers. ADRP 2-0 defines PED enablers as "the specialized intelligence and communications systems, advanced technologies, and the associated personnel that conduct intelligence processing as well as single-source analysis within intelligence units."[8] Within the 207th MIB–T, several intelligence systems support single-source operations. The CI/HUMINT Reporting and Collection System and subsystems provide CI/HUMINT personnel the ability to "collect, manage, receive, store and export maps, electronic data, digital imagery and audio/visual information" as well as "prepare, process and disseminate standard reports, forms, and associated files."[9] The Geospatial Intelligence Workstation is another DCGS–A system that enables geospatial analysis and production in a reachback capacity and provides a forward-deployed configuration through the Global Broadcast System communications platform. In coordination with INSCOM's functional brigades (704th MI Brigade and 706th MI Group), the 207th MIB–T SIGINT functional capabilities provide integrated tactical to national support to USAFRICOM/USARAF operations.

The 207th MIB–T DISE–T plays a critical role during contingency operations by providing a rapidly deployable intelligence reach capacity to forward operating units. The DISE–T also develops and maintains the tactical-level intelligence situation. The DISE–T supports the USARAF early entry command post and the contingency command post mission set by providing intelligence systems, communications, and analytical support while forward deployed.

The 207th MIB–T intelligence architecture extends the intelligence network forward to the African continent, enabling vital data discovery for deployed personnel and units. This task involves the employment of communication platforms that can provide two or more classified networks. For the 207th MIB–T, the TROJAN satellite communication systems provide a preponderance of the communication support for 207th MIB–T deployed personnel, providing SECRET Internet Protocol Router, National Security Agency, and Joint Worldwide Intelligence Communications System networks.

Data flow and discovery are dependent on the system configurations and connection management of intelligence systems between echelons and networks. This is a shared responsibility between the S-6/G-6, MI systems maintainers/integrators (35Ts), and DCGS–A field support contractors, who have the expertise and privileges to configure systems and manage networks. However, the operators of the intelligence systems have a significant role in identifying what information must move across the network(s) and systems. These relationships form the foundation on which the 207th MIB–T in-



COUNTRY	AREA x 1000 km²
USA	9.629
China	9.573
India	3.287
Mexico	1.964
Peru	1.285
France	633
Spain	506
Papua New Guinea	462
Sweden	441
Japan	378
Germany	357
Norway	324
Italy	301
New Zealand	270
United Kingdom	243
Nepal	147
Bangladesh	144
Greece	132
TOTAL	30.102
AFRICA	30.221
Just for Reference: The Surface of the MOON	37.930

The True Size of Africa

telligence architecture provides intelligence reach and sets the intelligence theater.

Many factors affect the 207th MIB–T's ability to establish the deployed intelligence architecture. The most significant factor is that the African continent is enormous, measuring more than three times the landmass of the United States, and its nations are largely undeveloped with inaccessible or unstable supporting infrastructures. An important planning consideration for establishing and extending the intelligence architecture on the African continent is that intelligence personnel will likely have to operate in a disconnected, intermittent, and limited communications environment. This requires maintainers and intelligence personnel to plan for and establish primary, alternate, contingency, and emergency plans that provide independent and redundant network connection(s) vital to satisfying mission requirements.

Conclusion

As OEs become more complex, the Army has recognized that it cannot afford to wait until large-scale combat operations are under way to initiate set the theater efforts. This realization has led to changes in Army doctrine that highlight the need to shape OEs and prevent (or deter) situations as they arise. As MIB–Ts are uniquely challenged in setting the intelligence theater for their specific AOR, they must understand the problem sets in their OE and what resources (standardized and non-standardized) are needed to accomplish their unique challenges. For the 207th MIB–T, this means enabling and employing its various collection and analytical assets as far forward as possible in order to provide an understanding of the OE and threat forces to ground force commanders.

Endnotes

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

2. Department of the Army, FM 3-94, *Theater Army, Corps, and Division Operations* (Washington, DC: U.S. GPO, 21 April 2014), 2-9. Change 1 was issued on 6 December 2017.

3. FM 3-0, 3-2.

4. Ibid., 2-42.

5. MG Mark Palzer and MAJ Joel M. Machak, "Setting the African theater," *U.S. Army Worldwide News*, September 5, 2017, https://www.army.mil/article/192463/setting_the_african_theater.

6. Ibid.

7. Department of the Army, Army Doctrine Reference Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 August 2012), 2-6.

8. Ibid, 4-12.

9. U.S. Army website, "CHARCS," *Distributed Common Ground System–Army*, last modified April 27, 2017, https://dcgsa.army.mil/capabilities/charcs/.

References

Blinde, Loren. "Army posts DCGS–A RFI." *Intelligence Community News*. October 20, 2017. http://intelligencecommunitynews.com/army-posts-dcgs-a-rfi/.

FedBizOps.gov website. "DCGS–A Capability Drop-2, RFI." 2017. https://www.fbo.gov/index?s=opportunity&mode=form&id=7905a9b96904d3431f51356dc366edba&tab=core&_cview=1.

U.S. Army Intelligence Center of Excellence, Military Intelligence School. *Communications Central TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) Lightweight Intelligence Telecommunications Equipment (LITE) AN/TSQ-226(V) [Update] (version 3.0)*. February 19, 2013. https://rdl.train.army.mil/catalog-ws/view/100.ATSC/82BD5650-B897-4D7E-95B7-231D80C98B40-1361305127996/doc.pdf.

U.S. Army website. "Fielding and Training." *Distributed Common Ground System–Army*. Last modified June 21, 2017. https://dcgsa.army.mil/capabilities/fielding-training/.

U.S. Army website. "Satellite Communications." *Program Executive Office Command Control Communications-Tactical*. Last updated April 7, 2017. http://peoc3t.army.mil/wint/satcom.php.

CW5 David Bassili is an all-source intelligence technician with 29 years of experience as an intelligence professional. He is presently serving as Command Chief Warrant Officer of the 207th Military Intelligence Brigade-Theater (MIB–T) in Vicenza, Italy. He has previously served in assignments from maneuver battalion to combatant command. He has an associate of arts in general studies and a bachelor of arts in homeland security from American Military University.

CW3 James Macfarlane is an all-source intelligence technician who has served in a variety of intelligence positions throughout his 17-year career. His previous assignments include A Company Operations Group, National Training Center; 30th Signal Battalion; 2-11 Field Artillery Battalion; 1-27 Infantry Battalion; 2nd Combat Aviation Brigade; U.S. Army Africa G-3 Fires; and 307th Military Intelligence Battalion. He has deployed twice in support of Operation Iraqi Freedom and once in support of Operation Enduring Freedom. He is currently serving as Brigade Intelligence Systems Integrator for 207th MIB–T in Vicenza, Italy. He holds an associate of arts in general studies and is pursuing a bachelor of science in space studies from American Military University.

The U.S. Army Intelligence and Security Command at Four Decades

1977 Part II: Winning the Cold War (1981 to 1989) 2018

by Mr. Michael E. Bigelow, INSCOM Command Historian

During the 1980s and into the early 1990s, the U.S. Army Intelligence and Security Command (INSCOM) continued its global outlook as the Army improved its abilities to both defend Europe and deploy elsewhere to meet potential threats. The Army's new overarching doctrine of AirLand Battle placed a premium on accurate and timely intelligence. INSCOM enhanced its ability to physically deploy for war and developed a global command architecture of robust and reliable intelligence processing and communications systems that would focus national assets on theater and corps requirements.

The largest and most tangible step toward this goal was the establishment of the 513th Military Intelligence (MI) Group at Fort Monmouth, New Jersey, in 1982. The group's primary mission was to provide multidiscipline intelligence support to the Army component of the Rapid Deployment Joint Task Force during contingency operations and to send reinforcing intelligence support to U.S. Army Europe during time of war. During peacetime, it would meet the training needs of both the Active Army and the Reserves.

In another improvement to support the Army, INSCOM reorganized three of its MI groups into brigades in 1986. More than just a name change, the 66th MI Brigade in West Germany, the 501st MI Brigade in South Korea, and the 513th MI Brigade in the continental United States (CONUS) were reorganized for combat rather than having structures geared toward peacetime collection and training. INSCOM also designated some of its strategic signals intelligence organizations as numbered MI brigades with the aim of fostering esprit de corps among their soldiers.

In the 1980s, the Army prioritized its mission in the defense of Western Europe against the Soviet threat. Reflecting this orientation, INSCOM allocated considerable resources to Europe. The 66th MI Brigade was the command's principal unit in theater and engaged in a broad range of intelligence operations. INSCOM continued to operate two fixed sites in West Germany—the 701st MI Brigade (formerly Field Station Augsburg) in Bavaria and Field Station Berlin—to gather information on the Soviets and their Warsaw Pact allies. A third site, Field Station Sinop, collected against the Soviets from Turkey's Black Sea coast.

While Europe remained the primary focus for the Army throughout the 1980s, INSCOM maintained an active presence in the Pacific. At Fort Shafter, Hawaii, the INSCOM Theater Intelligence Center provided and planned intelligence support to Army forces in the Pacific. At nearby Schofield Barracks, the 703rd MI Brigade occupied the Kunia field station. The station's sophisticated communication systems allowed INSCOM to close older facilities in the Far East while retaining the same capabilities. In South Korea, INSCOM's 501st MI Brigade continued to monitor the demilitarized zone in its support of the Eighth U.S. Army. In Japan, the smaller 500th MI Group satisfied numerous theater and national intelligence requirements in addition to supporting U.S. Army Japan.

In the western hemisphere, INSCOM maintained its presence in Panama. In 1982, the command established a new field station and subordinated it to the 470th MI Group. Initially, the group concentrated its efforts on gathering intelligence on the unstable political situations in Central America. Later, it would broaden its scope to support counter-drug operations throughout Latin America. To assist the 470th MI Group, INSCOM created the MI Battalion (Low Intensity), a specialized unit to test a variety of collection systems, including aerostats, unmanned aerial vehicles, and sophisticated aerial radio direction finding aircraft.

In the United States, INSCOM's remaining CONUS MI Group became the 704th MI Brigade. In addition to its mission to support the National Security Agency, the brigade assumed management of the Army's new TROJAN program that provided Army units in CONUS with access to a live signal environment for training. The 902nd MI Group remained INSCOM's principal counterintelligence (CI) organization; in the mid-1980s, it concentrated on specialized CI functions in the United States.

In 1988, INSCOM CI agents scored two significant triumphs against Soviet espionage. They neutralized Clyde Conrad, a retired Army noncommissioned officer who was

the key figure in an espionage ring that betrayed the North Atlantic Treaty Organization's war plans to the Hungarian intelligence services. INSCOM personnel liaised with and enabled the West German intelligence services and criminal justice system to prosecute Conrad and imprison him until his death in 1998. In late 1988, INSCOM CI officers discovered that Army Warrant Officer James Hall had sold classified material to East German and Soviet operatives. Based on that information, the Federal Bureau of Investigation was able to arrest Hall in Savannah, Georgia.

Mr. Michael E. Bigelow has served as the Command Historian for the U.S. Army Intelligence and Security Command (INSCOM) since 2006. He received a bachelor of arts in history from Colorado State University and a master of arts in military history from Temple University. He has written numerous articles for military publications such as Military Review *and* Military Intelligence Professional Bulletin*. Before becoming INSCOM's Command Historian, he served as an active duty military intelligence officer for 22 years.*

Photo courtesy of Wikimedia Commons

Field Station Augsburg

by Mr. Scott R. Hammon

Return of the Technical Control and Analysis Elements for Theater Signals Intelligence Support

Editor's Note: This article, originally titled Returning the Technical Control and Analysis Elements (TCAE) for Theater Signals Intelligence Support by Scott R. Hammon, is reprinted from Small Wars Journal per the Creative Commons license granted upon its original publication. (http://smallwarsjournal.com).

Rise and Fall of the Technical Control and Analysis Element

In mid-1975, the Intelligence Organization and Stationing Study conducted by the Army led to the creation of the U.S. Army Intelligence and Security Command (INSCOM). One of the outcomes of the study was that there was a recognized need to provide cryptologic support to tactical military intelligence (MI) units. To answer this requirement, INSCOM fielded technical control and analysis elements (TCAEs). These TCAEs were found at every echelon but played a vital role at what were then called the echelons above corps MI brigades. In the past, each of the ground component commands had a regionally aligned TCAE (e.g., Army South TCAE).

Although the name has changed from echelons above corps MI brigade to MI brigade-theater (MIB–T), what has not changed is the mission to provide intelligence support to operational theaters in order to protect U.S. national security interests and support the Army's primary mission—to fight and win the Nation's wars. A critical component of that support required by the AirLand Battle doctrine was the provision of timely electronic warfare support to all echelons. Throughout the Cold War and the early years of the post-Cold War period, the responsibility of electronic warfare support was the domain of the TCAEs. In the post-Cold War period, the U.S. intelligence community found itself in the awkward position of having no easily identifiable "enemy" at which to focus its strategic intelligence apparatus. The perceived threats to U.S. national security had changed radically.

As threats changed, signals intelligence (SIGINT) support to the Army formations also changed, starting with the transfer of TCAE assets to the new doctrinal concept of analysis and control elements (ACEs). These ACE structures, originally intended for corps-level intelligence support, also found their way into echelons above corps formations. This structure combined all intelligence disciplines under one central intelligence control. Many ACE formations still had an element that resembled a TCAE in both function and name, but as a member of the ACE and subordinate to its all-source-centric leadership, many cryptologic support organizations, whether called a TCAE, Technical Control and Analysis Cell, single-source section, or SIGINT section, became disconnected from the National Security Agency (NSA). Consequently, the Army's ability to bridge the connection between national collection assets and operational requirements degraded.

Since the terrorist attacks on September 11, 2001, Army SIGINT has seen massive changes in the conduct of business, the employment of the SIGINT Soldier, and the ever-changing technological advancements that have both challenged intelligence collection and enhanced intelligence production. From the beginning of the Global War on Terrorism, small detachments of SIGINT Soldiers deployed in support of U.S. Army Forces Command units to provide direct support to the several task forces in U.S. Central Command's area of responsibility. For cryptologic support, the task forces turned to the NSA and the newly formed cryptologic support groups (CSG) to close the gap and enable NSA to provide operational support to the warfighter; these CSGs filled the role of what had belonged to the TCAEs and ACE SIGINT sections in previous years. The development of the intelligence community's information technology enterprise provided networks by which the intelligence community could share technology, information, and resources and grant secure access to community-wide information. SIGINT Soldiers no longer had to be assigned to cryptologic centers to access national databases, and consequently NSA lost interest in managing and supporting the CSGs.

A New World Order Forces a New Strategic Plan

In the post-9/11 era, the Army finds itself in a more complex security environment, defined by rapid technological change, threats in all operating domains, and the longest sustained military operations in our Nation's history. The intense focus and duration of our operations against asymmetric adversaries has resulted in a period of strategic atrophy and diminished our competitive military advantage

in several critical capabilities. With increasing global disorder, terrorist organizations, criminal threat networks, and heavily armed rogue states, it is more critical than ever to provide decision makers the intelligence they need to make difficult choices. Interstate strategic competition has supplanted counterterrorism operations as the primary concern of U.S. national security.

A central challenge to lasting security and prosperity is the reemergence of strategic adversaries—what the *2018 National Security Strategy* classifies as "revisionist powers."[1] These powers, like China and Russia, want to shape a global political order that is consistent with their authoritarian models. Whether it is military modernization, influence operations, predatory economics, political interventions, or direct military action, these powers want to gain a position of dominance over other nations' economic, diplomatic, and security decisions. Nuclear conflict is emerging as a primary threat to the homeland and regional stability as rogue regimes like North Korea and Iran pursue nuclear programs and sponsor terrorist organizations. An increasingly isolated North Korea seeks to guarantee its regime's survival through the development and procurement of weapons of mass destruction—including biological, chemical, conventional, and unconventional weapons—and a growing ballistic missile capability.

To counter these renewed threats, the national strategy is based in four core tenants:

- Be strategically predictable, but operationally unpredictable.
- Integrate with U.S. interagency structures.
- Counter coercion and subversion.
- Foster a competitive mindset.

Army SIGINT plays a vital part in the accomplishment of all of these tenants. It is not necessary to reinvent the wheel, but we need to return to the theater-based echelons above corps approach. While typically thought of as a function of units at the corps level and below, contemporary SIGINT and intelligence community information technology enterprise applications are available to almost all echelons. Consequently, it is more important than ever to form a SIGINT organization that can provide the oversight, direction, control, and analysis of all aspects of SIGINT that range from the strategic to tactical levels. With this, the Army should return to the concept first envisioned by the Intelligence Organization and Stationing Study—the TCAE.

Understanding the Structure of a Theater Force

The Army's support to the geographic combatant commands (GCCs) is rooted in the Army Service component command (ASCC). The ASCC, the proponent for the land domain, is physically or virtually present in the unified combatant command theaters around the world.[2] The Army's force is tailored according to the military and strategic threats that exist for that theater. Consequently, INSCOM aligned each of its MIB–Ts to be the Army's primary intelligence support for their respective theaters.

It is vital that SIGINT supporting ASCCs perform functions at the operational level, being the bridge between the strategic and the tactical. As such, SIGINT must support the combatant commander's operational planning and intelligence requirements. However, these requirements for each theater are unique and affected by factors that include geopolitical relationships, threat situations, geography, and popular support for U.S. objectives in that theater.

As a theater element, SIGINT must be ready to simultaneously provide operational intelligence support to higher commands and push relevant, nationally collected intelligence to the tactical level—and often to interagency partners.

It is at the operational level where SIGINT must concentrate on collecting, analyzing, evaluating, and reporting information that identifies strategic and operational centers of gravity. The exploitation of these centers, through lethal or nonlethal operations, will achieve national and theater objectives. Additionally, it is at the operational level where we must analyze a threat's capabilities, vulnerabilities, and probable intentions.

Theater TCAEs (T–TCAEs), known in the past as the echelons above corps TCAE, would be critical to this effort. The T–TCAE would operate under the SIGINT legal authorities given to the MI SIGINT company/battalion found in each MIB–T. Its mission would be to conduct SIGINT operations in response to theater-level requirements, primarily those of the GCC and ground component commands, but also the assigned regionally aligned forces. While theater ground component commands retain SIGINT operational tasking authority and SIGINT direction, it is the T–TCAE that will provide the SIGINT technical support and mission management functions. The T–TCAE would perform collection, processing, exploitation, dissemination, analysis, and reporting of SIGINT via both tactical and strategic reporting channels. The T–TCAE would also deploy and manage tactical assets in support of the theater for the purposes of collection and geo-locating targets.

With integration into national-level databases either via a SIGINT operational tasking authority-based mission correlation table or via an NSA-delegated mission correlation table, the T–TCAE would be responsible for maintaining

SIGINT databases for both GCC and regionally aligned force-subordinate SIGINT forces that are either deployed or may be deployed in theater. It would serve as the theater ground component command's SIGINT point of contact for other T–TCAEs and the Army TCAE. It would also serve as the SIGINT point of contact for national SIGINT support organizations operating in the theater and any partner nation military SIGINT relationships.

Ultimately, the T–TCAE would be the Army's highest technical control architecture within its theater of operation. The T–TCAE would provide a single point of contact between the Army and any national SIGINT operations, ensuring a cooperative and mutually supportive SIGINT strategy, ultimately linking tactical to national objectives and ensuring that the combatant command is fully prepared to accomplish its objectives.

To date, the 66th MIB–T and the 470th MIB–T have begun to align their SIGINT forces into a TCAE structure. At the 470th MIB–T, the TCAE strives to organize the SIGINT personnel, assets, and missions to closely mirror that which is described in Chapter 5 of the historical (1991) FM 34-37, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations.*[3] While relevant updates are necessary, the result will be an agile SIGINT force that can answer national requirements as part of a nationally delegated mission, while providing forward collection and cryptologic support to both the ASCC and the GCC. While this concept is in its infancy in support of U.S. Southern Command (SOUTHCOM) (operational for less than a year as of this writing), SIGINT forces at the 470th MIB–T are already postured to quickly adjust missions to support emerging contingencies in the SOUTHCOM area of responsibility.

Endnotes

1. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, n.d., 2, https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. U.S. Army South is an example of an Army Service component command that is physically located in the continental United States but virtually present in its area of responsibility.

3. Department of the Army, Field Manual 34-37, *Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations* (Washington, DC: U.S. Government Publishing Office, 15 January 1991 [obsolete]).

Mr. Scott Hammon serves as the senior signals intelligence (SIGINT) advisor and director of SIGINT operations for the 470th Military Intelligence Brigade-Theater. He retired from the Army as a sergeant major (SGM) with 26 years of active service, with assignments including G-2 SGM, Special Operations Team SGM, and SIGINT operative for a national-level, brigade-sized special mission unit. He has completed all National Cryptologic School SIGINT requirements and is a member of the National Security Agency Reporters Board for Crime and Narcotics.

GREAT SKILL Program

Military Intelligence Excepted Career Program

Our Mission

The GSP identifies, selects, trains, assigns, and retains personnel conducting sensitive and complex classified operations in one of five distinct disciplines for the Army, DOD, and National Agencies.

Who are we looking for?

Those best suited for this line of work do not fit the mold of the "average Soldier." Best qualified applicants display a strong sense of individual responsibility, unquestionable character, good interpersonal skills, professional and personal maturity, and cognitive flexibility. **Applicants must undergo a rigorous selection and assessment process that includes psychological examinations, personal interviews, a CI-scope polygraph and an extensive background investigation**.

Basic Prerequisites:

- Active Duty Army.
- 25 years or older.
- Hold a TS/SCI clearance.

For a full list of prerequisites, please visit our website (SIPRNET www.aoa.north-inscom.army.smil.mil/great_skill) or contact the Accessions Team at gs.recruiting@us.army.mil

How INSCOM Supports Intelligence Readiness in Europe

by Mr. Steve Hughes

Zapad-17: Russia's Annual Strategic Command Staff Exercise

In September 2017, the Russian military conducted its annual strategic command staff exercise, Zapad 2017 (Zapad-17), in the Western Military District bordering Estonia, Latvia, Lithuania, and Poland. Zapad is one of four quadrennial strategic military exercises that had ceased for several decades near the end of the Cold War.[1] In 2008, Russia resumed its large-scale annual strategic exercises, and cycles them among four regions: Zapad ("West," last held in 2013), Vostok ("East," 2014), Tsentr ("Center," 2015), and Kavkaz ("Caucasus," 2016). Since 2008, Russia has conducted three significant military interventions in Georgia, Ukraine, and Syria. A critical enabler for these successful interventions was the use of military deception. These deception operations used the annual strategic and snap exercises [short or no notice drills] as covers for foreign military intervention.[2] It came as no surprise that European nations sharing a boarder with Russia's Western Military District were uneasy about the extent of similar operations along their borders. Zapad-17 provided an opportunity for the U.S. Army Intelligence and Security Command's (INSCOM's) European-aligned military intelligence brigade-theater (MIB–T) to assess Russian activities and to support U.S. Army Europe (USAREUR) and U.S. European Command (EUCOM) in their efforts to assure regional stability through collective deterrence for our partners and allies.

Adding to the anxiety of Western Europe are examples in which Russia has used exercises to pre-position or permanently station troops in sovereign nations such as Georgia and Ukraine. After the Kavkaz exercise in 2008, Russian troops, which were operating in Georgia as part of an exercise, remained and within 5 days of the exercise's completion an additional 40,000 troops arrived. During the 2014 illegal invasion of Crimea, Russia used a snap exercise to position forces and quickly moved to occupy areas on Ukrainian soil in conjunction with unmarked paramilitary forces.

In an attempt to mitigate the risk of escalations, European nations, the United States, Canada, and Russia signed the Vienna Document in 2011 (VDoc11). VDoc11 was a renewal of agreements beginning in 1990 that set parameters for military exercises and operations in order to reduce instability across Europe. Some of the provisions of VDoc11 centered on the reporting of force utilization quantities in the zones of application. The agreement established thresholds that would initiate warnings and observation requirements in order to monitor and reduce escalation risks.[3] In accordance with VDoc11, Russia officially released its participating troop counts in its planned strategic exercises. The North Atlantic Treaty Organization (NATO) estimates, however, assessed actual troop participation levels well above Russia's published troop strength. VDoc11 states that once military personnel strength reaches 13,000 for a given exercise, the signatory nations would then dispatch observers to monitor the exercise.

Zapad-17 was a highly visible exercise that attracted attention from the press and European governments because NATO has historically seen Russia's strategic and snap exercises as destabilizing events. Moscow announced that in Zapad-17, Russian troop strength would be 12,700 soldiers. NATO's estimation of participating personnel was approximately 70,000, with some sources reporting over 120,000 participating troops in the exercise, well over the Russian reported figures.[4] Russia deliberately misrepresented its military strength in this exercise in order to circumvent the agreement it had signed. Russia's willingness to disregard signed agreements and obfuscate troop numbers contributes to uncertainty and strategic anxiety in Europe. It is among the reasons why Europe is alarmed about Russian activities in the Baltics.

With this in the forefront, the USAREUR commander warned Europe that Russia could use these exercises to station and leave behind both troops and equipment in Belarus as part of Zapad-17.[5] Russia has long considered Belarusian compliance with Moscow's objectives as one of its vital national interests. Recent relations between Moscow and Minsk had been strained over a dispute in which Russian courts ruled that Belarus owed close to one billion U.S. dollars to a Russian corporation. As tensions mounted, it seemed more plausible that Russia would take measures to secure its access to Kaliningrad through Belarus in

conjunction with the Zapad-17 exercise. Eventually Russia eased some tension by providing a loan to Belarus exceeding the claimed one billion dollar debt. Although no escalation of hostility between Western Europe and Russia occurred during the exercise, it remained a high priority for European leaders and the European theater combatant commander.

INSCOM—A Critical Enabler

GEN Curtis M. Scaparrotti, the EUCOM commander, testified to the Senate Armed Services Committee that Russia is deploying military and nonmilitary tools in an effort to re-exert its dominance and advance its interests. Russia has deployed overt and covert asymmetric weapons short of military conflict, including an assortment of cyberspace operations, disinformation, propaganda, economic warfare, and assassinations. In an effort to confront the growing Russian threat, EUCOM realizes that it must adapt—it must adjust to a "posture, plans, and readiness" model in order to promote stability in theater.[6] To this end, EUCOM must—

- Match and outpace the advances and modernization of its adversaries.
- Invest in the tools and capabilities needed to increase effectiveness across the spectrum of conflict.
- Ensure it has a force that is credible, agile, and relevant to the dynamic demands of the European theater.

In order to set the theater, EUCOM emphasizes five focus areas:

- Intelligence, surveillance, and reconnaissance (ISR) collection platforms that improve timely threat information and strategic warning.
- Land force capabilities that deter Russia from further aggression.
- Enhanced naval capabilities for antisubmarine warfare, strike warfare, and amphibious operations.
- Pre-positioned equipment to improve crisis response.
- Enhanced missile defense.

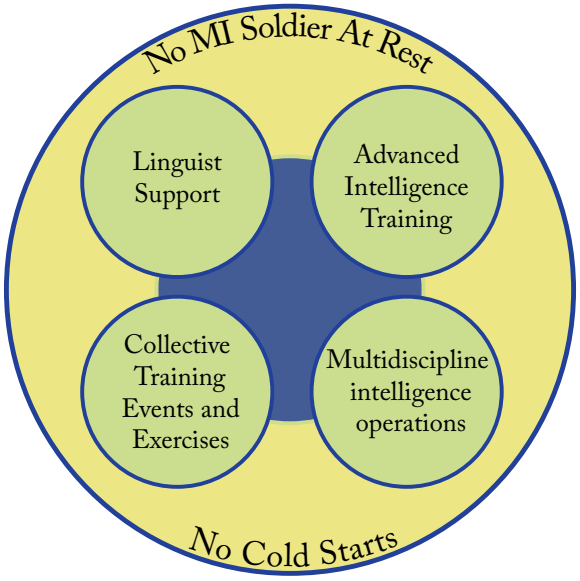
Enabling these areas will allow EUCOM to enhance its posture to set the theater, and INSCOM is a critical force provider and integrator that will support EUCOM's intelligence readiness.

EUCOM leads theater security cooperation in Europe, and INSCOM is the military intelligence (MI) enabler for U.S. Army organizations assigned to the theater. INSCOM's mission command of operational intelligence forces provides robust capabilities from across the intelligence community as immediately available resources in direct support to EUCOM and USAREUR. Operational tempo and a dynamic, collaborative environment in Europe require extensive resourcing through INSCOM. INSCOM's core contributions include—

- Linguist support.
- Advanced intelligence training.
- Administrative, logistical, and technical support to collective training events and exercises.
- Multidiscipline intelligence operations.

INSCOM manages manning, equipping, training, certifying, and supporting MI forces to ensure "no MI Soldier at rest; no cold starts."[7]

INSCOM supports EUCOM's intelligence readiness through various mechanisms: the Army Foundry Intelligence Training Program; aerial intelligence/processing, exploitation, and dissemination; and MIB–Ts are among those valuable resources available from INSCOM to support EUCOM.



Core Contributors to Intelligence Readiness

INSCOM administers the Foundry Program through the MIB–T and the functional leads for each intelligence discipline. The Foundry Program provides commanders with training tools to meet technical intelligence training requirements and maintain individual intelligence certifications. Soldiers participating in the Foundry Program receive technical training that builds on institutional, unit, and individual training. The program also allows units to train on distributed processing, exploitation, and dissemination architectures. Foundry training reflects the current and changing operating environment and increases functional and regional expertise while developing and expanding contact with the intelligence community.[8]

Foundry in EUCOM falls under USAREUR's designated MIB–T, the 66th MI Brigade, and supports other

organizations within EUCOM and U.S. Africa Command areas of responsibility (AORs). The European Foundry platform is a physical location providing reachback support for MI Soldiers deployed within the AOR, and it hosts live-environment training events for rotational units, enhancing Soldier proficiency to support theater operations. The European Foundry platform provides—

- Classified network connectivity.
- Regional expertise.
- MI equipment augmentation and training.
- Access to expertise from national-level intelligence agencies.
- MI leadership development.
- Senior leader engagements.

Beyond training, INSCOM helps set the theater in Europe through aerial intelligence support. The 116th MI Brigade is subordinate to INSCOM; it tasks, collects, processes, and provides feedback for multiple organic and joint aerial ISR missions.[9] In a combatant command, where the commander has access to ISR resources, INSCOM and 116th MI Brigade support the theater by augmenting resources and de-conflicting airspace. INSCOM is thus able to complement rather than compete for limited resources, and it advances EUCOM's current objectives with ISR collection platforms that provide timely threat information and strategic warning.

The MIB–Ts serve as anchor points to enable intelligence readiness in their designated theaters. In USAREUR, the 66th MIB–T is the theater anchor point for Europe, and it conducts national to tactical multidiscipline operations providing intelligence support to commanders. The anchor point concept is "the method for leveraging Brigade, other U.S. Army Intelligence and Security Command (INSCOM), and Intelligence Community capabilities to enable operational reach for contingencies, crisis, or exercises. The concept also explains how the TIBs [MIB–Ts] act as our Anchor Point for connectivity, intelligence fusion, and integration of commander intelligence requirements for forces operating in support of assigned theaters."[10] The 66th MIB–T employs collectors, maintainers, and analysts to provide theater-wide intelligence support to answer the combatant commander's intelligence requirements. These MI Soldiers will inform commanders, enabling them to understand, deter, and defeat adversaries. As an anchor point, the brigade supports regionally aligned forces by familiarizing those Soldiers with the AOR.[11] Finally, the 66th MIB–T works closely with multinational partners to strengthen strategic relationships.

Looking to the Future

In 2018, INSCOM and the 66th MIB–T hosted a tabletop exercise (TTX) in order to understand and assess the readiness of the intelligence warfighting function in Europe in the event of a repeat of Russia's 2008 and 2014 aggressions. The exercise incorporated observations from Zapad-17, and the outcome will allow INSCOM and the 66th MIB–T to better posture capabilities and inform future initiatives against peer threats.

First, the TTX underscored the importance of Foundry training in advance of potential conflicts. Rotational and major subordinate commands need to maintain intelligence proficiency and readiness. INSCOM can strengthen the European Foundry platform with training, equipment, and personnel.

Second, the TTX simulated INSCOM and the 116th MI Brigade's support to the EUCOM AOR with theater ISR assets such as Guardrail. This requirement was emphasized during Zapad-17 when aerial and terrestrial ISR operations provided critical situational awareness on Russian military activities and capabilities.

Finally, the TTX tested the efficacy of the concept that MIB–Ts are anchor points. Enabled units, such as the 66th MIB–T, would provide theater-wide intelligence support and technical and regional expertise to build a common operational picture across EUCOM.

EUCOM and the U.S. Congressional Armed Services Committees have underscored the value of cooperation and partner building in Western Europe, especially among those nations whose borders lie on the Russian front. Senator Jack Reed, the ranking member of the Senate Armed Services Committee, stated, "The NATO alliance remains strong and is grounded in a shared vision of an integrated and stable Europe rooted in respect for sovereignty and political and economic freedom." He also stated that we need to "send a strong signal of our unwavering support for the alliance."[12] Strengthening and sustaining relationships with multinational partners enable a stronger presence and allow opportunities to shape the environment now. We must regenerate "our abilities for deterrence and defense while continuing our security cooperation and engagement mission. This requires that we return to our historical role as a command that is capable of executing the full-spectrum of joint and combined operations in a contested environment."[13]

Conclusion

During Zapad-17, the world watched in anticipation to see if Russia would use this exercise to disguise its attempts to once again invade its neighbors. Ultimately, an incursion

into Belarus did not occur; however, Russia maintained its deceptions against NATO and obscured military strength estimates during the exercise. With Zapad-17, Russia exercised its naval and unmanned aircraft system operations, the capture of the Baltic states, and bombings of Germany and other NATO member countries. It also rehearsed attacks on neutral countries like Finland and Sweden.[14] It is during exercises like Zapad-17 and the TTX that the 66th MI Brigade, INSCOM, and the intelligence community learn valuable lessons about the peer threats we face.

Endnotes

1. Dave Johnson, "ZAPAD 2017 and Euro-Atlantic security," *NATO Review* (14 December 2017), https://www.nato.int/docu/review/2017/Also-in-2017/zapad-2017-and-euro-atlantic-security-military-exercise-strategic-russia/EN/index.htm.

2. Simon Saradzhyan, "100,000 troops will engage in Russia's Zapad-2017 war games," *The Washington Post*, September 13, 2017, https://www.washingtonpost.com/news/monkey-cage/wp/2017/09/13/100000-troops-will-engage-in-russias-zapad-2017-war-games/?utm_term=.ae344148642f.

3. "Vienna Document 2011," *Organization for Security and Co-operation in Europe* (22 December 2011), http://www.osce.org/fsc/86597.

4. Johnson, "ZAPAD 2017."

5. Emily Ferris, "The True Purpose of Russia's Zapad Military Exercises," *Foreign Affairs* (October 4, 2017), https://www.foreignaffairs.com/articles/russia-fsu/2017-10-04/true-purpose-russias-zapad-military-exercises.

6. "EUCOM Posture Statement 2017, Statement of General Curtis M. Scaparrotti, Commander, United States European Command," *Senate Committee on Armed Services* (March 23, 2017), http://www.eucom.mil/media-library/documents/2017.

7. Department of the Army, *Army Intelligence Training Strategy* (January 2013), http://www.dami.army.pentagon.mil/g2Docs/Foundry/Army%20Intelligence%20Training%20Strategy%202014.pdf.

8. Nick Rife, "Theater Intelligence Brigade Anchor Point Concept Supporting Distributed Common Ground System – Army," *U.S. Army Worldwide News*, June 29, 2015, https://www.army.mil/article/151380/Theater_Intelligence_Brigade_Anchor_Point_Concept_Supporting_Distributed_Common_Ground_System___Army/.

9. 116th Military Intelligence Brigade's Facebook page, https://www.facebook.com/pg/116th-MI-BDE-148355385714242/about/?ref=page_internal.

10. Rife, "Theater Intelligence Brigade."

11. Department of the Army, *Army Intelligence*.

12. "Opening Statement by Ranking Member Reed at SASC Hearing on US European Command," *Jack Reed, United States Senator for Rhode Island* (March 23, 2017), https://www.reed.senate.gov/news/releases/opening-statement-by-ranking-member-reed-at-sasc-hearing-on-us-european-command.

13. "EUCOM Posture Statement 2017."

14. Julian Röpcke, "Putin's Zapad 2017 simulated a war against NATO," *Bild*, 19 December 2017, http://www.bild.de/politik/ausland/bild-international/zapad-2017-english-54233658.bild.html.

References

Barnes, Julian. "NATO to Take Action on Trump Spending Call." *The Wall Street Journal*, May 21, 2017. https://www.wsj.com/articles/nato-to-back-trump-call-for-more-spending-1495364360.

Boulègue, Mathieu. "Five Things to Know About the Zapad-2017 Military Exercise." *Chatham House, The Royal Institute of International Affairs*. 25 September 2017. https://www.chathamhouse.org/expert/comment/five-things-know-about-zapad-2017-military-exercise.

"Independent International Fact-Finding Mission on the Conflict in Georgia." *Official Journal of the European Union* (September 2009). http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, CA: Rand Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1498.html.

"Opening Statement of Vice Admiral Frank C. Pandolfe, USN, Director for Strategic Plans and Policy, the Joint Staff, Before the House Armed Services Committee." *Armed House Services Committee*. 8 April 2014. http://docs.house.gov/meetings/AS/AS00/20140408/102108/HHRG-113-AS00-Wstate-PandolfeUSNF-20140408.pdf.

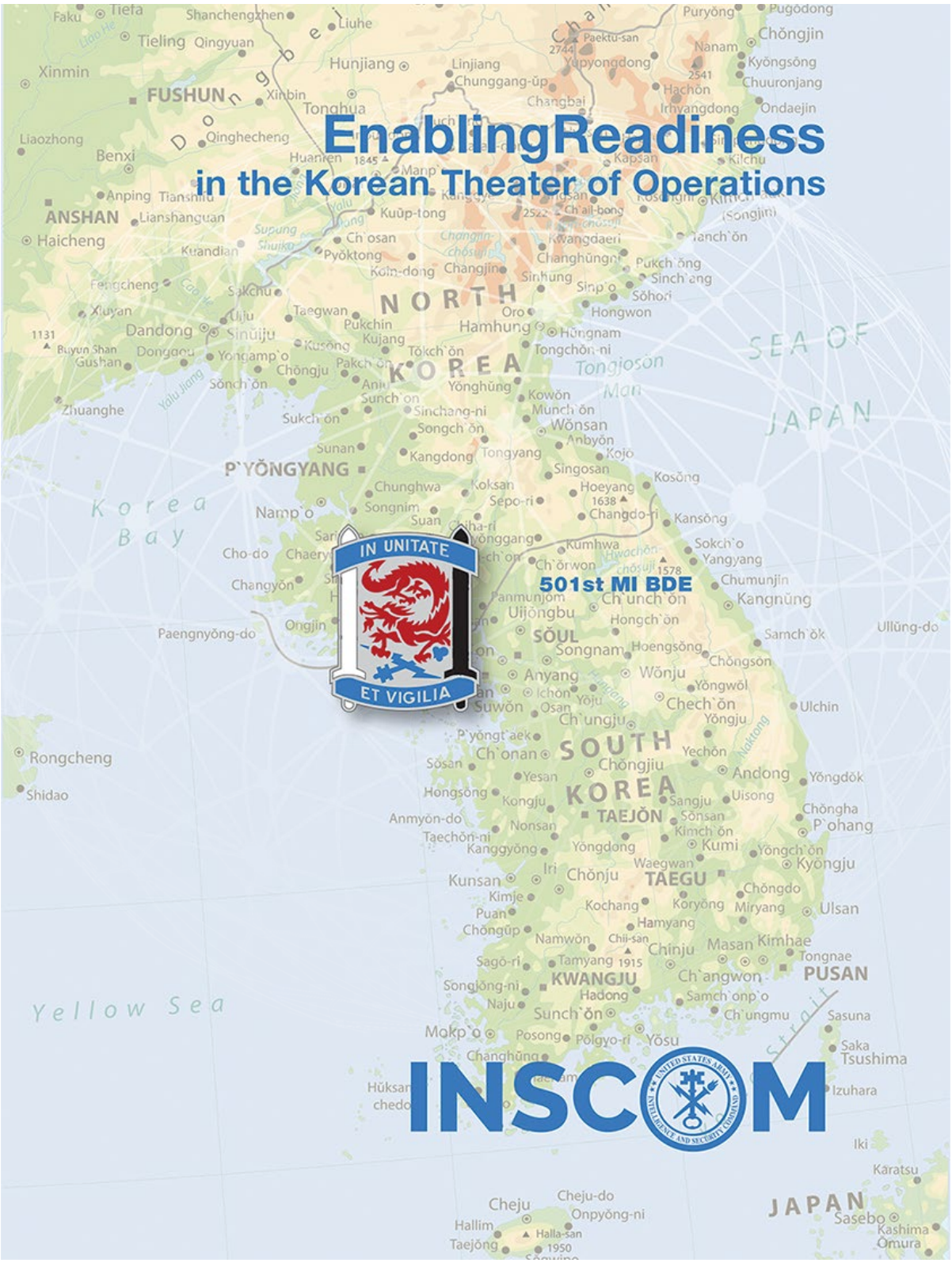
Standish, Reid. "The Ominous, Massive Military Exercises in Eastern Europe." *The Atlantic*, September 18, 2017. https://www.theatlantic.com/international/archive/2017/09/zapad-russia-baltics-lithuania-estonia-finland-trumpnato-eu/540126/.

Stelzenmüller, Constanze. "Order from Chaos, Why Europe needs America, a little." *Brookings*, September 29, 2015. https://www.brookings.edu/blog/order-from-chaos/2015/09/29/why-europe-needs-america-a-little/.

Techau, Jan. "The Politics of 2 Percent: NATO and the Security Vacuum in Europe." *Carnegie Europe*, September 2, 2015. http://carnegieeurope.eu/2015/09/02/politics-of-2-percent-nato-and-security-vacuum-in-europe-pub-61139.

U.S. Army website. "U.S. Army Intelligence and Security Command." n.d. https://www.army.mil/inscom/?from=org#org-about.

Mr. Steve Hughes is the senior signals intelligence advisor of the 66th Military Intelligence (MI) Brigade in Wiesbaden, Germany. He began his career in 1996 upon enlisting in the Utah Army National Guard as a 98G Arabic linguist, which included a 2-year activation after 9/11 supporting units at Fort Gordon, Georgia, until his enlistment completion in 2004. From 2004 to 2008, he worked as a mission manager and linguist for the 66th MI Brigade at the Army Europe Technical Control Analysis Element. In 2008, he transitioned to the Foundry Program at Fort Stewart, Georgia, where he served as the Deputy Director and Mission Manager until 2017. Mr. Hughes holds a bachelor's degree in international trade with a minor in Spanish from Georgia Southern University. He is a graduate of the Defense Language Institute with training in Arabic dialect. He has advanced training from the Army's Foreign Language Training Center in Moroccan dialect.



"North Korea will be among the most volatile and confrontational WMD [weapons of mass destruction] threats to the United States over the next year," the Director of National Intelligence, Daniel Coats, asserted in the 2018 *Worldwide Threat Assessment*.

To counter this threat, U.S. Army Intelligence and Security Command (INSCOM) made the Korean theater of operations its number one readiness priority. "You can only deter your opponent if your opponent believes that you have the will and the capability," says the Chief of Staff of the Army, General Mark Milley, "so readiness has a deterrent value as well as a war-fighting value." The 501st Military Intelligence Brigade-Theater (MIB–T) stands vigilant at freedom's frontier, ensuring that the Army, joint, and combined forces are prepared for any contingency on the Korean Peninsula. They keep their watch through unique data architectures, continuous training, and operational relationships; and with INSCOM's support and resources, the 501st MIB–T peers into the darkest places on Earth.

The Stage: Land of Interrupted Calm

by Colonel Derrick S. Lee and Major Margaret Dervan Hughes

Introduction

Since 2003, when the Democratic People's Republic of Korea (DPRK) announced its nuclear ambitions to the international community, a high-risk cycle of provocations and reactions has steadily increased tensions on the Korean Peninsula. After 15 years of nuclear demonstrations, economic sanctions, lethal and nonlethal provocations, aggressive rhetoric, and failed diplomatic initiatives and efforts, the risks of escalation and miscalculation have reached unprecedented levels since the outbreak of the Korean War. In 2006, DPRK successfully completed its first underground nuclear test, followed by an attempted long-range missile launch in 2009. In 2010, the DPRK sunk the Republic of Korea's (ROK's) Navy corvette *Cheonan*, killing more than 40 personnel on board, and conducted an artillery barrage against Yeonpyeongdo Island, resulting in the deaths of two ROK marines. Following Kim Jong-Il's death, DPRK, led by Kim Jong-Un, successfully launched a rocket-mounted satellite into orbit, demonstrating the potential for an intercontinental ballistic missile capability. In August 2015, an exchange of artillery fire after ROK soldiers struck a land mine along the military demarcation line brought inter-Korean tensions to a new level. However, tensions from tactical-level provocations gave way to strategic ones as DPRK conducted more than three dozen missile tests in 2016 and 2017. These tests included a demonstrated intercontinental ballistic missile capability that ranges most of the continental United States (CONUS) and two large-scale underground nuclear tests, one of which was likely a hydrogen bomb. Undeterred by the international community and the U.S.-led pressurization campaign, DPRK ended 2017 with threats to strike CONUS and conduct an atmospheric nuclear test.

Considering the lack of direct official military communications between the DPRK and the ROK, and the risk of rapid escalation and miscalculation, the need for unambiguous warning intelligence is critical. The 501st Military Intelligence Brigade-Theater (MIB–T) discerns meaning and intentions during armistice and periods of crisis in order to provide warnings of DPRK aggression. This is achieved through multidiscipline intelligence operations, including constant intelligence, surveillance, and reconnaissance (ISR) coverage; counterintelligence and human intelligence collection; and maintenance of the theater enemy ground common intelligence picture (CIP). Should conflict occur, the brigade must be prepared to transition to wartime operations to answer the ground component command and combined forces command (CFC) priority intelligence requirements. In addition, the 501st MIB–T has warfighting responsibilities, including area defense and operational decontamination requirements (chemical, biological, radiological, nuclear, and explosives), and tasks to support noncombatant evacuation operations and force protection.

Generating and Maintaining Readiness

In 2014, the Army transitioned from the Army forces generation model to the sustained readiness model; it designated regionally aligned forces to increase readiness and to better posture the Army to meet combatant command (COCOM) and theater operational requirements.[1] Concurrently, the U.S. Army Intelligence and Security Command (INSCOM) conceptualized the MIB–T as an anchor point to enable each MIB–T to support unique, multidiscipline intelligence requirements for each geographic COCOM and operational theater. Following the anchor point concept, the 501st MIB–T supports the U.S. Forces Korea and CFC commander's intelligence requirements and priorities to shape the operational environment and prevent conflict, while providing national, theater, and regionally aligned customers with access to operational intelligence, architecture, and training that is uniquely tailored for the Korea theater of operations (KTO).

Like all MIB–Ts, the 501st MIB–T is structured and resourced to conduct intelligence operations during phases 0 and 1—focused primarily on providing warning intelligence—and is not equipped to operate in a contested environment should deterrence fail. But unlike other geographic MIB–Ts that primarily reside outside operational theaters, the 501st MIB–T is located within range of North Korea's indirect fire and asymmetric capabilities, which are specifically designed to neutralize command, control, communications, computers, and intelligence nodes at the outbreak of conflict. As tensions escalate and a crisis is declared, the 501st MIB–T, at the current level of staffing and resources, will be challenged to

meet the theater intelligence requirements and functions that support large-scale combat operations and decisive action, to include providing theater CIP, warning intelligence, and intelligence integration support to force generation.

The application of the MIB–T anchor point concept in the KTO must be resilient enough to operate in a degraded communications environment, flexible enough to support the speed of maneuver beyond shaping operations, and sufficiently adaptable to mitigate a delay in the deployment of global response forces or regionally aligned forces due to adversary antiaccess/area denial operations. To achieve operational agility for the intelligence warfighting function and set conditions to ensure there are "no cold starts"—that units deploying into theater have requisite target familiarization and knowledge to support the full range of military operations—INSCOM, Eighth U.S. Army, and regionally aligned forces executed multiple initiatives to reinforce the 501st MIB–T as an anchor point. These include setting the theater, establishing intelligence handover lines, and developing target knowledge.

No Cold Starts: The MIB–T Anchor Point Concept in the Korea Theater of Operations Today

Until 2015, the principal CFC operations plan (OPLAN) featured several key planning assumptions that became outdated or needed revision. In some cases, a number of assumptions—such as the operational status of intelligence architecture and networks—simply wished the problem away, to facilitate further planning efforts. For the intelligence warfighting function, this meant that an intelligence "cold start" was inevitable in the KTO: plans lacked clarity and technical details regarding architecture; intelligence handover lines; support to reception, staging, onward movement, and integration; aerial ISR; processing, exploitation, and dissemination (PED); and sustainment. In 2017, under the direction of the INSCOM commanding general, the 500th MIB–T and the 116th Military Intelligence (MI) Brigade (Aerial) hosted a series of "set the theater" tabletop exercises designed to close various intelligence planning and capability gaps affecting the Pacific area of responsibility (AOR). The Eighth U.S. Army G-2 and the 501st MIB–T hosted a series of OPLAN rehearsal of concept drills designed to identify areas where additional PED and intelligence analytical capability and capacity were needed to address shortfalls. To resource these shortfalls, INSCOM held weekly working groups that tracked progress on materiel and staffing solutions.

Photo courtesy of INSCOM Public Affairs Office

Setting the Theater. Doctrinally, MIB–Ts are tasked to support force generation, which includes establishing theater intelligence communications and knowledge management architectures that enable collaboration among strategic, operational, and tactical intelligence organizations, including mission federation and replication through reachback operations.[2] The KTO's intelligence architecture requires redundant and survivable communications networks that will assure uninterrupted access to the theater CIP and enable potential intelligence reach PED operations during crisis or follow-on large-scale combat operations. A unique feature of the Pacific command's AOR is that it is the only geographic COCOM that hosts two MIB–Ts. As a result, the 501st MIB–T's intelligence architecture is inherently interwoven and reliant upon that of its adjacent MIB–T, the 500th MI Brigade. Moreover, because the 501st MIB–T operates in a combined environment with partners from the ROK military and their supporting national intelligence agencies, the brigade's intelligence architecture is further complicated by the requirement to share information on combined networks with cross-domain capabilities. This requirement is critical for intelligence-sharing purposes with ROK intelligence partners, for the integration of U.S. intelligence units and assets that will flow into theater, and for the execution of a seamless intelligence handover.

To increase the agility of the intelligence warfighting function in the KTO, INSCOM is establishing the Pacific PED architecture upgrade initiative at Fort Shafter, Hawaii. This initiative will upgrade intelligence architecture across the entire Pacific theater to support data replication, CIP dissemination, and potential federation of PED mission requirements. In keeping with retired LTG Mary Legere's vision for "no cold starts," a newly installed converged thin-client architecture with cross-domain capabilities and access to KTO-specific mission networks will employ "MI soldiers in dwell against live theater collection or production requirements, providing expert support to our Army forces forward, while sustaining hard-earned individual and unit readiness at home station for future contingencies."[3] KTO-specific mission networks include the Combined

Enterprise Regional Information Exchange System for the United States and South Korea, Greyrock, SECRET Internet Protocol Router Network, and Joint Worldwide Intelligence Communications System. Equally important, this initiative provides layered redundancy for CIP dissemination and PED mission federation in the event of surge mission requirements, critical losses, or a degraded communications environment. Planning is under way to make similar intelligence architecture upgrades and establish KTO-specific mission networks at other intelligence reach PED sites, at Fort Gordon, Georgia, and Joint Base Lewis-McCord, Washington.

INSCOM and the 116th MI Brigade developed an aerial ISR concept to support the KTO. This included providing redundant and layered data transport systems for the 3rd MI Battalion—the 501st MIB–T's aerial exploitation battalion—which will enhance mobility and survivability of aerial ISR platforms and sensors in support of large-scale combat operations. The concept features a robust sustainment and augmentation package, to include familiarizing CONUS-based pilots with KTO flight tracks and fitting additional CONUS-based aircraft to KTO specifications, which will build a ready reserve of aircraft that can support surge operations.

Intelligence Forward Passage of Lines. The 501st and 500th MIB–Ts collaborated with Eighth U.S. Army and regionally aligned forces to establish an intelligence handover concept that will facilitate the seamless integration of deploying forces by providing access to the CIP in all crisis or contingency scenarios. This includes integrating Active Component (AC) and Reserve Component (RC) capabilities via intelligence reach to support CIP replication and mission federation, which will enhance the theater analysis and control element's resiliency in a degraded communications environment. The 501st MIB–T is maximizing the capability provided by the brigade's aligned RC theater support battalion, the 368th MI Battalion, based at Camp Parks, California. The 500th MIB–T, based at Schofield Barracks, Hawaii, further reinforced these efforts by leading a theater-wide communications exercise that tested their ability to replicate and disseminate the theater CIP to regionally aligned and deployed forces.

Compared with the passage of lines definition in FM 3-90-2, Reconnaissance, Security, and Tactical Enabling Tasks Volume 2*, 22 March 2013, this particular forward passage of lines is metaphorical. Rather than a supporting unit physically passing through the 501st MIB–T's positions to support warfighters in Korea, it means that supporting units will pass and receive data through the 501st MIB–T's intelligence architecture.*

Using Active Duty for operational support orders, INSCOM and the Military Intelligence Reserve Command expanded the theater analysis and control element's "third shift" intelligence reach (manned by the 368th MI Battalion), which provides federated single-source geospatial intelligence analysis and all-source production and data management.[4] By integrating AC/RC capabilities, INSCOM and the 501st MIB–T have ensured layered and redundant replication of the theater CIP, and have increased geospatial intelligence PED capacity that will be sustainable in the long run. Although requests for forces to meet theater intelligence personnel shortfalls provide near-term solutions, this type of augmentation is unsustainable in the long term, as the sourcing mostly comes from AC units that are aligned or in support of other theaters and contingency operations.

Target Familiarization. Improvements in intelligence architecture are only effective if training and staffing investments keep pace with technology. Intelligence reach operations and the integration of regionally aligned forces require creative and robust language and cultural immersion training that maximizes exposure to the target environment. The 501st MIB–T must facilitate training opportunities for more than a dozen regionally aligned and supporting organizations in order to prevent "cold starts."

Recently, regionally aligned forces and global response forces, such as the CONUS-based 201st Expeditionary MI Brigade, 82nd Airborne Division G-2, and 300th MI Brigade (Utah National Guard), have used the Foundry live environment training (LET) program to develop target knowledge and familiarization of the PED mission in the KTO. In addition to obtaining critical familiarization with the 501st MIB–T's databases and target sets, regionally aligned forces are able to establish relationships and obtain cultural competence operating in a combined environment with the 501st MIB–T's ROK intelligence partners. Trained Soldiers are then able to extend knowledge management access to their units upon return to their home station. In 2017 alone, more than 80 MI Soldiers participated in the Foundry LET program on the Korean Peninsula—with projected expansion in 2018.

Because of an Armywide shortage of Korean linguists, INSCOM resourced a contract that provided the 501st MIB–T with 25 category II and III linguists, capable of augmenting both cryptologic and counterintelligence/human intelligence mission sets. In the event of conflict, the contract can be rapidly expanded to support theater-wide

linguist requirements in support of the Eighth Army and Army Forces–Korea.

No MI Soldier at Rest: The MIB–T Anchor Point in the KTO Tomorrow

The MIB–T anchor point concept sought to correct the theater intelligence brigade structure and doctrine after more than a decade of counterinsurgency warfare versus non-state actors in the U.S. Central Command AOR, which had inherently shaped the theater intelligence brigades by assuming risk in other theaters. In the KTO today, the requirement for tailored multidiscipline intelligence support in accordance with large-scale combat operations doctrine is evident. Army forces on the Korean Peninsula, including the 501st MIB–T, must possess the capabilities to support multi-domain battle while operating in contested areas in order to enable U.S. Forces Korea and CFC deterrence of DPRK aggression, and should deterrence fail, rapidly defeat DPRK aggression in support of the theater OPLAN.

INSCOM has made significant progress in addressing several critical planning and capability gaps that limited the 501st MIB–T's ability to provide uninterrupted intelligence support to the KTO during all phases of the CFC OPLAN. Major investments in intelligence architecture, RC/National Guard resources, and the Foundry Program have helped prevent intelligence "cold starts." Moreover, these investments have the potential to facilitate mission federation via intelligence reach in order to ensure that there will be "no MI Soldier at rest."

Shaping efforts in the KTO have highlighted unique aspects of the 501st MIB–T, which requires tailored materiel and manning solutions in order to provide continuous intelligence support to large-scale combat operations. Because of the 501st MIB–T's proximity to DPRK's long-range artillery systems and theater ballistic missiles, additional investments in expeditionary intelligence architecture capabilities will be necessary to increase the maneuverability and survivability of critical intelligence assets and mitigate delays in regionally aligned forces or global response force deployments.

The anchor point concept hinges on a collaborative approach by a network of major subordinate commands in order to reinforce any given theater. When executed in concert with adjacent functional and geographic military intelligence brigades, the MIB–T as an anchor point will allow INSCOM to flex intelligence resources to any crisis or contingency.

Endnotes

1. J. M. Bradsher, R.T. Dixon, B.P. Fleming, and J.J. Krause, *Concept Paper: INSCOM Theater Intelligence Brigade as an Anchor Point* (Fort Belvoir, VA: U.S. Army Intelligence and Security Command, 2014).

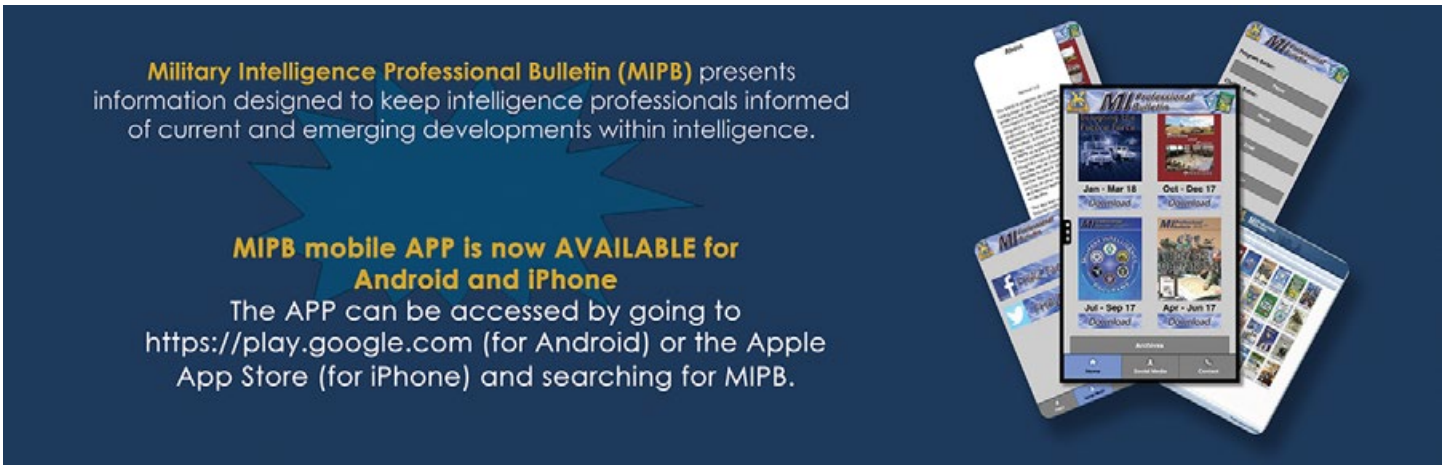
2. Department of the Army, Army Doctrine Reference Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, 31 August 2012).

3. Mary Legere, "Army Intelligence 2020: Enabling Decisive Operations While Transforming in the Breach," *Army* 62, no. 10 (October 2012): 165-169, https://www.ausa.org/sites/default/files/Legere_GB2012.pdf.

4. Kris Arnold, Jens Hansen, and David Hazelton, "Operationalizing the Army Total Force Policy: USFK's model for AC/RC Integration," *Military Intelligence Professional Bulletin* 42, no. 2 (April-June 2016): 8-9.

COL Derrick S. Lee is Commander of the 501st Military Intelligence (MI) Brigade.

MAJ Margaret Dervan Hughes is the 501st MI Brigade S-3.



Contact and Article

Submission Information

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

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

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

When submitting articles to MIPB, please consider the following:

- Feature articles, in most cases, should be under 3,000 words, double-spaced with normal margins without embedded graphics.
- We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- Although MIPB targets quarterly themes, you do not need to write your article specifically to that theme. We publish non-theme articles in most issues.
- Please do not include any personally identifiable information (PII) in your article or biography.
- Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

What we need from you:

- Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.
- A cover letter/email with your work or home email, telephone number, and a comment stating your desire to have your article published.
- **(Outside of USAICoE)** A release signed by your unit's information security officer stating that your article and any accompanying graphics and photos are unclassified, not sensitive, and releasable in the public domain. A sample security release format can be accessed via our webpage on the public facing Intelligence Knowledge Network website at: https://www.ikn.army.mil/apps/MIPBW
- **(Within USAICoE)** Contact the Doctrine/MIPB staff (at 520-533-3297 or 520-533-4662) for information on how to get a security release approved for your article. A critical part of the process is providing all of the source material for the article to the information security reviewer in order to get approval of the release.
- Article in Microsoft Word; do not use special document templates.
- Pictures, graphics, crests, or logos relevant to your topic. Include complete captions (the 5 Ws), and photographer credits. Please do not send copyrighted images. **Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg.** Photos must be at least 300 dpi. If relevant, note where graphics and photos should appear in the article. PowerPoint **(not in .tif/.jpg format)** is acceptable for graphs, figures, etc.
- The full name of each author in the byline and a short biography for each. Biographies should include authors' current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications.

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

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

VIGILANCE ALWAYS

INSCOM: On Beh
Supporting Global Intell

INSCOM is a Direct Reporting Unit; *DRUs provide broa*

INSCOM Staff Directorates enable mission command of the Army's globally dispersed Operational Intelligence Forces: 17x MSCs; 17.5K pax

G-1
DSN: 312-235-4675/6
- Manages manning for 17 x MSCs and HQ INSCOM

G-2
DSN: 312-235-4381/2
-G-2 dual hatted as INSCOM ACoS and the Army's SRA Dir
-INSCOM Security Ops Center is a spoke into the Army Insider Threat Hub
-Personnel Security Investigation Center of Excellence helps process SF 86
-Spt to MAVNI evaluations

Army Activity:
Insider Threat / Security Resiliency Activity

G-3
COM: 312-235-2975

DIR Operations
DSN: 312-235-1325
Oversees many activities, such as:
IP; AHOC; ACICA; FM AHOC/ACICA
DSN: 312-235-1881

G33 Oversees CUOPs
INSCOM Mission CMD Center
DSN: 312-235-2000

G37 Oversees Foundry
DSN: 312-235-1166

G3- Aerial ISR
DSN: 312-235-1900

Service Intelligence Enterprise Offices
Army OSINT Office
DSN: 312-235-1373
Army GEOINT Office
312-235-1461
Army Cryptologic Ops
312-235-6718
Army HUMINT Ops Center
312-235-1881
Army CI Coordinating Auth
312-235-1881

G-4
DSN: 703-235-4410/2
-Senior Logistician for Army Intel
-Global Integrated Facility & Log Spt
-Fielding & Life Cycle Sustainment
-Sustainment Spt to Foundry, TROJAN, TENCAP, DCGS-A
-Retrograde, Redeployment, & Materiel, Reduction Program for Intel Non-Standard Systems
-Op Intel Facility Planning, Sust, & Maintenance

CIO / G-6
DSN: 703-235-2468
- Provisions JWICS for Army
- Provisions MI SIPR/NIPR
- Directs Ground Intelligence Spt Activity
- Manages MI Data Centers
- Executes TROJAN comms down to the tactical layer

Ground Intel Spt Activity
COM: 703-706-2766

G-7
DSN: 312-235-1778
- Capability development
- Industry partnerships

G-8
DSN: 312-235-4419
- Manages CMDs $2.2B budget

Conducts:
- Mission CMD of Operational Intel Forces
- OSINT, SIGINT, CI, HUMINT, GEOINT, Biometrics
- All-Source Analysis, Production, Dissemination
- Support to Cyberspace Operations (DCO, DODIN, OCO)
- Theater Aerial ISR Operations
- Intelligence Knowledge Management

Delivers:
- Advanced MI Skills Training & Collective Training Support
- Linguist Support
- Specialized Capability Development
- Intel-Related Logistics, Contracting, and Comms
- Total Force Operations

Supports:
- Deploying Units and RAF
- CCMD / ASCC / SOCOM / JTF / Army / Joint
- National Intelligence Community

INSCOM Special Staff includes:
- The only Intelligence Law Office in the Army
  SJA: COL Jonathan Howard // DSN 314-706-2555
- An Intelligence Oversight Office that enables CG to execute Army-wide cryptologic oversight responsibility
  Snr Advisor: Mr. Larry Croce // DSN 314-706-2666

INSC
- S
- M
- P
- C
- T
- In
- S

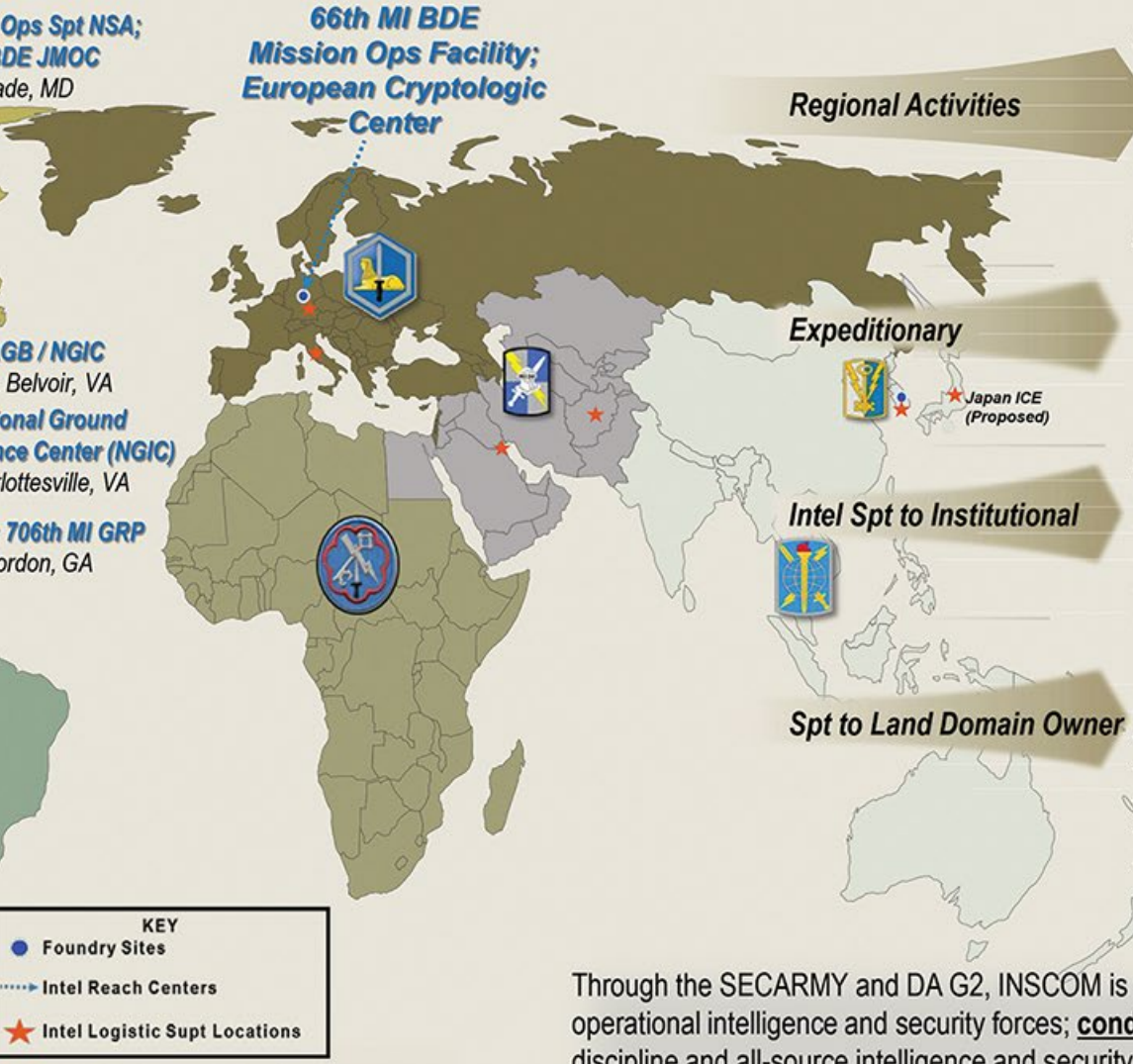
Foundry POCs:

INSCOM	Ft. Bragg 910-908-4878	JBLM 253-967-2793	Ft. Campbell 270-956-2907
	Ft. Hood 254-288-4212	Ft. Bliss 915-741-4208	Ft. Carson 719-524-1024
	Europe DSN: 314-474-2587	Ft. Irwin 760-380-3379	Ft. Polk 337-531-2147
USAR ARNG	MIRC 703-806-6398	Camp Bullis 210-295-7549	Ft. Gillem 404-469-3169
	Ft. Dix 609-562-5123	Draper 801-432-4399	Los Alamitos 562-936-1774

alf of the Army…
igence Operations 24/7

INSCOM
United States Army
Intelligence and Security Command

ad, general support to the Army not otherwise available



Set the Theater

- MIB–T: Anchor Point
- Shape the Environment – Enable SU
- Readiness – Foundry
- Advanced Skills – SMEs

Reinforce the Warfighter

- Win Wars
- Capability / Capacity Gaps
- Extend the Intel Enterprise (GISA/TROJAN)
- Reach Centers
- INSCOM Support Elements

Modernization ISO Lethality

- Future Army
- Capability Gaps
- Hard Targets
- Insider Threat
- OSINT

Joint Force Contributions

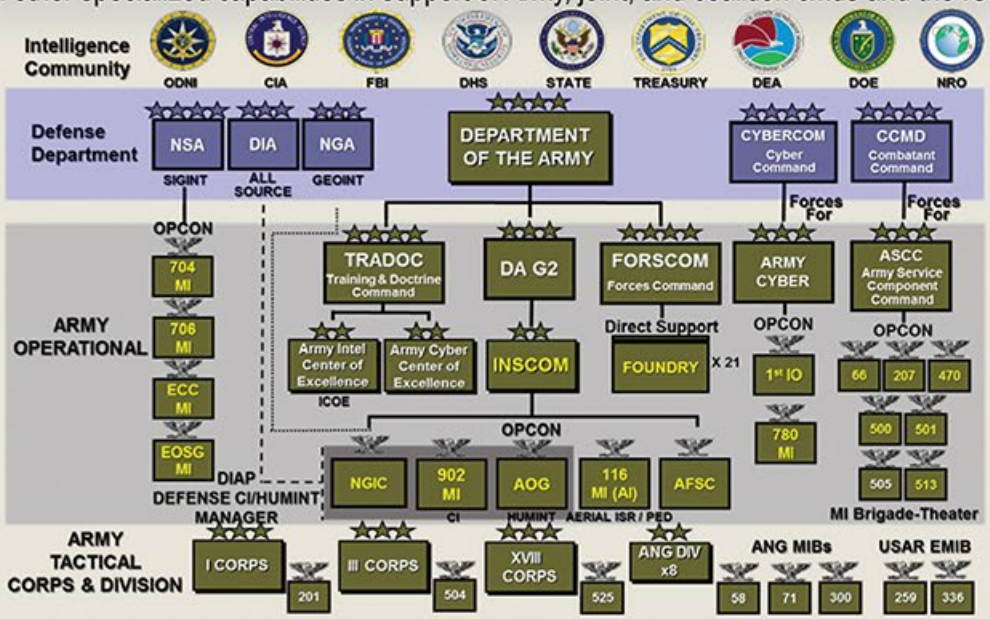
- Defense Intelligence Analysis Program
- Seams, Gaps, and Resources
- Army Requirements into UIS
- GFMAP Contributions
- Program of Analysis
- Units of Action (ex. ISR Weapons Tms)

Through the SECARMY and DA G2, INSCOM is tasked to execute mission command of operational intelligence and security forces; **conduct** and **synchronize** worldwide multi-discipline and all-source intelligence and security operations; **deliver** linguist **support** and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities in support of Army, joint, and coalition cmds and the IC

COM CG Roles and Authorities:

- ervice Cryptologic Component Cmdr
- ission Cmd Intel Ops
- roponent for Army CI & HUMINT
- apability Developer
- rainer (Foundry)
- formation Manager
- ecurity

Ft. Drum 315-772-4133	Ft. Stewart 912-435-1117
Ft. Riley 785-239-1256	Pacific 808-365-3622
Ft. Bragg 910-570-0536 (FASTIC)	IDTF 210-295-1142
Ft. Sherldan 847-266-2603	Cmp Parks 925-875-4501



INSCOM is the Operational Level of War Headquarters for the U.S. Ar
Reinforcing Intelligence efforts from the Tactical edge to the Strategic e
boundaries through the placement and access of its theater and functi
its ADCON and OPCON relationships.

INSCOM MI

INSCOM MI Brigades – OPCON to Theater… Set The Theater

513th MI Bde
Fort Gordon, GA
CDR: COL Deborah M. Ellis
CSM Jason C. Davis
COM: 706-791-1634

207th MI Bde
Vicenza, Italy
CDR: COL DavidConkle
CSM Michael C. Timme
DSN: 314-637-8464

505th MI Bde (MIRC)
Fort Sam Houston, TX
BDE OPCON & ADCON to MIRC
CDR: COL William Sears
CSM Richard A. Hall
COM: 210-295-8694

66th MI Bde
Weisbaden, GE
SIGINT Teams OPCON NSA European Cryptologic Center
CDR: COL Gregory L. Holden
CSM Christopher M. Matthews
DSN: 314-546-4013

470th MI Bde
San Antonio, TX
717th MI BN OPCON to NSA Texas
CDR: COL Ingrid A. Parker
CSM Lee K. Yoneyama
COM: 210-221-7574

500th MI Bde
Schofield Bks, HI
715th MI BN OPCON to NSA Hawaii
CDR: COL David P. Elsen
CSM Tammy M. Everette
DSN: 315-437-6900

501st MI Bde
Seoul-Yongsan, ROK
BDE OPCON To USFK
719th MI BN OPCON to NSA Pyeongtaek Mission Center
CDR: COL Derrick S. Lee
CSM Kristen L. Grover
DSN: 315-755-0588

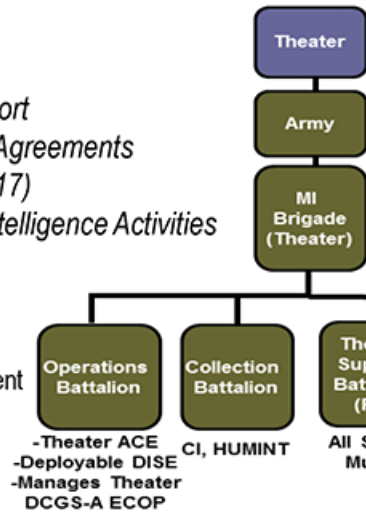
Military Intelligence Brigades – Theater (MIB–T) are Echelon Above Corps IN
Brigades, Assigned to the Combatant Command and OPCON to the Theater Arm
Component Command

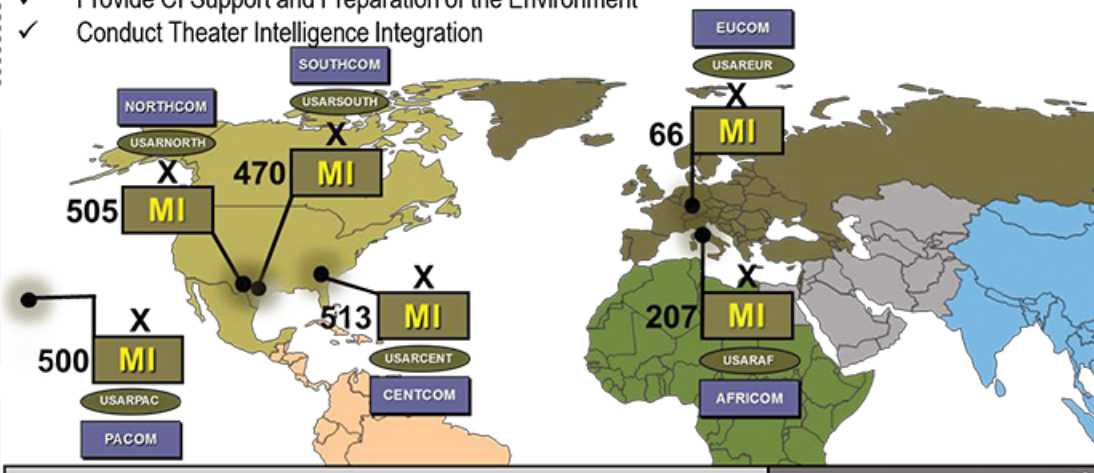
Theater Army's Set the Theater:

- *Establish Favorable Conditions through Exercises and Support*
- *Support the Formation of Bilateral or Multilateral Diplomatic Agreements*
- *Establish Area of Responsibility Transit Rights (FM 3-0, Oct 17)*
- ✓ *-MIB–T Set the Theater through conducting **Phase 0 / 1** Intelligence Activities that **Set Conditions** for Phases 2-4 Activities*

MIB–T Set the Theater Tasks:

- ✓ Set the Intelligence Architecture
- ✓ Develop Situational Understanding of the Operational Environment
- ✓ Conduct SIGINT Preparation of the Environment
- ✓ Conduct GEOINT Preparation of the Environment
- ✓ Conduct HUMINT Preparation of the Environment
- ✓ Provide CI Support and Preparation of the Environment
- ✓ Conduct Theater Intelligence Integration





OPCON to NSA

706th MI Group – NSA Georgia – CENTCOM Focus
-Shares Army SIGINT authorities with CG INSCOM
-Analysis and production
-Georgia Center for Language-dialect training
-CM assistance
-Support to JOIO – SIGINT PED

704th – NSA Washington & Colorado – Army's Strategic SIGINT BDE
-Army TCAE (NSA-W) - Army Access to SIGINT
-Foundry SIGINT Functional Lead
-Direct support to NSA, integrated into all operations and deployed activities
-Expeditionary SIGINT support
-TechSIGINT collection, reporting and anaysis

EOSG – Enables the NSA Directorate of Operations

ECC - Support to IC, EUCOM, AFRICOM

70
CDR:
CSM B
C

704
CDR: C
CSM
C

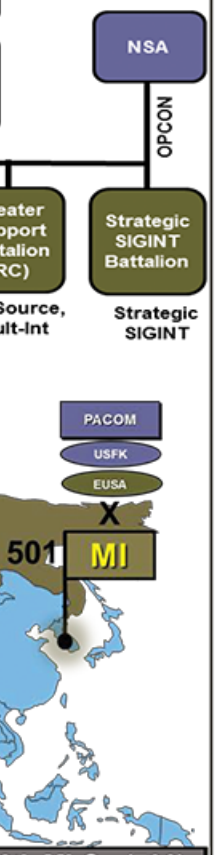
Expeditionary Ope
CDR: COL D
SMS
C

European Cryp
CDR: CO
D

my Intelligence Enterprise - Synchronizing, Shaping, Resourcing, and echelon. It is able to bridge intelligence related capabilities gaps and onal brigades (functional brigades tied to CSAs/IC), and by leveraging

SC Overview

SCOM
ny Service



6th MI Gp (706)
Fort Gordon, GA
COL John S. Chu
enjamin C. Lemon
OM: 762-206-1514

4th MI Bde (704)
Fort Meade, MD
OL Heidi A. Urben
M Corey E. Brown
OM: 301-622-0249

erations Spt Gp
Fort Meade, MD
ouglas J. Edwards
Sgt James Dickey
OM: 301-688-7738

otologic Center
Wiesbaden, GE
L Ralphael R. Bell
CSM John Deist
SN: 314-347-3678

INSCOM Functional Commands – General Support to US Army

116th AIB - Army's only A-ISR BDE
-Global employment of Army's Intelligence Weapons Team (IWT) and PED
-Conducts Intelligence, Surveillance, Reconnaissance and Target Acquisition (ISR/TA)
-Aerial GEOINT (FMV, LIDAR, G/DMTI, HIS, CCD, WAAS), SIGINT, COMINT, and Kinetic Capabilities
-Assets: JSTARS, EMARSS, MARSS, ARL, GRCS, Gray Eagle, Night Eagle, TACOP, Saturn Arch, Constant Hawk

116th MI Bde
Fort Gordon, GA
CDR: COL Daniel S. Mettling
CSM Kendall E. Bean
COM: 706-849-5046

902nd MI Group – Army's only CI BDE
-Foreign Intelligence Entities (FIE)
-International Terrorist Organizations (ITO)
-Insider Threats / Threat Awareness and Reporting Program
-Research, Technology, Critical Infrastructure Protect
-CI Analysis and Production
-CI Investigations
-Cyber CI Operations
-Foreign Travel Debriefs

902nd MI Gp
Fort Meade, MD
CDR: COL Jay W. Haley
CSM Steve L. Freedle
COM: 301-677-7400

National Ground Intelligence Center
-All Source and Geospatial Intelligence (Army GEOINT BN)
-Foreign ground force capabilities
-Military technologies: Weapons, C4ISR, Foreign Materiel, Technologies, Cyberspace, WMD, Identity Intel, Biometrics, WMD, Collection Strategy, and regional expertise.

NGIC
Charlottesville, VA
CDR: COL Dana Rucinski
CSM Jason H. Murray
COM: 434-980-7085

US Army Operations Group – Army's only HUMINT BDE
-Global reach
-Operational & Strategic level of war focus
-Live environment training
-Foundry HUMINT Functional Lead

AOG
Fort Meade, MD
CDR: COL Meriwether Sale
MSG Harvey Walker
COM: 301-833-8027

Army Field Support Center
-Force provider of CI, HUMINT, SIGINT, and Cyberspace
-Attaché recruitment
-Closed system personnel management
-MICEP Program Management

AFSC
Fort Meade, MD
CDR: COL Todd Hanlon
SGM Deborah Patterson
COM: 410-290-2586

OPCON to ARCYBER

780th Military Intelligence Brigade
-Cyberspace and SIGINT operations
-Live environment training
-CTC training support

780th MI Bde (ACB)
Fort Meade, MD
CDR: COL Brian D. Vile
CSM James M. Krog
COM: 301-833-6357

1st Information Operations Command
-IO and Cyberspace operations
-Deployable teams
-Reachback support
-IO Vulnerability Assessments
-CTC training support
-OPSEC MTTs and IO related courses

1st IOC (IOC)
Fort Belvoir, VA
CDR: COL Brian C. Mellen
CSM Cecil V. ReynoldsGitten
COM: 703-706-1560

The U.S. Army Intelligence and Security Command at Four Decades

1977 Part III: Regional Conflicts and Drawdown (1989 to 2001) 2018

by Mr. Michael E. Bigelow, INSCOM Command Historian

The end of the Cold War presented the U.S. Army Intelligence and Security Command (INSCOM) with a new set of challenges. Largely structured and deployed with the Cold War's priorities in mind, the command looked toward its role in a supposedly transformed world. Before much time had passed, however, INSCOM found itself committed to a series of conflicts unrelated to old American-Soviet tensions.

At the end of 1989, Panamanian strongman Manuel Noriega posed a threat to U.S. interests and provoked an American military intervention, Operation Just Cause. As American ground forces engaged Noriega's security forces, INSCOM's 470th Military Intelligence (MI) Group deployed its assets to support the operation. Intimately familiar with both the terrain and the disposition of Panama's armed forces, the group's teams provided spot reports throughout Panama City. Using their sources, 470th MI Soldiers obtained critical information on troop movements and locations of weapons caches. After the fighting, they helped identify and apprehend a number of Noriega's senior aides. For its role in the operation, the 470th MI Group was awarded a battle streamer.

Less than a year later, and halfway across the world, another crisis developed when Iraqi troops invaded Kuwait. American ground, naval, and air forces quickly deployed in Saudi Arabia to prevent further Iraqi expansion. As the situation stabilized, elements of INSCOM's 513th MI Brigade began to arrive on the Arabian Peninsula with a wide array of assets. Meanwhile, INSCOM shifted resources to ensure intelligence support for U.S. Army Central (ARCENT). Companies and teams from the 66th MI Brigade and reservists from the United States deployed to support the brigade; by Christmas 1990, the 66th MI Brigade's strength was over a thousand Soldiers.

INSCOM's professionals quickly proved their worth. A terrain team from the 513th MI Brigade assured Army planners that the desert area around Kuwait was trafficable by Army tanks and armored vehicles, a critical element in the planned operation of U.S. Central Command (CENTCOM). INSCOM technicians reconfigured the TROJAN system for use as a secure intelligence communication link that could transmit real-time information to the division level. Force protection teams helped secure ports, while technical intelligence teams trained U.S. forces on Soviet equipment used by the Iraqis.

For Operation Desert Storm, INSCOM elements played significant roles at several of CENTCOM's joint intelligence centers, and the 513th's echelons above corps operations center was expanded by a full battalion and placed in support of ARCENT's G-2. As the U.S.-led forces quickly defeated the Iraqi military, INSCOM counterintelligence personnel were among the first to enter Kuwait City where they seized enemy documents and provided support to force protection efforts. When combat operations ceased, human intelligence (HUMINT) and technical intelligence specialists from INSCOM screened and examined 50,000 Iraqi prisoners, thousands of documents, and numerous pieces of Soviet-made equipment.

The challenges of Operations Just Cause and Desert Storm placed large demands on the Army's intelligence community, and INSCOM was critical in meeting these demands. As a result of INSCOM's Cold War posture, the command's relevant organizations were well positioned to support emerging contingencies. For Operation Just Cause, the 470th MI Group had been in place under INSCOM for more than a decade when the crisis broke. For Operation Desert Storm, the 513th MI Brigade had a long-standing contingency mission to support ARCENT.

The Army began withdrawing from Iraq after Operation Desert Storm; the drawdown of U.S. military forces that were no longer needed for the Cold War began in earnest. For INSCOM, the most noticeable reductions occurred in Europe where, by 1995, it closed three major field stations—Berlin, Augsburg, and Sinop—and downsized the 66th MI Brigade to a provisional group. However, reductions were not limited to Europe: INSCOM had transferred most of its HUMINT assets to the Defense Intelligence Agency; in 1997, the Army inactivated the 470th MI Group and reduced the 500th MI Group in Japan.

In the midst of these reductions, it became apparent that the post-Cold War world would hold unforeseen and perhaps unforeseeable dangers. Throughout the 1990s, INSCOM was called to support peacekeeping, stability, counter-drug, and humanitarian operations in Africa, the Caribbean, the Middle East, and the Balkans. As the 20th century ended, new menaces arose in the form of terrorism and cyberspace warfare. The reduction of resources and redefinition of missions meant that INSCOM faced its greatest reorganization since 1977.

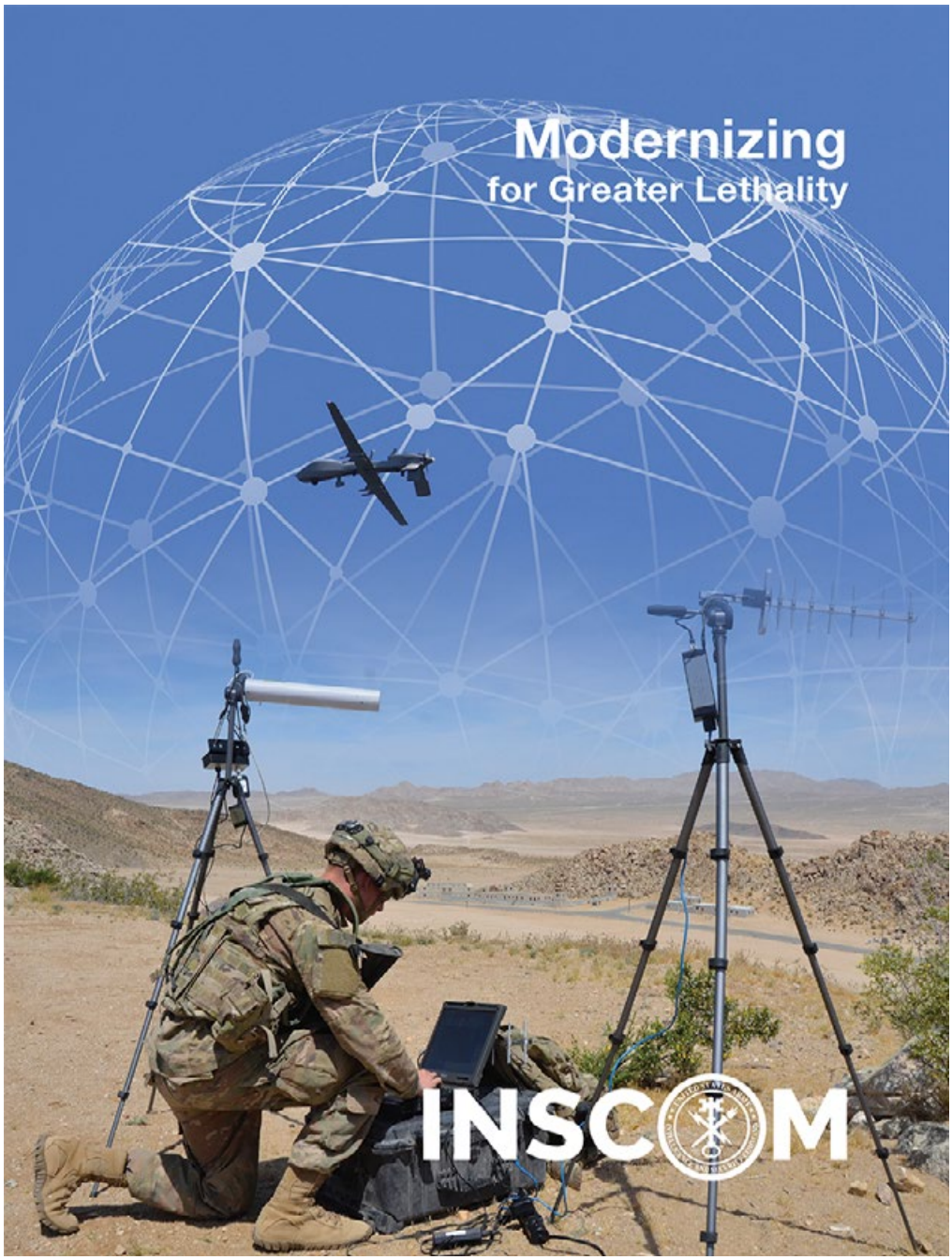
To respond more effectively to various regional crises, INSCOM reorganized once again, beginning in 1994. It merged the Army's intelligence production agencies to form the National Ground Intelligence Center. The center's capabilities were improved when the center moved into its new headquarters in Charlottesville, Virginia. INSCOM became the executive agent for two mission sites with cutting-edge technologies in Bad Aibling, Germany (under the 718th MI Group) and Menwith Hill, United Kingdom (under the 713th MI Group). At Fort Gordon, Georgia, INSCOM established a Regional Security Operations Center (RSOC) comprising personnel of the newly organized 702nd MI Group (later replaced by the 116th MI Group). The 513th MI Brigade, the command's rapid response unit, moved to Fort Gordon in 1994 and colocated with the RSOC, allowing the theater brigade personnel to participate in national missions. Finally, INSCOM established the Land Information Warfare Activity (LIWA), an action that proved prescient by the prominence of cyberspace operations by 2014. LIWA received the missions of defending the Army's automated communications and data systems from intrusion and developing Army capabilities for offensive and defensive operations in cyberspace.

The 1994 reorganization allowed INSCOM to coordinate the movement of intelligence specialists from worldwide units and deploy them where needed. Instead of operating at echelons above corps, INSCOM began to provide interaction between national-level agencies and tactical units. To strengthen connectivity, it developed intelligence cells (called Corps Military Intelligence Support Elements) to provide direct and dedicated support to commanders in the field. Improvements in automation and dedicated intelligence communications gave INSCOM an unprecedented ability to coordinate its subordinate units when deployed. The forward-deployed intelligence assets could access databases and other intelligence information located in the United States, Europe, or other secure areas. As INSCOM reduced its physical presence around the globe, it found itself working more closely with the intelligence community and with the Army's own tactical intelligence assets.

Mr. Michael E. Bigelow has served as the Command Historian for the U.S. Army Intelligence and Security Command (INSCOM) since 2006. He received a bachelor of arts in history from Colorado State University and a master of arts in military history from Temple University. He has written numerous articles for military publications such as Military Review *and* Military Intelligence Professional Bulletin*. Before becoming INSCOM's Command Historian, he served as an active duty military intelligence officer for 22 years.*

Photo courtesy of Wikimedia Commons

RAF Menwith Hill



The Secretary of the Army, Dr. Mark Esper, noted that "while we've been rightly focused on fighting and winning in Iraq and Afghanistan, China and Russia have invested in advanced technologies, professionalized their militaries, and changed facts on the ground that have reduced our military advantage. Both countries are modernizing their militaries at a pace that is steadily eroding our capabilities overmatch, and improving their ability to threaten our national interests." At this pivotal moment in history, the U.S. Army is embarking on a campaign to posture the future force with modern manned and unmanned ground combat vehicles, aircraft, sustainment systems, and weapons. These systems, coupled with "robust combined arms formations and tactics based on a modern warfighting doctrine and centered on exceptional leaders and Soldiers of unmatched lethality," will deliver an Army capable of thriving in the modern operating environment. Although the joint services recognize five domains in which we counter adversary adaptations—air, land, maritime, space, and cyberspace—the emerging multi-domain battle concept espouses that we must also confront adversaries contesting the electromagnetic spectrum and the information environment. As the Army meets the Secretary's charter to fully integrate the multi-domain battle concept into doctrine at every echelon over the next 10 years, the U.S. Army Intelligence and Security Command (INSCOM) plays a critical role. In addition to several other modernization efforts, INSCOM is leading the charge to advance the Army's intelligence architecture so that we can dominate in an era of unprecedented data. Decision makers at all levels depend on a system in which data is processed, exploited, and disseminated at the speed of mission command. INSCOM's Big Data strategy, which will enable the rapid analysis of data derived from a variety of platforms—ranging from aerial intelligence, surveillance, and reconnaissance systems to open source tools—recognizes the need to adapt and innovate, and it delivers an essential capability so that formations become more robust, agile, and lethal.

INSCOM Innovation and Modernization: INSCOM's Aerial Intelligence, Surveillance, and Reconnaissance

by Lieutenant Colonel Tony K. Verenna, Lieutenant Colonel Keith A. Haskin, Major Trevis C. Isenberg, Mr. Stephen A. Gasparek, and Mr. Marco A. Garavito

Organizational Modernization

The U.S. Army is modernizing and optimizing its aerial intelligence, surveillance, and reconnaissance (A–ISR). This effort will enable massed A–ISR to synchronize with operations, integrate with all-source intelligence, and facilitate control through simpler mission command architectures. Advances in multi-intelligence platforms, combined with high volumes of intelligence data and consolidation of A–ISR processing, exploitation, and dissemination (PED) functions, are increasing A–ISR efficiencies and synchronization at an unparalleled rate.

Before 2006, aerial exploitation battalions (AEBs) were assigned to U.S. Army Forces Command (FORSCOM) and served the corps echelon and below, while the 204th Military Intelligence (MI) Battalion (Aerial Reconnaissance) was assigned to the U.S. Army Intelligence and Security Command (INSCOM) and supported echelons above corps requirements. This arrangement provided limited A–ISR flexibility for commanders. In 2006, all AEBs and aerial reconnaissance battalions (ARBs) were consolidated at INSCOM. INSCOM's ability to provide A–ISR support to all echelons, from corps to brigade combat team (BCT) levels, was a major determining factor in assigning them under one command. The centralization of A–ISR mission command supported an aggressive modernization effort while fulfilling worldwide intelligence requirements.

INSCOM activated the 116th MI Brigade (Aerial Intelligence) in 2015, and for the first time all AEBs and ARBs (except the 3rd MI Battalion) were under a single command. The restructuring streamlined INSCOM's ability to provide tailored A–ISR packages worldwide in support of Army Service component command and joint intelligence requirements. This action also aligned the Army's 138th MI Company, Joint Surveillance and Target Attack Radar System, under the 116th MI Brigade. Today, every battalion in the 116th MI Brigade contributes to global A–ISR requirements and provides specialized geospatial intelligence (GEOINT), signals intelligence (SIGINT), and electronic warfare, which satisfy BCT-level requirements. Any INSCOM A–ISR asset can support any combatant command (COCOM) through the Joint Staff Global Force Management Allocation Plan process; when the AEBs were assigned to the corps, supporting a corps with external assets was more complicated.

Manned Fleet Modernization

The A–ISR fleet underwent an extensive modernization during this same period. Guardrail aircraft numbers were reduced, and the Guardrail SIGINT payload was modernized to exploit digital signals. In addition to Guardrail's Cold War-era "deep look" into denied areas capability, Guardrail received a near-vertical exploitation capability that was more suitable for supporting counterinsurgency missions. INSCOM is fielding two new A–ISR platforms in addition to the Guardrail: the Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS) and the Airborne Reconnaissance Low (ARL)-Enhanced, which will replace the ARL.

As combat operations in U.S. Central Command increased from 2001 to 2011, so did maneuver commanders' demand for additional ISR capabilities. INSCOM met the demand with an "ISR surge" and developed new sensor technologies under a rapid fielding approach called quick reaction capabilities (QRC). The plethora of new A–ISR systems included Constant Hawk, Saturn Arch, Desert Owl, Tactical Operations, Buckeye, Vehicle and Dismount Exploitation Radar, Copperhead unmanned aircraft system (UAS), and Warrior Alpha UAS. INSCOM aircrews supported the U.S. Air Force's multi-intelligence ISR mission known as Liberty until 2015, for which INSCOM provided all Liberty mission aircrew members, including pilots, aerial geospatial payload operators, and aerial SIGINT payload operators. This ISR surge provided corps, division, and BCTs with new SIGINT and electronic warfare capabilities and greater lethality against adversaries.

INSCOM also upgraded A–ISR ground stations in order to provide them access to the architectures of multiple intelligence disciplines, rather than just one—the National Security Agency Network. The early generation Guardrail ground baseline improved to become the Surveillance Information Processing Center. The latest generation of this ground station is the Operational Intelligence Ground Station (OGS), which is Distributed Common Ground System-Army (DCGS–A) compliant and supports the National

Security Agency Network, Joint Worldwide Intelligence Communications System, SECRET Internet Protocol Router Network, and coalition networks. Of 12 total OGS systems planned for fielding, 9 of them have been delivered to units since 2011; the last 3 will be operational by the third quarter of fiscal year 2018. Ground station modernization expanded dedicated Guardrail support and now includes a variety of platforms such as ARL, four variations of EMARSS, and a growing fleet of nonstandard QRC aircraft.

The introduction of nonstandard QRC platforms into the A–ISR inventory presented some technical challenges, but it unleashed innovations that accelerated modernization, and it continues to serve the intelligence community. Tactical common data links or satellite communication capabilities were added to many QRC systems, which enabled them to operate farther from ground stations and made them compatible with the OGS. Many systems began as GEOINT systems, but evolved into multi-intelligence payloads. This allowed the Army to quickly determine best of breed emerging technologies, which were then infused into A–ISR programs of record. The EMARSS family grew into four distinct configurations using new sensor technologies.

The EMARSS-GEOINT (EMARSS–G), first fielded in May 2017, demonstrates how QRC efforts can support cost-effective and mission-critical modernization. The EMARSS–G variant is the first INSCOM A–ISR aircraft that uses a multi-intelligence sensor rail configuration system, allowing the operating element to reconfigure between the wide-area aerial surveillance and light detection and ranging sensors at forward locations. This approach provides maximum flexibility for the supported unit. Lessons learned from unsuccessful QRCs informed the development of EMARSS–G, which divested the program of wasteful and ineffective features.

Today, more sensors and intelligence capabilities are available to maneuver commanders than ever before. Even though there are fewer airframes in the Army inventory, true multi-intelligence capabilities of today's A–ISR configurations provide greater capability. The reduction of the Guardrail fleet and EMARSS in four separate configurations has resulted in an increased level of support while providing more flexible and smaller fleets, which are logistically simpler to maintain. This means that INSCOM can do more with less, and the less is more reliable. Two AEBs currently operate EMARSS in support of COCOM requirements worldwide.

Unmanned Fleet Modernization

These modernization efforts were not limited to the manned A–ISR fleet. The MQ–5B Hunter UAS was upgraded from a full motion video-only capability to a multi-intelligence capability with the addition of aerial precision geolocation and a modern datalink.

The MQ–1B Warrior Alpha UAS was fielded to INSCOM as a QRC and provided INSCOM AEBs with their first organic strike capability. Their success and aggressive operational tempo prompted accelerated fielding of the MQ–1C Gray Eagle UAS with enhanced sensors. Two AEBs are deployed supporting warfighters in two separate areas of responsibilities with MQ–1C Gray Eagles. INSCOM is developing an extended-range MQ–1C airframe, which will double the Gray Eagle's current flight time and range.

The modernization of A–ISR platforms and ground stations necessitated PED architecture modernization. A–ISR systems could no longer be confined to dedicated ground stations at dispersed locations. INSCOM used lessons learned from the U.S. Air Force's Distributed Ground System architecture and developed PED capabilities that used a new distributed PED enterprise, called converged infrastructure. Converged infrastructure introduced cloud computing to the DCGS–A enterprise at Fort Gordon, Georgia, in January 2017, and it is now the Army's leading PED organization. The converged infrastructure PED architecture provides joint interoperability between U.S. Air Force and Army A–ISR. INSCOM is working to transition converged infrastructure to the Project Manager DCGS–A. The European PED service center, established in May 2017, now operates converged infrastructure, while fielding of converged infrastructure at the Pacific PED service center is under way. Converged infrastructure PED architecture has achieved initial operation capability at several FORSCOM Active Duty military intelligence facilities, and initial operation capability is planned for FORSCOM

Photo courtesy of INSCOM Public Affairs Office

U.S. Army Reserve and Army National Guard sites in the near future. FORSCOM and INSCOM units will retain their expeditionary PED capabilities with no impact to their deployability.

The overseas PED service centers have expanded all aspects of PED computing while offering alternate processing capabilities to the Fort Gordon PED facility and to the COCOMs. The consolidation of dispersed A–ISR PED manpower from several U.S. Central Command locations (Hunter Army Airfield, Georgia; Fort Hood, Texas; Fort Bliss, Texas; and Clay Kaserne, Wiesbaden, Germany) to Fort Gordon enabled federated management of all Army A–ISR PED. Since 2013, it has ensured that no MI Soldier would be at rest because the consolidation supported enhanced personnel readiness through better training logistics and simpler workforce management.

Because of the high operational tempo for A–ISR worldwide, the current major limiting factor for most A–ISR support is the individual dwell time requirements for aircrew members. Soldiers are intended to remain at home station between deployments twice as long as they are deployed; once INSCOM units deploy, the aircraft and sensors only return when they require depot-level maintenance or the mission has ended.

Persistent Stare on the Future

INSCOM is coordinating with the U.S. Army Intelligence Center of Excellence (USAICoE) to modernize the A–ISR fleet. The Next Generation A–ISR Working Group is a USAICoE initiative to pursue a DOTMLPF-P (doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy) study that seeks to address future requirements to the year 2035 and beyond. The DOTMLPF-P team is working to identify capability gaps, and to identify how to answer priority intelligence requirements in all phases of operations. The Next Generation A–ISR Working Group has divided its efforts into three time periods to focus on relevant questions for near-, mid-, and long-term requirements. **Near term.** The near-term phase covers the present through 2020. This portion focuses on current deployments and immediate threats using existing programs and technology. The team identifies existing systems, force structures, and doctrine to document how A–ISR currently operates and recommends changes to improve operations with what is available today. The ISR weapons team (IWT) concept was developed to answer many of the challenges A–ISR battalions face. The RC–12X Guardrail Common Sensor (GRCS) is an example of near-term planning. In 2017, U.S. European Command conducted an exercise in which the GRCS played a pivotal role in discerning enemy order of battle against a peer adversary during shaping operations. The exercise proved the importance of A–ISR during phase 0 and identified sensor capability gaps in contested airspace. INSCOM's industry partners used these findings to improve existing sensor technologies and integrate them with the GRCS. **Mid term.** Mid-term discussions focus on the years 2021 through 2025 and identify the capability gaps in sensor technologies to plan upgrades and replacements for today's sensor packages. It then aims to determine how to employ those emerging capabilities against relevant adversaries. **Long term.** Long-term planning looks beyond 2025 to deliver advanced sensor packages on upgraded platforms to execute missions against near-peer and peer adversaries in contested and congested airspace.

Economy of Force Through Remote Split Operations

INSCOM's unmanned A–ISR organizations are exploring a new Army operational paradigm known as Remote Split Operations (RSO). To explain, RSO means that a UAS flight crew anywhere in the world could launch an airframe from a foreign airfield and hand over its control to another aircrew located in the continental United States (CONUS) (or anywhere else in the world with the right data architecture).

RSO presents INSCOM with the opportunity to employ the Gray Eagle UAS in a more operationally flexible configuration and as a way to maximize the employment of UAS operators in spite of their relative scarcity.

In 2016, the Office of the Under Secretary of Defense for Intelligence conducted a comprehensive study of alternative methods and techniques to employ MQ–1C Gray Eagles. The study concluded that RSO presents the Army with opportunities to more efficiently employ Gray Eagles while continuing to provide a lethal A–ISR capability. LTG Robert Ashley, then U.S. Army Deputy Chief of Staff, Intelligence, directed INSCOM to explore the viability of RSO and confirm the results of the study.

In order to adequately assess the technical viability and operational benefits of RSO for AEB Gray Eagle companies, INSCOM conducted an RSO demonstration in 2017, and it will conduct an RSO proof of concept later in 2018. The RSO demonstration verified technical viability in two phases. In phase 1, INSCOM tested RSO from a single CONUS location and then from two CONUS locations. In phase 2, INSCOM tested RSO by handing over Gray Eagle controls from a location outside CONUS to a CONUS location.

The subsequent proof of concept will commence in the third quarter of fiscal year 2018; it will assess the operational viability and discern possible operational limitations

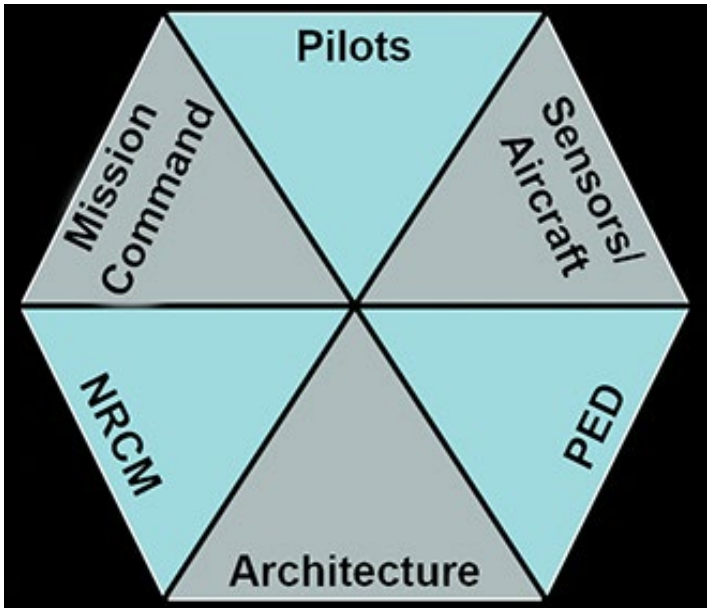
and constraints. The RSO proof of concept will also further assess the capability and reliability of Army transport data architectures to support Gray Eagle RSO operations.

ISR Weapons Teams: Improving Readiness for A–ISR

GEN Mark Milley stated during his first address to the Army in 2015 that "readiness for ground combat is—and will remain—the U.S. Army's number one priority." For the majority of Army units, readiness is reported through the unit status report (USR) to the highest levels of Army leadership and describes the units' ability to deploy and execute their missions. The force structure of A–ISR units as reported in the USR is based on obsolete models when the AEBs were assigned to the corps; the USR system is inadequate for INSCOM A–ISR units because they do not deploy in accordance with their modified table of organization and equipment configurations. In order to facilitate an accurate depiction of Army A–ISR readiness and accurately represent the way it deploys, changes must be made to the force structure of these units as well as the method for reporting readiness.

Beginning in October 2019, A–ISR units will deploy as IWTs and their force structures will change accordingly. Each IWT will consist of one, two, or three aircraft, depending on the type of asset requested, with accompanying crewmembers and mission command. PED is always included as part of the IWT but often operates through an intelligence reach element to reduce the footprint of deployed personnel. In the greater Army aviation community, there are units that already deploy in similar weapons team models. As the A–ISR units of action change, the way we report readiness will be adjusted to accurately report the overall readiness.

Six critical components of each IWT govern its readiness: pilots; sensors/aircraft; tasking, collection, PED, and feedback; architecture; nonrated crewmembers; and mission command. The availability of fully trained and qualified pilots is a critical piece to the functionality of the IWT. The typical IWT will include a 1.5 crew-to-cockpit ratio and will be accompanied by a small mission command element that manages the assets and crewmembers. The mission command element will also assist supported COCOM planners to understand the capabilities, limitations, and logistical needs of the IWT. Because PED functions occur through intelligence reach elements located in CONUS, the result is outstanding intelligence products. However, that model is dependent on a stable network infrastructure and sufficient bandwidth covering thousands of miles. If infrastructure is degraded, expeditionary PED capabilities will be necessary for the IWT to function. INSCOM will continue to confront these challenges as we modernize and optimize Army A–ISR, improving our readiness posture so that ground commanders receive the best intelligence available.



ISR Weapons Team Components

LTC Tony Verenna is the U.S. Army Intelligence and Security Command (INSCOM) Chief, G-3 Aviation and Air Sensors.

LTC Keith Haskin is the INSCOM Deputy Chief, G-3 Aviation and Air Sensors.

MAJ Trevis Isenberg is the INSCOM Operations Branch Chief, G-3 Aviation and Air Sensors.

Mr. Steve Gasparek is the INSCOM Senior Aerial ISR Engineer, G-3 Aviation and Air Sensors.

Mr. Marco Garavito is the INSCOM Unmanned Aerial Systems, G-3 Aviation and Air Sensors.

INSCOM

OSINT: Increasing Readiness by Leveraging the Digital Environment

by Mr. Daniel Zieminski

Disclaimer: Open-source intelligence is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement (Public Law 109-163). Only intelligence personnel perform this task. Only intelligence professionals may conduct OSINT activities due to the authorities and restrictions placed upon them in Executive Order 12333 as amended, DODM 5240.01, DOD 5240.1-R, DODI 3115.12, JP 2-0, and AR 381-10.

Introduction

The U.S. Government, through various agencies and organizations, has looked to open sources to augment other forms of information collection and mitigate their inevitable gaps. Now, recent U.S. Army efforts to refine and institutionalize the use of open-source intelligence (OSINT) are gaining momentum. The increasing global participation in the internet, combined with technological advances, highlights the benefits of OSINT as a viable form of intelligence for military operations.

In 2016, Army Directive 2016-37 outlined the policy for the Army's OSINT activities, citing earlier governing documents that codified OSINT language.[1] The Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, cites OSINT as a valuable source that must be integrated into the intelligence cycle in order to fully and completely inform U.S. policymakers, and charged each element of the intelligence community to use OSINT consistent with the mission of the element.[2] The National Defense Authorization Act for Fiscal Year 2006, Public Law 109-63, defines OSINT as "Intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[3]

As the overall amount of publicly available information (PAI) has increased, so has the confidence in relying on OSINT to make critical decisions. In mid-2017, the International Criminal Court issued an arrest warrant for Mahmoud Mustafa Busayf Al Werfalli. According to the warrant, Mahmoud, allegedly a commander of Al Saiqa Brigade in Libya, was accused of mass executions in or near Benghazi. This was the first arrest warrant issued by the International Criminal Court that solely took into account evidence collected from social media, one of the many forms of PAI.[4]

The value of OSINT lies in the ever-increasing amount of PAI available on the internet. The National Defense Authorization Bill for fiscal year 2017 has very specific language describing the use of PAI:

> ***"The committee notes that PAI use and exploitation is having a revolutionary impact on both operations and intelligence within the Department. Further, the committee recognizes that while intelligence activities have important uses for PAI, the Department also has unique operational uses and requirements for PAI that support force protection, targeting, battlespace awareness, and other traditional military activities. As a result, the demand signal for the operational use of PAI has increased across the force."[5]***

Department of Defense (DoD) Manual 5240.01, *Procedures Governing the Conduct of DoD Intelligence Activities*, updated the definition for PAI and the characterization of collection in order to reflect the current online open source environment, which set guidelines for OSINT. The manual defines PAI as "Information that has been published or broadcast for public consumption, is available on request to the public, is accessible on-line or otherwise to the public, is available to the public by subscription or purchase, could be seen or heard by any casual observer, is made available at a meeting open to the public, or is obtained by visiting any place or attending any event that is open to the public."[6]

Some of the data that exists today is on the indexed internet—the part of the internet that is typically found using popular search engines like Google or Bing—in the form of billions of webpages, tweets, YouTube videos, and photos posted on Instagram.[7] This does not account for the content created and hosted on the deep web (the part of the non-indexed internet) or the dark web (where access requires specialized software such as the Tor browser). Most of the indexed internet, deep web, and dark web can be accessed through publicly available means, making them PAI.

Sources of PAI are extensive. Examples include social media, commercially available mapping and imagery systems, gray literature, academic websites, public records, forums, blogs, dating sites, gaming, and traditional news media. The internet has reached 67 percent of the planet's 7.6 billion people with more than 5 billion unique mobile subscribers as of 2017.[8] This constitutes a sensor network with

near-global coverage. The distributed nature of internet data is based on cloud computing; it provides a platform that is persistent and can deliver near-real-time answers often faster than our classified systems. OSINT can augment our traditional intelligence collection and enhance it through collaboration, tipping, and queuing.

An Adaptable Single-Source Discipline

Intelligence, surveillance, and reconnaissance (ISR) assets function off the tasking, collection, processing, exploitation, and dissemination process, and OSINT is no different. OSINT can be tasked as a single-source discipline, in support of other intelligence or operational planning, or as an intelligence requirement. Consider a missile launch: there would be some reflection associated to that launch represented in the electromagnetic spectrum either before, during, or after the event. Traditional sensors are tuned to be able to detect this event in visible, infrared, or radio portions of the spectrum, which are then collected by some platform outfitted with those sensors. Although OSINT still depends on newspapers, magazines, television, etc., it is relying more and more on the internet, i.e., the sensed environment (or platform). The sensors—the OSINT-enabled collector/analyst outfitted with tradecraft and OSINT tools or technology—are tuned to detected events, like a missile launch, from the internet. This means everything that is posted, commented, shared, liked, tweeted, blogged, or documented is placed in a publicly assessable way on the internet and becomes the sensed environment. OSINT analysts using tradecraft and specialized tools become the sensors to detect, search, extract, and organize data from the internet. Unique to OSINT is the fact that the sensed environment (the internet) is also the collection platform on which the sensors are collecting.

In terms of conducting military operations, OSINT enables commanders and staffs to initiate planning where collection of other forms of intelligence are not available because of requirements prioritization issues or because existing reporting is stale. Alternately, when collection assets are available, commanders will most likely have to compete for coverage. A scarcity of assets means that collection managers must prioritize requests. If a commander does not have a priority mission, he or she will most likely not receive the requested coverage. The pervasive nature of the internet can help mitigate intelligence gaps in the face of the lack of current reporting or the denied use of other assets.

In 2011, the U.S. military used OSINT in support of lethal operations during Operation Odyssey Dawn, which conducted air and missile strikes. The operation began on 19 March 2011 as the U.S. responded to United Nations Security Council Resolution 1973, which called for the establishment of a no-fly zone over Libya and the protection of Libyan civilians from Muammar Gaddafi's forces. U.S. and partner nation ground forces were prohibited from entering Libya, which meant the operation was predominantly conducted by air and naval forces from long range. With this lack of intelligence coming from first-hand collection by friendly ground forces, OSINT was used to create accurate and timely pictures of the fluid situation in Libya. The operation's joint task force (JTF) and North Atlantic Treaty Organization (NATO) partners monitored social media to augment or fuse the data with classified reporting when selecting targets. Because the United States and partner countries were prohibited from establishing a footprint within Libya, the civilian population on the ground within Libya became a sensor for the JTF and participating NATO countries.

The ever-expanding amount of PAI, global presence of the internet, and increasing sophistication of tools available to OSINT collector/analysts allow planners to address intelligence gaps identified during intelligence preparation of the battlefield, especially in the case of previously nonpermissive environments that lack current reporting. OSINT can draw real-time information such as pictures, descriptions, geolocations, and eyewitness accounts to form a current situational understanding or pattern of life analysis, often directly from the ground. Analysis of PAI can lead to the identification of targets previously undetected by traditional information collection methods, such as a mention on social media about sightings of threat personnel at specific locations or posts about enemy troop movements. Because of competing requirements or other constraints, there is no guarantee that requested ISR or other forms of collection will be available and timely.

The requirement for fires to reach operational or strategic deep fires areas places more demand on sensors to "see deep." Even with collection assets available, as seen during Operation Odyssey Dawn, OSINT can assist with long-range targeting efforts. ISR is only as effective as what it can "see" or "hear" at that time, but OSINT draws from the internet, which enables persistent monitoring and does not rely on a sensor's geographic location to collect. Virtually every person who chooses to connect or every object that automatically connects to the internet becomes a potential source, producing PAI for collection and analysis throughout the battlespace. Collecting and analyzing PAI not only assists with establishing target locations through geolocation, selection, and deconfliction, but also it is able to offer insight in determining battle damage assessment or collateral damage estimation. Social media and traditional media

are quicker to capture this sort of information as they compete to publish a story first.

Open source information is collected on an unclassified network, and thereby can facilitate information sharing in a combined and joint environment, but there are some limitations. Analysis of PAI usually consists of collecting large amounts of data, which requires significant amounts of bandwidth and access to the internet. Creation of more robust networks may mitigate bandwidth issues, but a network is still susceptible to degradation from the enemy. The future fight in large-scale combat operations calls for us to consider fighting in a degraded, intermittent, and latent environment, but that should not keep us from pursuing and growing OSINT capabilities, as every intelligence discipline comes with its own unique challenges. Additionally, every intelligence discipline is susceptible to having to operate in a disrupted, intermittent, limited environment. Today, units have no organic force structure identified to receive OSINT training on a recurring basis. Therefore, commanders, realizing the importance of OSINT, have created OSINT cells out-of-hide, taking away from their internal resources working other mission sets.

U.S. Army graphic by Peggy Frierson, Defense Media Activity

With the U.S. Army's effort to evolve the multi-domain battle concept, OSINT serves as an enabler for fires to draw on previously untapped information. Collecting and analyzing PAI from current or future battlespaces will allow targeting operations at any range in the absence of collection coverage, or layer and cue with existing ISR. There is much more to be gained from OSINT than we realize and much more still to accomplish. It is important for intelligence leaders to become familiar with the capabilities of this intelligence discipline and with the cyberspace domain where we derive much of OSINT. We must continue to train the force on the OSINT tradecraft and provision the best-of-breed technology and tools available. To do this well, collaborating with private industry and keeping pace with technology development will be paramount to success. There is a compelling need for an OSINT force structure in order to conduct persistent collection and analysis at all echelons. We need a robust and secure training environment to practice the tradecraft and employment of tools. Finally, we share many common interests with the cyberspace operations community, but for different purposes.

The Army OSINT Office

In 2016, the Department of the Army G-3/5/7 issued a memorandum titled "Requirement for U.S. Army Open Source Intelligence (OSINT) Program" to validate the enduring requirement for Army global OSINT capabilities. It established the Army OSINT Office (AOO) at the U.S. Army Intelligence and Security Command (INSCOM), and charged the AOO to manage training of and access to capabilities provisioned by the defense and national OSINT enterprise. Army Directive 2016-37 identifies INSCOM as the Army operational proponent for OSINT and the capabilities requirements manager for the Army OSINT program, which it manages through the AOO.

Although there is no force structure for OSINT, nor is there a military occupational specialty/additional skill identifier, the AOO enables commanders across the Army to operationalize OSINT capabilities as follows:

- Serves as a starting point for units interested in OSINT capabilities.
- Provides advice/assistance on standing up OSINT activities.
- Manages requirements for data and data sources.
- Trains, certifies, and provisions capabilities to Army intelligence professionals (military, civilian, and contractor) based on the Army's operational priorities.
- Validates appropriate technologies, and manages licenses and access to the DoD enterprise suite of OSINT tools and technology.
- Plans for and validates Army intelligence funding for technologies and contractor subject matter experts for OSINT.

- Audits the use of technologies to ensure authorized OSINT activities are taking place in accordance with applicable law and policy.

Since 2015, the AOO has trained more than 2,800 personnel on OSINT tradecraft, with over 980 active trained "OSINTers" as of February 2018, and has set the standard in DoD for a coherent training program. The AOO works with the Military Intelligence Readiness Command's SE-ARISC in a successful partnership to conduct foundational OSINT training (OS301/Basic Open Source Intelligence Course)—a recent intelligence community/joint-certified program of instruction—that serves as a prerequisite for training on OSINT collection and analytic tools (OS302/Analytic Tools Training). Additionally, the AOO has recently initiated advanced skills and tradecraft training, as well as an Introduction to Advanced Data Analytics that leverages data science techniques to access and analyze data. The AOO enables commanders throughout the Army, with INSCOM brigades at the forefront of Army efforts to capitalize on OSINT. Each INSCOM theater intelligence brigade has an ad hoc OSINT cell, and each functional brigade incorporates OSINT into its primary mission.

In support of the intelligence warfighting function, OSINT makes a significant contribution to developing situational understanding for the commander—as a single-source intelligence activity and in concert with other intelligence activities. OSINT contributes to all-source analysis/fusion; tips and cues other multidiscipline activities; supports targeting activities; and contributes to situational understanding and awareness of the operational environment. And as stated earlier, there are untapped opportunities to leverage and exploit PAI especially in cyberspace.

The internet provides a vast and growing amount of PAI that exists today. Exploiting that data smartly is where the advantage lies across the Army, but especially for Army intelligence.

Endnotes

1. Department of the Army, Army Directive 2016-37, *U.S. Army Open-Source Intelligence Activities* (Washington, DC: U.S. Government Publishing Office, November 22, 2016).

2. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3683 (2004).

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

4. Bellingcat Investigation Team, "How a Werfalli Execution Site Was Geolocated," *Bellingcat*, October 3, 2017, https://www.bellingcat.com/news/mena/2017/10/03/how-an-execution-site-was-geolocated/.

5. FY17 National Defense Authorization Bill Subcommittee on Emerging Threats and Capabilities, H.R. 4909, 114th Cong. (2016), 87-88.

6. Department of Defense Manual 5240.01 *Procedures Governing the Conduct of DoD Intelligence Activities* (August 8, 2016), 53.

7. Internet Live Stats, http://www.internetlivestats.com/.

8. GMSA Intelligence, "Number of unique mobile subscribers worldwide hits five billion," 15 June 2017, http://www.gsmintelligence.com/research/2017/06/number-of-unique-mobile-subscribers-worldwide-hits-five-billion/624.

Mr. Daniel Zieminski served for 10 years in the U.S. Army, beginning as a branch detailed armor officer before transitioning to military intelligence. He deployed twice to Iraq in support of Operation Iraqi Freedom—as a tank platoon leader and then while working in the 1st Armored Division G-2. Mr. Zieminski also served as a battalion S-2, deputy G-2, and in various other intelligence positions during his time in the Army. After leaving the Army, he worked as an all-source intelligence analyst at the Army Threat Integration Center. Mr. Zieminski is currently an open-source intelligence (OSINT) trainer at the Army OSINT Office. His primary duties as an OSINT trainer are to provide subject matter expertise in support of OSINT efforts and utilization of the intelligence discipline across the U.S. Army, and conduct the Foundry OS 302 course.

The U.S. Army Intelligence and Security Command at Four Decades

1977 – 2018

Part IV: Global War on Terrorism

by Mr. Michael E. Bigelow, INSCOM Command Historian

The attacks of 11 September 2001 presented the United States with a new kind of threat: a complex network of international terrorists who transcended national borders and military areas of responsibility. This new Global War on Terrorism demanded a global intelligence effort. Consequently, the U.S. Army Intelligence and Security Command (INSCOM), with its ability to draw on Soldiers and information around the world, played a major role in this conflict. In response to the attacks, the United States and its allies launched Operation Enduring Freedom (OEF) in Afghanistan. To support the deployments, INSCOM units sent counterintelligence (CI) and force protection teams to the Philippines, Uzbekistan, and Afghanistan.

The scope of combat expanded in March 2003 when U.S.-led forces began Operation Iraqi Freedom (OIF). The 513th Military Intelligence (MI) Brigade once again found itself at the center of INSCOM's support to combat operations in Iraq. The brigade successfully executed split-based operations when its main body deployed in Camp Doha, Kuwait, while elements of its headquarters and subordinate battalions remained at Fort Gordon. In Kuwait, the brigade manned joint intelligence centers to produce fused intelligence for ground-force commanders and provided force protection support.

To support the campaigns from the United States, INSCOM's National Ground Intelligence Center sent customized intelligence products and services to the theaters of operations. INSCOM provided interpreters and translators proficient in 30 languages. The National Ground Intelligence Center's 203rd MI Battalion trained and equipped weapons intelligence teams to gather intelligence on improvised explosive devices and their makers. The 704th MI Brigade's Meade Operations Center trained and deployed signals intelligence (SIGINT) terminal guidance teams to support brigade combat teams with targeting information. At Fort Gordon, the 116th MI Group provided direct support to units in Southwest Asia.

INSCOM fielded the first battalions, the 201st MI and the 14th MI, specifically designed to operate within a joint interrogation and debriefing center (JIDC). In October 2005, these two battalions deployed to Iraq and Afghanistan. To ensure that the Army's interrogation battalions would be prepared to work in a JIDC, INSCOM established the INSCOM Detention Training Facility. Completed on 22 April 2008 at Camp Bullis, Texas, the facility began training battalion personnel in JIDC operations, and it continues to provide this service today.

Seeking to harness emerging technologies for intelligence synchronization, fusion, and mission command, forward-thinking leaders over the course of years incorporated unconventional capabilities and technologies into INSCOM's mission command structure. This relatively slow evolution received official recognition in 2002 when INSCOM headquarters formally established the Information Dominance Center (IDC). The IDC fused intelligence pertaining to terrorist activity and provided national, theater, and tactical reporting and actionable intelligence products to forward-deployed commanders. The technology and capabilities were field tested with the 501st MI Brigade in South Korea and eventually employed in Iraq as the Joint Intelligence Operations Capability-Iraq. Later, the capability would become part of the Distributed Common Ground System-Army program of record.

On 16 October 2002, the 1st Information Operations (1st IO) Command assumed the duties of the Land Information Warfare Activity, and it supported operations in OEF and OIF with deception planning, psychological operations, and other unconventional, technically sophisticated capabilities. U.S. Army Cyber Command (ARCYBER) assumed operational control of 1st IO Command on 2 February 2011, and 1st IO has continued to defeat adversaries in all domains of the information environment. On 1 October 2011, INSCOM established the 780th MI Brigade, which provided the Army with an organization devoted to cybernetic operations and advanced capability development to support those operations; like the 1st IO Command, ARCYBER assumed operational control of the 780th, and this arrangement has allowed ARCYBER to benefit from greater support from the U.S. intelligence community.

U.S. Army photo courtesy of INSCOM Public Affairs Office

U.S. Army Cyber Command Information Center

Besides providing individual soldiers and teams to reinforce Afghanistan and Iraq, the other INSCOM theater brigades and groups tracked terrorist activities and supported worldwide operations. In 2010, the 470th MI and 500th MI Groups were reorganized into theater brigades for U.S. Army South and U.S. Army Pacific, respectively. In 2016, the 207th MI Brigade joined INSCOM as the theater brigade for U.S. Army Africa.

To these theater MI brigades, INSCOM added an array of single-discipline or functional units. General CI support for the Army remained with the 902nd MI Group. To provide similar support for human intelligence (HUMINT), INSCOM established the Army Operations Group for collection operations and the G-2X staff element for HUMINT policy. INSCOM reactivated the 116th MI Brigade as the Army's consolidated MI aviation organization, allowing for more efficient use of the low-density, high-demand aerial assets.

INSCOM is both a microcosm of the entire U.S. intelligence community adapted to the specific needs of the Army and a liaison to the intelligence community, which allows the Army to synchronize national-level capabilities against operational and tactical requirements. INSCOM emerged from the Army Security Agency, an organization devoted to technical intelligence disciplines, and subsequently incorporated and expanded other disciplines under its global purview. While originally emphasizing SIGINT and electronic intelligence, the necessity to exercise mission command globally and over essentially disparate organizations led to INSCOM's unique technical and bureaucratic capabilities and structures. Similarly, INSCOM's organizational culture has prized innovation, sophistication, and nontraditional thought while never forgetting the primacy of the human element across all the intelligence disciplines. Thus, the same essential organization that broke East German and Soviet radio encryption in an old schoolhouse under strict secrecy, now leads HUMINT operations, CI activities, manned and unmanned reconnaissance flights, and cybernetic operations around the world. Because of its proximity to the intelligence community's leading innovators, INSCOM has been and will remain a modernization laboratory for the Army, where nonstandard, low-density, and arcane capabilities become battle-tested and shape the Army's future technologies.

Mr. Michael E. Bigelow has served as the Command Historian for the U.S. Army Intelligence and Security Command (INSCOM) since 2006. He received a bachelor of arts in history from Colorado State University and a master of arts in military history from Temple University. He has written numerous articles for military publications such as Military Review *and* Military Intelligence Professional Bulletin*. Before becoming INSCOM's Command Historian, he served as an active duty military intelligence officer for 22 years.*

INSCOM

The Road to the Data Strategy for Army Intelligence

by Mr. Kirk G. Brustman, Mr. Erik K. Christensen, Dr. Holly A. Russo, Lieutenant Colonel Russell J. Edmiston, and Mr. Richard H. Saddler

It's my belief that we are on the cusp of a fundamental change in the character of warfare, and specifically ground warfare. . .the failure to connect those dots pre-World War I, the failure to see and the failure to connect those dots in the 1920s and '30s, cost 100 million lives, a huge amount of blood, and years and years of human suffering. It is our task, the task of you and I, the task of us, both civilian and military, to do better, to see the trends, and to get the future less wrong than our enemies.

—GEN Mark Milley, Chief of Staff of the U.S. Army

The Environment

Disruptive, transformative technologies may be creating an operational environment where many current warfighting paradigms are irrelevant. Artificial intelligence-powered decision making, human-machine interfaces, robotics, biological and genetic engineering, quantum computing, global social media, and increased access to space are just a few of the challenges that require land forces to evolve and adapt. The transformation of human-machine interfaces will change the role of humans in operational decisions.

> ***"No matter where you go in the world today, it's observable from some device. The ability to surveil, to see and communicate, is at levels never before seen in human history. Almost everyone and everything is a potential ISR platform capable of transmitting real-time information, that if properly analyzed can be useful intelligence which can significantly help or seriously hinder military decision-making and operations"[1]***

The U.S. Army intelligence enterprise must adopt transformative technologies and develop dramatically different approaches to data, information, and intelligence to remain relevant. Such an approach requires a data strategy to modernize the people, capabilities, network architecture, and the data itself to enable effective operations within a fluid data environment. Currently, Army intelligence analysts dedicate the majority of their time and resources to manual data discovery and data management rather than analyzing and transforming data into actionable intelligence. The volume and velocity of available data now outpaces the manpower available to extract, correlate, or condition data.

The scope of the data problem is striking: the Army intelligence enterprise needs to collect and exploit classified military intelligence; acquire and exploit publicly available information; exploit data collected by an increasingly large and varied array of sensors; and exploit data provided by allied, coalition, and international partners. As the quantity of data increases, so does the complexity in delivering a common intelligence picture to support collection, targeting, and decision making. Finally, the Army intelligence enterprise's transformation must comply with U.S. law and the various U.S. intelligence community, Department of Defense (DoD), and Army policies and regulations.

Where We Are Now

Although the Army intelligence enterprise is a collector and producer of raw data, exploited data, and finished intelligence products, it is also a voracious consumer of data and products from the DoD and intelligence community. Intelligence is inherently joint, interagency, intergovernmental, and multinational, and it requires assured data in a contested environment from sensor to analyst to consumer.

The Army's intelligence process consists of four steps (plan and direct, collect and process, produce, and disseminate) and two continuous activities (analyze and assess). Within the intelligence process, the Army uses data and products to support the decision-making processes of operational and tactical commanders. The U.S. Army must execute intelligence processes in an era of "Big Data" where traditional data architectures cannot handle new datasets. Primary characteristics of Big Data are volume, variety, velocity, veracity, and variability,[2] which require a scalable architecture for efficient storage, manipulation, and analysis. The time currently required for identifying gaps in data, developing collection plans, planning for employment of sensors and assets, and collecting the data often results in a failure to provide "intelligence at the speed of mission command." We must gather relevant data more efficiently in order to empower analysts to perform their primary role of transforming data and information into actionable intelligence.

The Army intelligence enterprise data architecture is an assortment of legacy stovepiped applications, tightly coupled to database tables that exist on multiple security fabrics and domains. The architecture and supporting infrastructure are outdated: they lack advanced data analytics; they cannot ingest, compute, store, and transport exponentially growing data; and they cannot effectively employ publicly available information. However, existing commercial technologies present an opportunity for the Army to transform

Graphic design courtesy of INSCOM's Public Affairs Office

collection, storage, processing, and data exploitation, which returns time to the analysts to perform their core missions. Building a data architecture requires a holistic understanding of how the U.S. Army designs, acquires, integrates, and employs its data capabilities.

While adopting the U.S. intelligence community services of common concern[3] (a Director of National Intelligence-designated service, developed and maintained for the intelligence community) represents a path to future capabilities, there is room for interim improvement. The Army intelligence enterprise should implement recommendations from the Distributed Common Ground System-Army (DCGS–A) independent study:[4] namely, development of data science capabilities,[5] and adoption of commercial-off-the-shelf and free/open source analytic tools to increase data exploitation capabilities.

DCGS–A (the program of record for analysis) tasks, processes, exploits, and disseminates intelligence, surveillance, and reconnaissance information from battalion to echelons above corps by combining 16 independent legacy systems of record into one comprehensive network. It includes the capability to process top secret/sensitive compartmented information. The Office of the Secretary of Defense, Director, Operational Test & Evaluation, evaluated the current configuration (Increment 1, Release 2) to be operationally effective and suitable but not survivable against cyberspace threats due to Army network vulnerabilities. DCGS–A allows Soldiers and units to receive and organize intelligence from more than 700 sources, search relevant information, perform analysis, and share results with the Army command and control network and the intelligence community through the DCGS Integration Backbone. DCGS–A Increment 1 requires intensive training for users and continuous refresher training to units in garrison:

> ***"DCGS–A is a complex system, and the skills required to use it are perishable. The operational availability of DCGS–A satisfied the requirements at all echelons, and reliability improved from the IOT&E [Initial Operational Test and Evaluation] in 2012. There were no hardware failures during the FOT&E [Follow-on Operational Test and Evaluation]. Software failures were still a challenge for users; the system required reboots about every 20 hours for users who had heavy workloads such as the fire support analysts and data managers in Brigade Combat Team Tactical Operations Centers."[6]***

The hardware and software designs, development, and deployment are costly, with upgrades often taking more than 10 years. The Army intelligence enterprise's acquisition strategies must be informed by an understanding of intelligence data analysis, sources, and formats. They must also be informed by cyberspace threats to reduce vulnerability, other technologies used daily by analysts to provide an intuitive interface, and the rapidly changing data environment. All of these factors will enable analysts to answer today's intelligence requirements—not the last decade's.

The Technology. The current revolution in technologies, referred to as Big Data, arose because the previous relational data model could no longer handle the current needs for analysis of large and unstructured datasets. It is not just that data is bigger than before; it is now more complex due to its unstructured nature. The Big Data revolution will be a fundamental shift in architecture as stark as the shift from filing cabinets to the first computers.

Recent technology pilots at the U.S. Army Intelligence and Security Command (INSCOM) have demonstrated that

in-memory analytics—an approach to normalizing, correlating, and geo-referencing data when it resides in a computer's random access memory—provides unprecedented capabilities to hasten data conditioning and support data-driven decisions. Analysts would retain the capability to conduct deep, exhaustive searches against the entire data corpus from disks while simultaneously enjoying rapid access to more recent operational data.

All-source analysts rely on a plethora of data, represented in a variety of ways. Generally, data falls into three categories:

- Structured (think of a properly written significant activities report).
- Semi-structured (like a web page with pictures and text).
- Unstructured (like raw full motion video footage from a payload).

Structured data has historically been the focus of most enterprise analytics, including DCGS–A, and has been handled using relational data models. However, intelligence reports written in Microsoft Office and Adobe formats lack structure, metadata, or even accurate document properties. Most of these are manually transformed and structured to enable analysis. Recently, the quantity of new types of semi-structured and unstructured data, such as microtexts, web pages, relationship data, images, and videos, have proliferated, and intelligence analysts increasingly rely on the incorporation of semi-structured and unstructured data in the intelligence process.

The Fabric. While the U.S. intelligence community primarily operates on the top-secret fabric, the U.S. Army operational force primarily operates on collateral networks. The SECRET Internet Protocol Router Network (SIPRNet) is the principal command and control network for DoD, including the U.S. Army. Several elements within the Army intelligence enterprise are providing varying degrees of data access and data management. Various programs, systems, and applications ingest this data, including the DCGS–A fixed-site brains. Though manual processes have resulted in success in the past, their limitations are exposed by the exponential growth and variety of data; technology solutions currently exist and present an excellent opportunity for change.

The Army intelligence enterprise requires a multilevel secure data environment that allows for authentication and access controls against validated mission needs, and it must support joint, interagency, intergovernmental, and multinational interoperability. The data environment must include a master data warehouse and a series of operational data stores, including tactical sensor ground stations. To support the Army intelligence enterprise, the data environment must be accessible from U.S. networks, including the Joint Worldwide Intelligence Communications System, SIPRNet, and international and coalition networks. The data environment must take advantage of capabilities that include in-memory processing, machine learning, natural language processing, and foreign language machine translation. Finally, the data environment must be able to store, transport, and process the data volume, variety, and velocity representative of Big Data.

The Factors. Intelligence data is often collected from international sources in non-English languages. Automated language detection capabilities are necessary to add metadata identifying the underlying language that the data represents. This metadata will support the effective use of automated foreign language translation tools. Data in foreign languages should be translated during ingestion, and the translated data should be tied to the source data, so that an analyst has both at hand.

Intelligence systems naturally focus on threat data, but data from neutral or unknown actors and friendly force data must be merged with intelligence databases in order to achieve an accurate common operating picture.

Data is ingested from numerous sources on multiple security domains, networks, and fabrics. Converging the data across domains is necessary to provide a common/consolidated view of data to the analyst, so that complete analysis occurs. Swivel-seat environments limit analyst effectiveness and place undue burdens on their time. Ingestion of data from low to high security domains is a suboptimal approach. Data should exist on the domain in which it originated, but the data must be accessible across domains to provide a complete picture to the analyst on a single environment. One of the lessons learned from establishing cross-domain and multilevel secure databases is that the Director of National Intelligence's security markings program data classification levels are inconsistent and often incomplete. Effective cross-domain solutions require data to be marked according to standards, at the field level, with tear-line and paragraph markings to enable the effective movement of data through and across domains. Testing of current systems must include compliance testing of security markings programs to ensure cross-domain interoperability.

Data solutions must satisfy intelligence oversight requirements, particularly in the conduct of open-source intelligence from publicly available information. Limitations on the collection and storage of U.S. person data, questionable intelligence activities, insider threat activity, and other

constraints require us to embed auditing capabilities within our analytical tools to enable identification and forensic analysis.

The Paradigm. The Big Data paradigm has caused such a shift in processing that traditional data processes are no longer valid. In a traditional relational data model, data is stored after its preparation. This is typical for cases in which data is produced by trusted sources; as the data is ingested, it is enriched with metadata and committed to a database (or "data lake"). All the data must pass through this refining process before it becomes useable for intelligence. Only after that refining is complete does the metadata become available to the analyst. This means a lot of computational resources are potentially consumed by processing useless data into useless information.

In a high-volume, low-confidence use case such as social media exploitation, the data often persists in the raw state in which it was produced before being cleansed and organized (or "data swamp"). Given the high volume, enriching all data would overwhelm even the most robust processing capabilities. The data is only enriched and promoted to the data lake after an analyst assigns it some value. Data in the data swamp is aged out if not referenced. The consequence of data in its raw state is that a schema or model for the data is only applied when the data is retrieved for preparation and analysis. This concept is described as schema-on-read. In a high-velocity application, the data is prepared and analyzed for alerting, and only then is the data put into persistent storage, thus speeding the ingest process and making data available faster by limiting the wasteful activity of enriching irrelevant data. Future analytic capabilities must have the ability to allow the promotion of data between raw storage (data swamps) and databases (data lakes).

Another concept of Big Data, called distributed data processing (system scaling), is often referred to as moving the processing to the data, instead of moving data to the processing. It implies that data is too extensive to query and move into another resource for analysis, so the analysis program is instead sent to the data-holding resources while the results are moved to another resource. Therefore, the Army intelligence enterprise must leverage technology that allows for the processing of data as close to the collection point as possible, or "intelligence at the edge." "Intelligence at the edge" is a concept used to describe a process whereby data is analyzed and aggregated in a location close to its capture in a network. This presents volume and velocity challenges for distributed networks that are uncommon to industry and the intelligence community's national organizations.

Scaling computing resources is critical to distributed data processing. There are two methods for system scaling, often described metaphorically as "vertical" or "horizontal" scaling. Vertical scaling increases processing speed, storage, and memory for greater performance: it means building a bigger and better set of computer systems devoted to a service or task. This approach is limited by physical capabilities requiring ever more sophisticated elements that are more costly and time-consuming to procure, and it often implies that a single organization owns and pays for all the resources. In contrast, horizontal scaling integrates distributed individual resources to act as a single system; it is a sort of crowd-sourcing of machines, possibly owned by many parties to a common effort. The Army intelligence enterprise's evolution will transform its architecture from vertically scaled systems such as DCGS–A to horizontally scaled systems such as the intelligence community information technology enterprise (IC ITE) (pronounced "eye sight").

IC ITE

What is IC ITE?

IC ITE is a sensitive compartmented information-based suite of enterprise-level information technology components and infrastructure, operated by a consortium of service providers adhering to intelligence community enterprise principles, governance, and technology standards.

Why IC ITE?

IC ITE creates a powerful platform for innovation. With the latest cloud technologies, powerful computing capabilities create opportunities from the challenge of Big Data and enhance safeguards to protect the intelligence community's most sensitive data.

Additionally, budget constraints in an increasingly dangerous world necessitate responsible reductions. The intelligence community can achieve efficiencies through consolidation and sharing of information technology as a service and realign the savings to mission priorities.

How will it Function?

IC ITE's sharing capability will be realized through the use of a cloud-based architecture known as the IC-Cloud—a secure resource delivering information technology and information services and capabilities to the entire community. The IC-Cloud will allow personnel to log on to their desktop from any intelligence community location and access mission-related information.

Each agency has a unique role within the intelligence community. The individual agencies will internally determine necessary changes in preparation for the transformation to IC ITE. The details of these changes will continue to develop as the services are enabled, decision points are reached, and implementation is started. Throughout the process, each intelligence community element will prepare its workforce through training and education to adapt to the new IC ITE operating model.

The Transition

> ***"Most conflicts will quickly become transregional—expanding beyond one or two countries—and become multi-domain, to include land, sea, air, space, and cyberspace. . . We need to make sure in the context of transregional, multi-domain, multifunctional conflicts that we have the right command-and-control construct in place to integrate joint capabilities and support rapid decision-making by national command authorities."***[7]

Modernization efforts to 2030 and beyond must transition and posture the Army intelligence enterprise to adapt and evolve quickly to future threats in a multi-domain environment. Recognizing the power and potential of commercial technologies, the intelligence community has developed a strategy that changes its information technology's operating model. This new model, IC ITE, moves the intelligence community from an agency-centric information technology architecture to a common platform where the community easily and securely shares technology, information, and resources. By managing and providing the information technology infrastructure and services as a single enterprise, the intelligence community will not only become more efficient, but it will also establish a powerful cloud-based platform to deliver more innovative and secure technology to desktops at all levels across the intelligence enterprise. These new capabilities, with seamless and secure access to community-wide information, will positively change how users communicate, collaborate, and perform their mission.

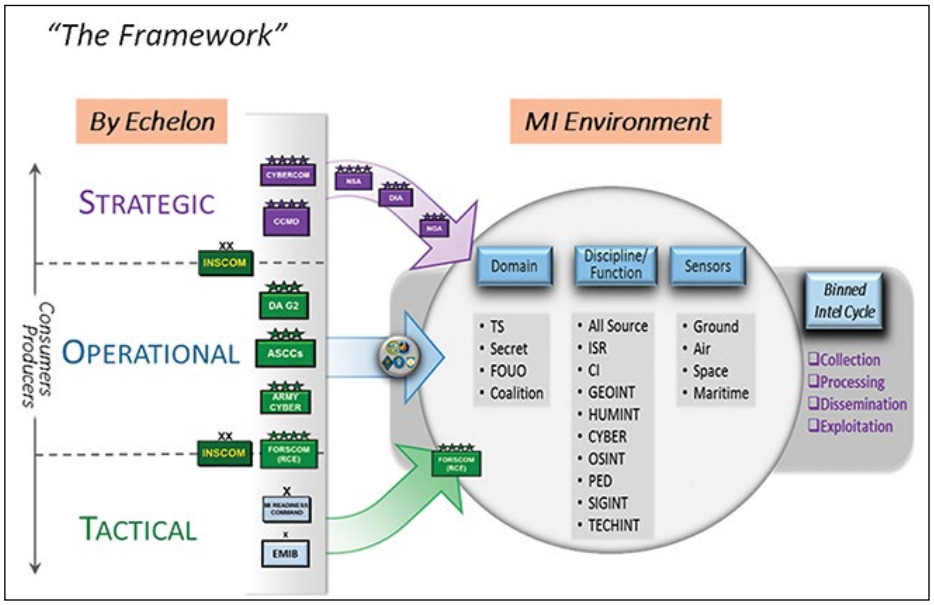
Horizontally scaled IC ITE services use a loosely coupled set of resources in parallel that provide on-demand delivery of computing power, storage resources, and applications that will allow the Army intelligence enterprise to keep pace with data proliferation. Commercial cloud computing has reduced the barriers to entry for building and maintaining systems; that in turn has fostered innovations to quickly build reliable, high-performance systems. The Army intelligence enterprise needs to migrate to the cloud, leveraging the flexibility, scalability, efficiency, and redundancy that this computing model offers.

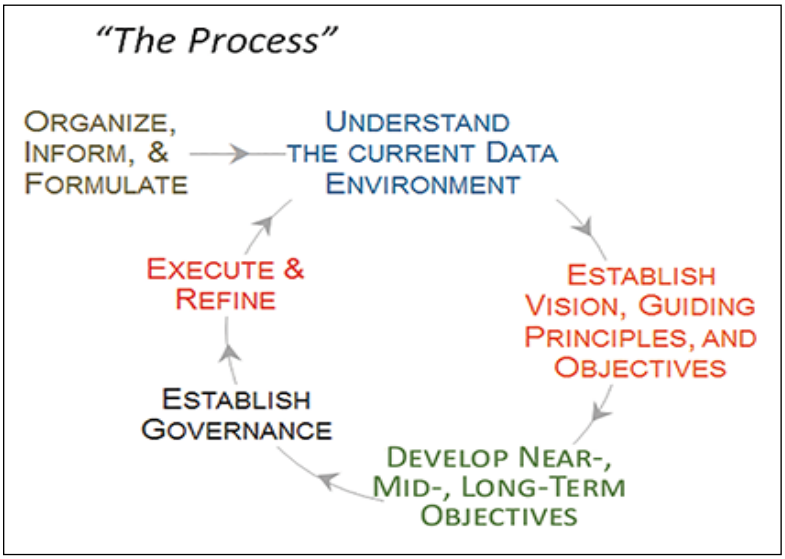
Data correlation analysis is arguably the single most important thing that an analyst does with a data set. Correlation analysis can help define trends, make predictions, and uncover patterns and relationships. Currently, correlation analysis is primarily a manual process. Automated tools that leverage supervised machine learning are necessary to perform data correlation initially upon ingestion but ideally continuously as the data is being mined. In addition, intelligence analysts should receive training on data science methods to perform advanced analysis, which can provide a basis for machine learning to improve automated analysis algorithms. Machine learning gives computers the ability to learn without explicit programming. Although analysts can effectively enrich data with metadata, this manual process is labor-intensive, taking time away from their primary function of producing actionable intelligence. Data enrichment should instead be a natural side effect of the analysis process, and analysts should have access to data science tools and functions embedded within applications. As the analyst discovers relationships within data sets that are consistent and repeatable, rules can be created to teach machine-learning algorithms to mine the data for these relationships and relate them to the metadata.

Strategy and Implementation Plan

Beginning in 2017, the U.S. Army Office of the Deputy Chief of Staff, Intelligence (ODCS, G-2), and INSCOM initiated the development of a framework for a comprehensive data strategy and implementation plan. The intent is to align the Army intelligence enterprise's vision, guiding principles, and objectives with the data policies and strategies of the DoD, intelligence community, and Army. The desired end state is the Army intelligence enterprise integrated into a "cloud-first" environment, able to extend from strategic to tactical, across all echelons, domains, intelligence disciplines, functions, and sensors.

This effort does not prescribe or direct the acquisition of material solutions to solve the Army intelligence enterprise's data problems. The data strategy establishes the





initial near-, mid-, and long-term goals for the Army intelligence enterprise. It establishes principles to guide and serve as the left and right limits on the movement toward those goals. Finally, it identifies mechanisms and governing bodies that will enable and lead the modernization effort. The data strategy is a continuous process: as the operating and data environments, technologies, and national strategies continue to evolve, so too must the Army intelligence enterprise's strategy.

To achieve the desired end state, we must modernize along four lines of effort—people, capabilities (including tools and technology), network architecture, and data. We must—

- Develop agile leadership and workforces with the diversity of expertise necessary to analyze, understand, and operate in a dynamic environment.
- Enable the rapid provision of relevant, intuitive, and accessible tools and analytics to answer today's intelligence requirements in part by leveraging open sources.
- Transform to a collaborative, agile, secure, cloud-first environment with networks that leverage open architecture and intelligence community/DoD investments.
- Adopt and enforce intelligence community/DoD standards for data tagging, data ingestion, and data management.

We use the term "cloud-first" purposefully. First, cloud operations mandate data standards, improved management and access, and common tools. Second, while we fully recognize the tremendous benefit from cloud technologies and the fact that our defense and intelligence communities are moving toward operating in cloud environments, "cloud-only" solutions are insufficient for the needs of the Army intelligence enterprise; it must be able to operate in dark and disconnected environments that would cripple formations dependent on cloud technologies.

The Army intelligence enterprise data strategy will provide multiple benefits for analysts, warfighters, the DoD, and the intelligence community. The paradigm of time spent in search and conditioning rather than analysis will shift from 80/20 percent to 20/80 percent. The speed and effectiveness of decision making will dramatically increase through improved visibility of trusted and comprehensive information. We will see an increase in interoperability and shared understanding with mission partners, while protecting and responsibly sharing information.

To date, INSCOM completed an abbreviated mission analysis to inform and set the conditions for transition to the ODCS, G-2. The mission analysis included a problem statement, vision, end state, and methodology. Now, under the leadership of the ODCS, G-2, the effort is working to ensure transparency and full participation across the Army intelligence enterprise. Stakeholder organizations are being identified, with key participants incorporated into working groups aligned with their expertise. Both ODCS, G-2 and INSCOM are exploring consultation options to ensure that the necessary expertise, experience, timeliness, and relevance are on hand.

The 2018 Intelligence Senior Integration Group forum addressed INSCOM's data strategy. The forum convened key intelligence leaders from across the Army intelligence enterprise to share their understanding of Army and intelligence community data strategies and existing efforts within the Army intelligence enterprise; it validated the strategy's methodology; and it formalized working groups along lines of effort. Some of the participating organizations included U.S. Army Forces Command; U.S. Army Materiel Command; U.S. Army Special Operations Command; U.S. Army Reserve; U.S. Army Intelligence Center of Excellence (USAICoE); INSCOM; ODCS, G-2; and interagency partners. The tentative publication date for the initial Army Data Strategy Intelligence Implementation Plan is fall 2018.

The Future

INSCOM is integrating national-to-tactical intelligence with multi-domain operations to provide a high degree of situational understanding across the range of military operations, while operating in complex environments against determined and adaptive enemy organizations. Current INSCOM initiatives, established in coordination with ODCS, G-2; USAICoE; and Project Manager, DCGS–A, represent a solid foundation for the Army intelligence enterprise's movement toward IC ITE implementation.

A data revolution within the Army intelligence enterprise is not a luxury. "Future conflict will be decided based on who is fastest at collecting, correlating, fusing, analyzing and securely transporting the right decision-quality data across multiple domains to the right decision maker."[8]

Epigraph

GEN Mark A. Milley, "Keynote Address" (2016 Dwight David Eisenhower Luncheon, Association of the U.S. Army, Washington, DC, October 4, 2016), https://www.ausa.org/events/ausa-annual-meeting-exposition/sessions/eisenhower-luncheon.

Endnotes

1. GEN Mark A. Milley, "Keynote Address" (2016 Dwight David Eisenhower Luncheon Association of the U.S. Army, Washington, DC, October 4, 2016), https://www.ausa.org/events/ausa-annual-meeting-exposition/sessions/eisenhower-luncheon.

2. National Institute of Standards and Technology (NIST), NIST Special Publication 1500-1, *NIST Big Data Interoperability Framework: Volume 1, Definitions, Final Version 1* (Gaithersburg, MD: National Institute of Standards and Technology, September 2015), 4.

3. Intelligence Community Directive 122, *Services of Common Concern*, 2018.

4. DCGS–A Independent Study Final Briefing ("Review 2"), Independent Company chartered by PM DCGS–A, 27 January 2017.

5. Consolidated Intelligence Guidance Fiscal Years 2018-2022, Planning and Programming Guidance for the National Intelligence.

6. Director, Operational Test and Evaluation, "Army Programs, Distributed Common Ground System – Army (DCGS–A)," *FY 2016 Annual Report,* December 2016, 152, http://www.dote.osd.mil/pub/reports/FY2016/.

7. GEN Joseph Dunford, "Dunford: Command, Control Must 'Keep Pace' in 21 Century," interview by Jim Garamone, *DoD News Defense Media Activity*, January 4, 2018, https://www.defense.gov/News/Article/Article/639844/dunford-command-control-must-keep-pace-in-21-century/.

8. Robert K. Ackerman, "Air Force Banks on New ISR Strategy," *Signal Magazine*, December 13, 2017, https://www.afcea.org/content/air-force-banks-new-isr-strategy. The comment in the article is a quote by COL Johnson Rossow, Air Force A-2 chief of capabilities-based planning under the Future Warfare Directorate.

Mr. Kirk Brustman is the U.S. Army Intelligence and Security Command (INSCOM) Director of Department of the Army Intelligence Information Services.

Mr. Erik Christensen is the INSCOM senior Intelligence Community Information Technology Enterprise project manager for INSCOM G-7.

Dr. Holly Russo is the INSCOM data scientist for INSCOM G-7.

LTC Russ Edmiston is the Chief of the Operations Analysis Division, INSCOM G-3.

Mr. Rich Saddler is the INSCOM senior operation advisor.

INSCOM

Developing a Big Data Strategy: Where We Are and Where We Need to Go

by Colonel Ingrid Parker

Editor's Note: Developing a Big Data Strategy: Where We Are and Where We Need to Go by Colonel Ingrid Parker is reprinted from Small Wars Journal per the Creative Commons license granted upon its original publication. (http://small-warsjournal.com).

The world is on the cusp of an epochal shift from an industrial- to an information-based society. History demonstrates that changes of this magnitude do not occur without being accompanied by fundamental change in the way war is conducted. This "Information Revolution" is a product of advances in computerized information and telecommunications technologies and related innovations in management and organizational theory.

—Norman Davis, "An Information-Based Revolution in Military Affairs"

Recognizing Transformation: Revolutionary Military Affairs

Throughout our military history, innovation caused adaptations on the battlefield that have been remarkable and innovative. We call this type of adaptation *revolution in military affairs*. The easiest technological adaptation (or revolution in military affairs) to recognize is the repeating rifle, patented in 1860 by Benjamin Tyler Henry.[1] The repeating rifle caused armies to consider standoff, cover and concealment, and new forms of maneuver in their tactical formations. Before the repeating rifle, armies fought mostly using Napoleonic formations, but the accuracy of the repeating rifle caused a transformation in maneuver on the battlefield. Another adaptation, which is less noticeable but just as important, is the shift from courier reporting to radio reporting that accompanied the introduction of the radio into tactical formations during World War I (WWI). The technological innovations of WWI mark it "as 'the first modern war,' since a number of technological inventions made their debut during the war."[2] Like the repeating rifle, the technological innovations of WWI changed the conduct of battle to include rigid reporting techniques like scheduled reports, standard formats, a common language, and taxonomy. While commanders and leaders still used face-to-face communications and battlefield circulation as the main method to grapple with situational awareness, reporting augmented and improved battlefield visualization.

This revolution in military affairs or technological transformation occurred in the summer of 1914, when Germany conducted a hasty military mobilization for an impending war in Europe. The chief of the general staff of the German Army, Helmuth von Moltke (the Younger), understood that as he prepared his Army to execute the Schlieffen Plan in a war which would have unpredictable outcomes due to military overmatch and plans spanning noncontiguous battlespaces. As directed by Kaiser Wilhelm II, Moltke readied the military for war, even though he believed that the Schlieffen Plan contained ill-defined political objectives, was too audacious in operational reach, and was too aggressive in tempo for the limited forces that were available. Nonetheless, the Kaiser and field commanders favored the Schlieffen Plan because it sought political objectives that were desirable to military and national leaders.

Before a hasty mobilization, Moltke wanted to change the Schlieffen Plan because he did not think his army was ready to execute a two-front war with both Russia and France. In addition, he recognized that the plan assumed (or predicted) the British would not intervene in the conflict and he doubted this was a valid assumption. Moreover, the Schlieffen Plan allowed no room for error, and it did not account for changing political conditions in the international balance of power or the impact of technological innovations.

In 1914, Moltke's subordinate Army commanders put the Schlieffen Plan into motion by going on the offensive at the Battle of the Frontiers. Likewise, Moltke's follow-on offensive actions and choices reinforced the plan, making it a maneuver decision and battlefield reality. After the Schlieffen Plan commenced, Moltke struggled to gain and maintain situational awareness throughout the depth of the battlespace because of poor battlefield visualizations and ineffective operational reach in the range and depth of the battlefield. Historians often assert that Moltke weakened the Schlieffen Plan by massing forces on the south side of the western theater and diminishing the north side; thus, he did not set the conditions for a French Army defeat.[3]

To assist with information management, which Moltke believed was the heart of the problem, he implemented rigid reporting techniques, mostly field reports, to better understand the battlefield. The German Army predominantly used couriers as the means for battlefield visualization; however, this quickly became obsolete on the noncontiguous battlefield because of the implementation of radios. Nevertheless, Moltke had neither the staff, nor the staff expertise, to conduct thorough analyses of the reports as they arrived in the headquarters. Consequently, information arrived but went unevaluated for decision making. Having only a partial view of the battlefield, Moltke often assessed the situation and made decisions based on conjecture in the theater of war. His inability to see the battlefield in depth often caused him to make poor use of military resources.[4] In retrospect, Moltke believed that the reports had the information and answers that he needed, but they were still unusable because of his inability to manage and organize the information. Moltke was not able to visualize the battlefield in depth, causing campaigns to become disjointed.

During the interwar period, the German Army's leadership conducted a rigorous after action review. To address some of the challenges they faced in WWI, the new chief of staff, Hans von Seeckt, transformed the Army's staff, doctrine, training, and tactics.[5] He implemented new organizational hierarchies for modern warfighting and for adaptation to air-land battle. More importantly, he recognized that telecommunications made the courier obsolete and continued to refine reporting structures and mechanisms that began under Moltke's tenure. The revolution in military affairs from courier to radio occurred between 1914 and 1926 because of the German Army's inability to manage the volume of information and ineffective staff processes for the emergent technologies during WWI. The reporting techniques formalized at the conclusion of WWI were appropriate for new military technologies, information needs, and new modes of warfighting, and later they proved their viability in World War II (WWII).

Although Germany lost WWII, the German Army mastered information management with the new reporting techniques and methodologies. The U.S. Army and the Department of Defense (DoD) ultimately adopted the German Army's business practices and incorporated similar principles into their doctrine, training, organizational force structure, and reporting schemas. Over the subsequent decades, reporting permeated all facets of U.S. Government operations and remains the primary deliverable for intellectual exchange and knowledge production. Like the German Army, the U.S. Army, DoD, and U.S. intelligence community continue these reporting techniques today, even as technologies, information, and warfighting change again.

U.S. Army and the DoD Adaptation

While it is true that the U.S. Army, DoD, and intelligence community have changed force structures and information systems over the last few decades, it was not caused by the exigency of information or due to unlimited data. The nature of war was the driver, causing data management to be an afterthought, and ad hoc in its implementation. As in 1914, we are now at the crossroads of technology and data, pushing analysts and organizational leadership into the middle of another technological revolution in military affairs; the U.S. Army must evolve its intelligence apparatus to meet the demands of information, intelligence, and speed. As an organization, it must implement Big Data management processes to augment and improve battlefield visualization and organizational decision making and to economize analysts' time.

The Fundamentals of Data Management

Housekeeping. Housekeeping is the process of record keeping, maintenance, and other routine tasks that must be completed in order for a computing environment to function efficiently and succinctly. Housekeeping occurs in tools and services such as databases, system processes, core services, and interfaces. Although mundane, often overlooked, and under executed, housekeeping is as necessary for Big Data implementation as processing, exploitation, and dissemination (PED) is for the intelligence cycle. In addition, core services must be implemented with embedded mechanisms that ensure intelligence oversight compliance. These services should include—

- Purge and recall capability for data provenance.
- Foreignness determination for compliance with Executive Order 12333, *United States Intelligence Activities*.
- Serialization of bulk data for auto-dissemination.
- Entity disambiguation and entity resolution for enrichment.
- Correlation, merge, and canalization for data curation.

Understanding Emergent Intelligence Tasks. Data has evolved exponentially and staff hierarchies are no longer a viable solution or adaptation to the current information environment. Corporate America already implements Big Data methodologies in micro- and macromarketing strategies, enabling decision making in motion; greater agility and increased stakeholder participation; micro- and macroconsumerism; and targeted information campaigns. In order to keep pace, adaptation in the intelligence community is necessary and it will come; however, adaptation will require new tasks that may involve—

- **Back-End Work**, or the hidden side of a technology or tool. This activity is often done on databases and servers or functions such as cataloging or indexing. This type of work creates a technological foundation, a security apparatus, and the necessary content to be leveraged on the front end.[6]
- **Front-End Work** is the user interface and user experience.[7] Brilliant technologists create a graphical user interface (GUI) that mimics human learning models, as it requires less training. The best example of a GUI that requires little training with high payoff is Google Maps. Google Maps is a multi-data analytic tool that offers decision making to customers while on the move. It now uses customers to catalog and index through their route selections and Google searches; hence, Google has automated the back-end work.
- **Machine Learning** "is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data" while simultaneously learning from it.[8] AI uses TTP mapping, enabled from hierarchical tools, analyst documentation, and algorithms, meaning it must be able to replicate analyst decisions, as seen with IBM's Watson.
- **Databasing** is a systematized and hierarchal collection of data that can be accessed immediately and manipulated by data processing systems for a specific purpose.[9] Usually databasing involves maintaining records composed of hierarchal fields that contain information about a particular phenomenon. Databasing enables machine learning and AI because it contains organized information that AI can understand. In addition, technologists can then create and construct algorithms that emulate human thought in areas such as warnings intelligence, merges/correlations, and anomaly detections.

For intelligence activities, databasing will include adding information to specified data fields, structured reporting, entity enrichment, transliteration, and the implementation of ontological standards.

- **Web Scraping** is the process of extracting targeted information from the internet and storing it locally.[10] Scrapers extract information from websites, portable document formats (PDFs), or other openly available source in order to make it useable for further processing or data enrichment. Entity and topic scraping are used for purposes such as the enrichment of order of battle and identity intelligence, chi-square for anomalies, and trend analysis.
- **A Data Management Strategy** is necessary in order to plan or create a long-term plan for handling data that is "created, stored, managed and processed by an organization. It is an IT [information technology] governance process that aims to create and implement a well-planned approach in managing an organization's data assets" and data equities.[11] A data strategy should include front-end classification tagging, some front-end processing, automated dissemination, geo-tagging, and data modeling.

Getting Back to the Basics. In order to introduce new data methodologies to intelligence tasks, organizations must concentrate on the core competencies: collection by area of intelligence responsibility, PED, analysis, and intelligence synchronization, rather than complicated details or new theories. This means the intelligence apparatus must be optimized against the commander's priority intelligence requirements (PIRs). As such, the intelligence apparatus must focus on the PIRs, specific information requirements (SIRs), specific orders and requests (SORs), source-directed requirements (SDRs), and associated reporting mechanisms. These mechanisms consist of intelligence information reports, tactical reports, reconnaissance exploitation reports, Klieglight reports, intelligence reports, captured enemy material, geospatial intelligence reports, searchable PDFs, annotated PowerPoint slides, simple text reports, and Microsoft Word reports. Consequently, optimizing delivery is as necessary as clean business practices. Some data methodologies that increase efficiencies or lay foundational processes to leverage later, using analytics, apps, interfaces, or statistics include—

- **Develop Word Repositories:** Word-format data is the intelligence community's staple and basic product. Word data is commensurate to transactional data in corporate America, which is used for micro- and macromarketing. When stored in all-source repositories, word data can be used for anomaly detection by instantiating apps that simply use chi-square. In addition, long-term historical analysis can be used by creating phenomenon baselines. For example, the number of extra judicial killings by month and by threat entity. This information can then be examined in the context of current governmental activities, which is often the impetus for an increase or a decrease in this activity. Examples of word repositories are iSight and High Point.
- **Clean Processes:** Go back to the basics on area of intelligence responsibility and intelligence handover lines, enforce PIR-SIR-SOR-SDR linkages and feedback loops, and optimize the intelligence cycle. Enforce the use of intelligence systems of record; and develop interfaces for the Distributed Common Ground System-Army (DCGS–A) to receive that intelligence from commercial and non-program of record tools.
- **Clean Data:** "The process of detecting and correcting (or removing) corrupt or inaccurate records from a record set, table, or database and. . .identifying incomplete, incorrect, inaccurate or irrelevant parts of the data and then replacing, modifying, or deleting the dirty or coarse data."[12]
- **Manage Organizational Technologies and Initiatives:** Annually review initiatives and technologies and fund only those that are effective. Delegate leadership tasks for governance, policy management, and technology funding/perpetuation. Allow for disruptive technological pilots because they challenge the status quo and force technological adaptation.

Interfacing in the Intelligence System of Record, DCGS–A. In order to make these types of systems and tools work seamlessly, interfaces must be developed to create bridges between technologies. Interfaces are independent and often-unrelated services that enable "disparate" systems to communicate, interact, and build upon each other's capabilities. Interfaces require the movement of information multiple ways; therefore, proprietary systems and tools pose a problem for interfaces, as proprietary systems limit the movement of information, usually in a unidirectional way. As such, proprietary technologies inhibit true cross-collaboration and communication because they usually only "receive" data and often "do not share" their own data. Businesses design proprietary business strategies to dominate and control the technology market and extend the life of a particular technology. For leaders, understanding proprietarism is critical in order to decide technological acquisitions, such as interfaces, system features, apps, and future growth.

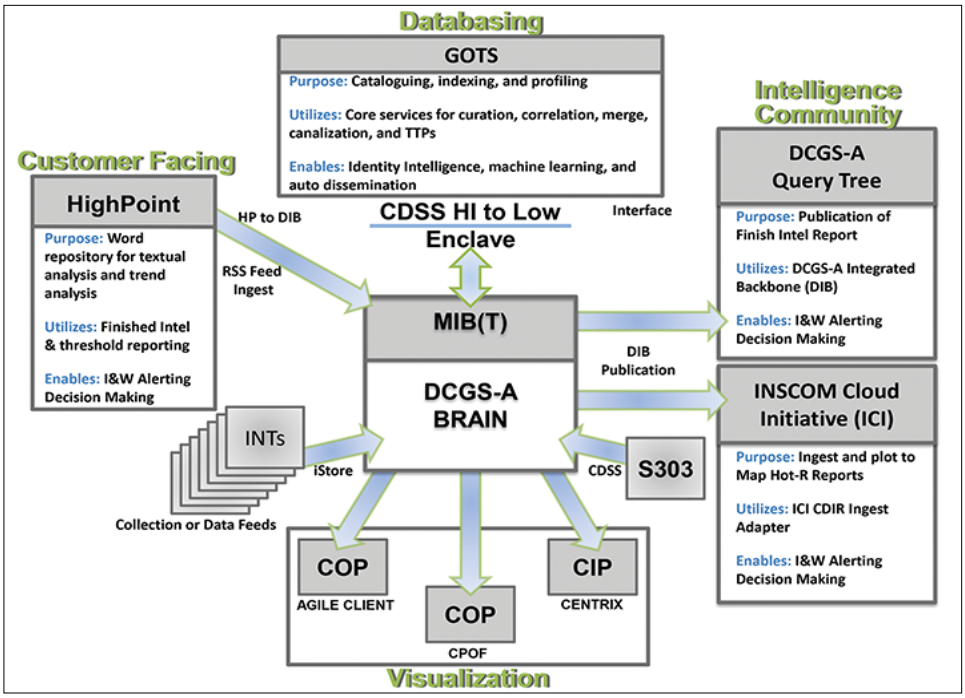


Figure 1. Proposed Information Flow in the 470th Military Intelligence Brigade

To demonstrate cross-collaboration and communication strategy with fully developed interfaces, the proposed strategy (Figure 1) shows four distinct systems and tools with one addition, a government-off-the-shelf (GOTS) solution for databasing with its own interface. This schematic is the proposed solution for the 470th Military Intelligence Brigade and its unique mission set. In the diagram, the interfaces between the technologies are really simple syndication (RSS) feeds (e.g., for enrichment), the DCGS–A Integration Backbone for dissemination, the Cross Domain Solution Suite to create data flows, Oracle's iStore to receive data flows, and a GOTS interface for databasing back-end work. These interfaces create finished intelligence, dissemination methodologies, venues for customer consumption, a common intelligence picture, and other common operating pictures.

Know Your Data. Understanding the purpose behind data allows developers to plan repositories. Optimal repositories have a GUI that mimics how consumers receive information from news media and social media, which reduces training and maximizes consumer consumption and understandability. In addition, it creates relevancy while new features are added in later iterations. Examples of types of data and their corresponding purpose are—

- Word Data: Reports, analytical thought, or intelligence products.
- Metadata: Information about other data (structural, descriptive, and administrative).
- Sensor Data: Collection information.
- Geo-data: Computerized geographically represented information.
- Network Data: Technical information from digital telecommunication networks.

Big Data Decision Making. The most common decision-making model for data management is the Responsibility Assignment Matrix. Essentially, it manages risk by determining who has organizational authority.[13] This methodology accords with AR 600-20, *Army Command Policy*, which assigns legal and intelligence authorities to commanders, unless subsequently delegated. Common questions in this framework include—

"(1) Responsible – Who is completing the task.

(2) Accountable – Who is making decisions and taking actions on the tasks.

(3) Consulted – Who will be communicated with regarding decisions and tasks.

(4) Informed – Who will be updated on decisions and actions during the project."[14]

Although simplistic, the model retains the legal framework necessary to define the decision makers, the doers, and the associated responsibilities.

- **Decision Making:** For what purpose, how much to keep/purge, and where to house the data.
- **Determine Codependencies:** Linking, geos/technologies, intelligence collection, databases, and database access, etc.
- **Define Data by Purpose:** Order of Battle—people, place, and things (database and analyst work), targeting products, lead generation, customer products, etc.

Conclusion

As an intelligence organization, we must consider data management processes, including "acquiring, validating, storing, protecting, and processing required data to ensure the accessibility, reliability, and timeliness of the data for its users" and organizational stakeholders.[15] More importantly, we need a long-term strategy that organizes, makes sense of, and applies analytics to raw data for real-time, military decision making, better customer engagement, and critical insights to threat steams. Optimally, our data management strategy would include:

- Data cleaning.
- Storage considerations by purpose.
- Implementation of core services.
- A suite of web-based tools for analytical work.
- Introduction of necessary intelligence tasks.

These tasks would formalize products that are wedged between intelligence analysis and PED—products such as geos, tips, raw data, running estimates, and targeting products. Second, there should be a unified management process, perhaps an open management standard, to differentiate purposes in the data environment. Planners must understand intelligence storage needs as well as the purpose of storage in their planning efforts.

Epigraph

Norman Davis, "An Information-Based Revolution in Military Affairs," *In Athena's Camp Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (RAND Corporation, 1997), 79, https://www.rand.org/pubs/monograph_reports/MR880.html; and Norman Davis, "An Information-Based Revolution in Military Affairs," *Strategic Review* 24, no. 1 (Winter 1996): 43.

Endnotes

1. Website for Henry Repeating Arms, Inc.; the "Henry History" page, http://www.henryusa.com/henry-history/.

2. Marc Lallanilla, "The Science of World War I: Communications," *Live Science*, May 15, 2014, https://www.livescience.com/45641-science-of-world-war-i-communications.html.

3. Terence Zuber, "The Schlieffen Plan Reconsidered," *War in History* 6, no. 3 (1 July 1999): 262-306, http://journals.sagepub.com/doi/abs/10.1177/096834459900600302?journalCode=wiha.

4. Tillmann Bendikowski, "Moltke: the fallen chief of staff," *Deutsche Welle*, September 4, 2014, 2.

5. Ibid.

6. Pluralsight LLC, "What's the Difference Between the Front-End and Back-End?" https://www.pluralsight.com/blog/film-games/whats-difference-front-end-back-end.

7. Ibid.

8. Charles Zulanas, "From Around the Web: You're Being Disrupted!" *MSS Business Transformation Institute*, January 8, 2017, https://mssbti.com/youre-being-disrupted/.

9. "Database," The Free Dictionary by FARLEX, 2018, https://www.thefreedictionary.com/databasing.

10. Jonathan A. Yee, "Characterizing Crowd Participation and Productivity of Foldit Through Web Scraping" (master's thesis, Naval Postgraduate School, 2016), https://calhoun.nps.edu/handle/10945/48499.

11. "Data Management Strategy," Techopedia Inc., https://www.techopedia.com/definition/30194/data-management-strategy.

12. Ivan Kosyakov, "Decision Tree for Enterprise Information Management (EIM)," *Business Excellence*, April 17, 2017, https://biz-excellence.com/2017/04/17/eim/.

13. Cara Doglione, "Understanding Responsibility Assignment Matrix (RACI Matrix)," *Best Project Management Software Reviews*, July 25, 2018, https://project-management.com/understanding-responsibility-assignment-matrix-raci-matrix/.

14. Ibid.

15. Molly Galetto, "What is Data Management?" *NGDATA*, March 8, 2018, https://www.ngdata.com/what-is-data-management/.

COL Ingrid A. Parker is the commander of the 470th Military Intelligence Brigade at Joint Base San Antonio-Fort Sam Houston, TX. She holds a master of business administration from the University of Phoenix and a master of military art and science from the Army Command and General Staff College. She is a doctoral student at University of Maryland, Baltimore County. Over the years, COL Parker has served in every echelon of the Department of Defense—tactical, strategic, and force providing—with more than 25 years of active, federal service. To date, she has commanded in the Army for 70 months.

Army Processing, Exploitation, and Dissemination Capabilities: Adapt, Evolve, Innovate

by Chief Warrant Officer 3 Otis Griffin III

Processing and exploitation, in intelligence usage, is the conversion of collected information into forms suitable to the production of intelligence...Dissemination and integration, in intelligence usage, is the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions.
***–ADRP 2-0,* Intelligence**

Introduction

The U.S. Army Intelligence Center of Excellence (USAICoE) Requirements Determination Directorate (RDD) Processing, Exploitation, and Dissemination (PED) Team assists the U.S. Army Training and Doctrine Command (TRADOC) in determining required capabilities to assess gaps; to specify risks; and to develop doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) domain solutions. These efforts provide capability analysis and management to develop a combat-ready intelligence force for the Army and joint forces.

Efficiently conducting the intelligence PED of data is the foundation of this effort, beginning with the transition from platform-centric PED to a more holistic enterprise strategy. Tailorable, scalable intelligence PED supports commanders by projecting expeditionary intelligence PED forces into underdeveloped theaters. Once the communications and intelligence architectures mature, each PED can support commanders' intelligence requirements while minimizing forward presence. Regionally focused technical and target immersion provides expert support to regionally aligned forces. By leveraging the full resources of the national to tactical intelligence effort, we will maintain intelligence overmatch. As we move forward, the intelligence warfighting function must develop technology to speed exploitation, tip and cue sensors, and discard less useful data. Ultimately, intelligence PED must evolve to meet the requirements of our complex, rapidly changing operational environments.

Advancing Army PED Capabilities

One manner in which the USAICoE RDD PED Team evolves the required capabilities is by hosting the annual Army PED Summit. The summit and its resulting face-to-face interactions afford the best environment for enhanced collaboration to articulate and align efforts in accordance with PED strategic plans, while addressing the way ahead for the Army PED concept of operations and TRADOC task order. As a core competency, PED is a necessary function that answers information and intelligence requirements to support all components of multi-domain battle and large-scale combat operations. The purpose of the 2017 summit was to discuss the evolution and future of PED capabilities in key areas, given the emerging and forecasted technological advancements of peer and near-peer adversaries. This differed from the previous two summits, which captured operational lessons learned, reviewed PED-related gaps, and identified possible solutions using the DOTMLPF-P domain framework.

According to the Army G-2's strategy booklet, *Army Intelligence 2017-2025: Intelligence at the Speed of Mission Command*, progressively intricate air, land, sea, space, and cyberspace capabilities afford adversaries the potential to challenge U.S. force dominance.[1] This potential is further exacerbated by the enhancement of U.S. air and ground forces toward counterinsurgency operations, which further decreases our ability to effectively counter sophisticated threats. Based on the enhanced enemy threat throughout multiple domains, U.S. forces should expect to be contested across a potentially expansive area of operations from an enemy possessing systems equal to or greater than current U.S. ground combat capabilities.

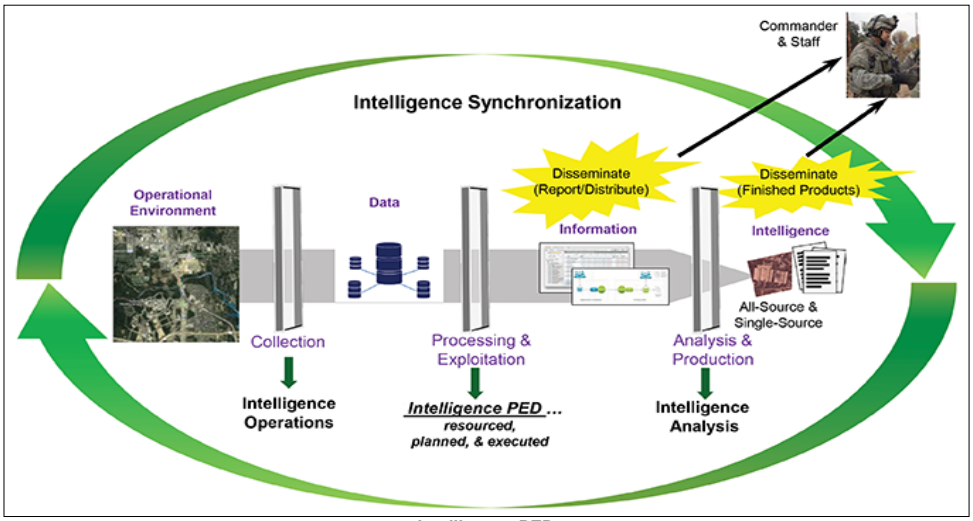
The significance of PED in this instance is that PED supports the Army as part of joint, interorganizational, and multinational teams in protecting the homeland and engaging regionally to prevent conflict and shape security environments, while creating multiple options for responding to and resolving crises.[2] Additionally, the Army PED enterprise includes all forces, from national to tactical, that conduct PED. The primary mission for Army PED personnel at every echelon will be to support their organization's information and intelligence collection assets in enabling mission command. A PED team adapts as the situation develops to support the commander's exercise of mission command and to integrate into the joint, interorganizational, and multinational team.

The Army intelligence strategy document provided foundational data points for the 2017 summit, as it lists three distinctive lines of effort (LOEs)—

- LOE 1, Trained, Ready, and Resilient Soldiers and Civilians.

- LOE 2, Tailored Force.
- LOE 3, Enabling Technology.

Each LOE maintains several nested major objectives; Expand and Evolve PED is Major Objective 2.2 (part of LOE 2). This served as the precursor to reviewing future PED capabilities. It will ultimately provide commanders with decision space to fight from a position of relative advantage.



Intelligence PED

The Summit

From 31 October through 2 November 2017, the USAICoE RDD PED Team hosted the third annual Army PED Summit on Fort Huachuca, Arizona. The summit brought together representatives from—

- Office of the Under Secretary of Defense for Intelligence.
- Headquarters, Department of the Army, G-2.
- U.S. Army Intelligence and Security Command.
- U.S. Army Forces Command.
- U.S. Army Special Operations Command.
- TRADOC.
- U.S. Army Reserve.
- U.S. Army National Guard.
- U.S. Army Service component commands.
- Expeditionary-military intelligence brigades.
- Military intelligence brigades–theater.
- Program Manager, Distributed Common Ground System-Army.
- USAICoE directorates.
- Coalition partners from the United Kingdom, Canada, and Australia.

The primary objective of the summit was to build upon the events of the previous 2 years by focusing on identifying PED gaps and shortfalls, while developing viable solutions for the next 3 to 10 years. The "future of PED" was the summit's theme—intended to align PED capabilities specifically against future operating environments; for example, denied, intermittent, limited; antiaccess; area denial; and dense urban areas (DUAs). The desired outcomes were to—

- Explore and examine future PED capabilities, considering current technologies and complex operating environments.
- Validate existing gaps, discuss new capabilities, and review the available technology's ability to provide solutions.
- Review available solutions based on current and future technologies.

The expressed intent for the 2017 summit was to address the evolution of PED capabilities in key areas, given the emerging and assessed future technological advancements. The RDD PED Team organized the summit's discussions into three distinct areas:

- Adapt: fiscal year (FY) 18 to FY19.
- Evolve: FY20 to FY25.
- Innovate: FY25 and beyond.

Adapt (FY18 to FY19). The summit served as a synergic event to look toward the future and at how emerging science and technology efforts should focus on survivable, interoperable, and relevant architectures; sensor-processing capabilities; and exploitation/analytic tools and technologies from the PED perspective. The summit also focused on ensuring PED capabilities effectively operate in and increase the survivability of denied, intermittent, limited; antiaccess; area denial; and DUA environments, as well as successfully migrating emerging PED capabilities from national agencies to applicable Army intelligence programs.

Evolve (FY20 to FY25). This phase should look to enhance processing and exploitation tools to enable advanced and automated PED processes and to correlate multiple sensor data inputs into a single output. It should also mandate, enforce, and integrate the intelligence community's and joint mission command's data standards within warfighting functions and intelligence capabilities.

Innovate (FY25 and Beyond). The increase of battlespace sensors has resulted in an exponential increase in available data. Yet the pace of current and future operations necessitates usable, consumable, and timely information and intelligence at the speed of mission command. To meet that timeline while reducing the cognitive burden, future

analysts will require powerful automated fusion tools capable of correlating data from various sources. Advanced automated PED capabilities for tasking, processing, fusing, exploiting, and disseminating relevant and observational data require a focused stakeholder effort to develop an integrated and synchronized capability road map.

The Way Ahead

Working with the Department of the Army G-2 PED Team, the USAICoE RDD PED Team will use multiple future force documents to create a PED capabilities strategy "road map" using the adapt-evolve-innovate framework. Capturing the operational capabilities and requirements from the summit, the RDD PED Team will also amend the existing 2014 Army PED concept of operations and associated appendices to reorient the Army PED community of interest to emerging capabilities. Synchronizing these documents will assist the PED community to better posture collective tasks for the future operating environments.

Conclusion

The third annual Army PED Summit achieved its primary objective of examining future PED capabilities based on the current program's evolution and the incorporation of emerging technologies over the next 3 to 10 years. The event allowed substantive discussion on major PED-related materiel requirements and capabilities necessary for improved support to an integrated Army, joint, and unified partner PED enterprise. Additional dialogue in PED stakeholder work groups and key leader engagements is required to further refine the PED capabilities' strategy, leading to recommended actions and mitigating solutions formalized for implementation as part of the Department of the Army PED execute order.

Epigraph

Department of the Army, Army Doctrine Reference Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, 31 August 2012), 4-12.

Endnotes

1. Department of the Army, Office of the Deputy Chief of Staff, G-2, *Army Intelligence 2017-2025: Intelligence at the Speed of Mission Command,* n.d., 2.

2. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army Operating Concept: Win in a Complex World 2020-2040* (Fort Eustis, VA: TRADOC, 7 October 2014), 17. Change 1 was issued on 31 October 2014.

CW3 Otis Griffin III is currently a capability developer and team chief for the Requirements Determination Directorate (RDD) Processing, Exploitation, and Dissemination (PED) Team at the U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. He has served in numerous intelligence positions during his 19-year career, from tactical through strategic levels. Previous assignments include the Brigade Production Manager, 470th Military Intelligence (MI) Brigade-Theater; Syria Crisis Cell Team officer in charge, Defense Intelligence Agency; and Analysis and Control Element Fusion Team Chief, 1st Infantry Division G-2. He holds a master of science in public safety and emergency management from Capella University.

Contributors:

Mr. John DellaGiustina has been the contract task lead for the USAICoE PED Team for the past 7 years. He is a retired MI officer who has planned and executed Army and joint aerial intelligence, surveillance, and reconnaissance/PED missions for Task Force Observe, Detect, Identify, and Neutralize (ODIN) Iraq, 12th U.S. Air Force/U.S. Air Force, Southern Command, and Joint Task Force-6/North. He was the Deputy Training and Doctrine Command Capability Manager (TCM) for the Joint Surveillance Target Attack Radar System/Common Ground Station in TCM Sensor Processing/Distributed Common Ground System-Army, as well as the Coalition Forces Land Component Command, Command and Control Joint Air Control Element and Term Fusion Chief in Operation Iraqi Freedom.

Mr. William Donner has been a capability developer for the RDD, USAICoE, since 2011 and is currently a member of the RDD PED Team. He served 20 years in the Army and retired as a sergeant first class. He was a signals intelligence (SIGINT) and imagery analyst, with assignments ranging from readiness and capabilities noncommissioned officer in charge (NCOIC) for the National Security Agency to Task Force ODIN shift supervisor. His last assignment was as a Senior Leader Course instructor at the Noncommissioned Officer (NCO) Academy, Fort Huachuca, AZ. He has a master of business administration in project management and organizational leadership.

Mr. Zachary Kendrick is a former NCO who served as a SIGINT analyst with the 82nd Airborne Division and Joint Special Operations Command. He deployed multiple times in support of Operation Iraqi Freedom as a SIGINT collector/analyst as well as S-2 NCOIC at the battalion level. After transitioning from the military, he completed his bachelor's degree in business and now serves as a contractor for the USAICoE PED Team.

Mr. James Myatt has been with the USAICoE PED Team for 5 years, with a focus on the terrestrial layer and unmanned aerial system PED. He is a retired Army sergeant first class who worked in several intelligence disciplines throughout his military career. As a civilian, he helped establish and operate the Intelligence Electronic Warfare Tactical Proficiency Trainer in Grafenwoehr, Germany. He assisted and advised Joint Forces Command J-7 information operations and Battle Command Training Program exercise planners on electronic warfare in support of joint military exercises. Upon returning to Fort Huachuca, AZ, he instructed deploying military and civilian personnel on counter radio-controlled improvised explosive device electronic warfare systems.

Building a Strong Europe Through Collaborative Intelligence

by Colonel David W. Pendall and Lieutenant Colonel Christopher J. Heatherly

A strong and free Europe, bound by shared principles of democracy, national sovereignty, and commitment to Article 5 of the North Atlantic Treaty is vital to our security. The alliance will deter Russian adventurism, defeat terrorists who seek to murder innocents, and address the arc of instability building on NATO's periphery.

—Summary of the 2018 National Defense Strategy of the United States of America

Introduction

In 2017, U.S. Army Europe celebrated the 75th anniversary of its founding during the early days of World War II. Officially created on 8 June 1942, U.S. Army Europe was charged to restore peace in Europe—a mission it successfully completed just 3 years later. After the war ended, U.S. Army Europe helped rebuild a shattered European continent, restored democracy, and deterred Soviet aggression against the West. Although the Soviet Union collapsed in 1989, U.S. Army Europe's mission evolved to meet the emerging threats of the late 20th and early 21st centuries. U.S. Army Europe personnel continued to serve on the frontlines of global conflict, intervening to prevent further genocide in the Balkans and deploying forces to the Middle East for Operation Desert Shield/Desert Storm, Operation Enduring Freedom, and Operation Iraqi Freedom.

A Tradition of Service

Today, U.S. Army Europe continues that strong tradition of service and is uniquely positioned in its 51-country area of responsibility to advance American strategic interests in Europe and Eurasia. The mutually beneficial relationships built during more than 1,000 theater security cooperation events in over 40 countries each year support the North Atlantic Treaty Organization (NATO) and multinational contingency operations around the world, strengthen regional partnerships, and enhance global security. A key player throughout U.S. Army Europe's long and distinguished history has been the G-2 through implementation of the intelligence warfighting function. The U.S. Army Europe G-2, in partnership with the U.S. European Command, NATO allies, and regional partners, contributes to the overall safety of Europe through a robust system of intelligence collaboration.

The G-2 is the U.S. Army Europe staff entity responsible for planning and directing the command's intelligence enterprise in support of U.S. Army Europe, U.S. European Command, and NATO intelligence and security requirements. The G-2 has three broad mission sets it achieves on a daily basis:

- Understanding the theater via predictive intelligence analysis, enabling leader decision making.
- Setting the theater by ensuring the readiness of military intelligence (MI) personnel and equipment.
- Building sustained relationships with key allies and partners.

Moreover, it is a team of teams focused on delivering high-quality intelligence reporting, security, and intelligence capabilities that enable mission command. These capabilities also sustain the theater ground component intelligence operational capacity across the operating environment and demonstrate a commitment to the NATO alliance and European partners. The G-2-led enterprise is much more than the combined Civilian-military staff element working inside the headquarters in Wiesbaden, Germany. The G-2 is U.S. Army Europe's most distributed staff element, in terms of assigned billets; it has European-wide operating locations and a breadth of relationships.

U.S. Army photo by SPC Stefan English

Battle Group Poland U.S. Soldiers review the maps and update current activity locations for movements during Saber Strike 2017, at Bemowo Piskie Training Area near Orzysz, Poland, June 15, 2017.

The Year of Integration

U.S. Army Europe declared 2018 as "The Year of Integration," with then Commanding General, U.S. Army Europe, retired LTG Ben Hodges, advocating for a military-free travel zone agreement. The agreement would reduce and streamline the varied host-nation administrative requirements on NATO units moving across borders throughout Europe's NATO countries. This would facilitate military responsiveness and agility as forces deter threats and demonstrate readiness. Recognizing both the wisdom of that goal and how exclusive military-to-military intelligence sharing is insufficient to defeat today's myriad threats, the U.S. Army Europe G-2 maintains a multitude of bilateral and multilateral partnerships with intelligence, security, and host-nation law-enforcement entities across Europe. As such, the G-2 enterprise routinely engages with national and state-level law enforcement agencies and foreign MI partners through scheduled training events, conferences, workshops, or formalized intelligence collaboration agreements. The G-2 has standing partnerships with a wide range of organizations across the global intelligence community, including NATO, combatant and unified commands, the U.S. intelligence community, and bilateral and multilateral agreements.

The U.S. Army Europe G-2 directs a multifaceted organization responsible for key intelligence programs and activities across Europe to accomplish its assigned mission. The enterprise sustains and adapts intelligence architecture and systems with international reach to support forces across the continent, facilitating collaboration with joint, national, host-nation, allied, and partner intelligence services. It provides intelligence support to anti- and counter-terrorism activities and force protection across Europe; facilitates more than 90 NATO, multinational, and joint service exercises annually; and trains more than 270 U.S. and European intelligence professionals each year. Despite being the smallest directorate in terms of personnel on the U.S. Army Europe staff, the G-2 hosts two senior intelligence officer conferences, two military liaison officer conferences, and four Army attaché conferences annually. The G-2 Directorate also supports 15 intelligence training events, engages 40 partner nations, and conducts 60 security cooperation activities annually.

Recognizing that intelligence drives operations, the U.S. Army Europe G-2 is working to more fully integrate NATO allies and partners into a collective intelligence picture to best understand and address potential threats before they may act against U.S., NATO, or partner-nation interests. The G-2 implemented several initiatives to prove the effectiveness of a collective intelligence picture to participating nations and, ultimately, gain additional partners in this process. One such example is the Multi-National Intelligence Readiness Operations Capability (MN-IROC), located in Grafenwoehr, Germany. The MN-IROC provides a ready facility and NATO-accredited information technology infrastructure that enables exercise and real-world on-site multinational intelligence collaboration, training, and multinational analysis. Another Grafenwoehr-based capability, the European Foundry Platform is operated by training cadre assigned to the 66th MI Brigade and the U.S. Army Intelligence and Security Command Foundry Program with overall direction from the U.S. Army Europe G-2. The European Foundry Program delivers advanced skills training on-site and coordinates mobile training to theater-assigned and allocated intelligence units and individual career management field Soldiers and Civilians.

The G-2 further provides contracted translators to units deployed in support of Operation Atlantic Resolve, Kosovo, Joint Multinational Training Group-Ukraine, and Turkey through the Contract Linguist Program Support Office. While engagement and relationship building between intelligence professionals remains our paramount focus, the G-2 has also devoted significant financial resources to achieve its mission. Of the total G-2 annual budget, over 25 percent is earmarked for the G-2's Title 10 support to force

protection missions; and most of our resourcing supports military-to-military intelligence engagements, intelligence capability integration, and relationship-enabling events. Examples of these events include—

- Formal intelligence security cooperation engagements and directed military-to-military training.
- Combined fusion capabilities and network architecture support, including the MN-IROC.
- Partner nation intelligence working groups.
- Intelligence conferences.
- Recurring security events at the local, state, and federal levels with multiple host-nation entities.

Conclusion

At its core, the intelligence enterprise is not solely about systems, processes, or architecture. The most vital element of U.S. Army Europe's intelligence enterprise are the 900 military and Civilian professionals positioned across 17 European nations in support of U.S. Army Europe, our allies, and our partners. They are committed both personally and professionally to ensuring the successful accomplishment of the intelligence mission, initiatives, and agreements. Our current Civilian-military team's individual experience reaches back to 1968 and, when combined, totals thousands of years of collective intelligence work against a vast array of problem sets. These dedicated men and women stand ready to address the new challenges facing our command today and into the future. These are the very people fundamentally contributing to keep Europe Strong.

Epigraph

Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, 9, https://www.defense.gov/portals/1/documents/pubs/2018-national-defense-strategy-summary.pdf.

COL David W. Pendall is currently assigned as the Deputy Chief of Staff G-2, Headquarters, U.S. Army Europe in Wiesbaden, Germany. Commissioned through the Ohio University Army Reserve Officer Training Corps program, COL Pendall holds a bachelor of arts in political science from Ohio University, a master of science in administration from Central Michigan University (CMU), a master's in military art and sciences in theater operations, and a graduate certificate in information systems management from CMU. He is a graduate of the U.S. Army's Command and General Staff College, the Army's School of Advanced Military Studies, the Army War College's Defense Strategy Course, and the Joint Staff College. Previous assignments include battalion and brigade S-2 positions, company command, multiple planning positions, division G-2, and brigade commander. His deployments include Bosnia and Herzegovina, Qatar, Iraq, Turkey, and Afghanistan.

LTC Christopher J. Heatherly is currently assigned as the Deputy G-2 3/5/7, Headquarters, U.S. Army Europe in Wiesbaden, Germany. He graduated from Monmouth College with a double major in business administration and environmental studies. Upon graduation, he enlisted in the U.S. Army and later earned his commission via Officer Candidate School. LTC Heatherly's operational experience includes deployments to Afghanistan, Iraq, Nigeria, Mali, Kuwait, Germany, and South Korea. A career military intelligence officer, LTC Heatherly holds master's degrees from the University of Oklahoma and the School of Advanced Military Studies. He is also a freelance author with nearly 80 publishing credits.

A Special Mission unit on Fort Bragg is looking for qualified 35F/X, 35G, 35M and 35Ls for potential assignments. Serving as a Special Operations Intelligence Sergeant is a unique and challenging assignment. This assignment requires an individual who is highly motivated, confident, intelligent, and capable of working without direct supervision. You will be provided the opportunity to work with many national agencies and state-of-the-art systems in order to execute a unique mission of highest importance. Soldiers assigned here have a great opportunity to seek advanced training, be it civilian or military, and also be offered additional pay and accelerated promotion rates for the increased responsibility we place upon our analysts. We are looking for the right Soldier to be a part of the Army's top intelligence innovators who desire the challenge of conducting analysis for strategically directed operations.

Assignment prerequisites:
- **Volunteer**
- **CMF 35F/X, 35G, 35M, 35L**
- **Minimum 22 years old**
- **Minimum GT Score of 110**
- **Rank of SGT – MSG**
- **Minimum of 4 years - Time In Service**
- **Must be able to pass an APFT – permanent profiles are considered on a case-by-case basis**
- **U.S. citizen**
- **Airborne qualified or volunteer for airborne training**
- **UCMJ / Financial: No recurring adverse actions**
- **Security Clearance: Secret; eligible for upgrade to Top Secret**

If you have any questions or are interested in applying please contact Jody at (910)643-0689/0649 or at army.sofsupport-recruiter@mail.mil.

SINE PARI

Joint Certification of Service Human Intelligence Collector Training and Professional Development

by Chief Warrant Officer 5 Joseph P. Lancaster

War as a Human Endeavor—War is chaotic, lethal, and a fundamentally human endeavor. It is a clash of wills fought among and between people. All war is inherently about changing human behavior, with each side trying to alter the behavior of the other by force of arms. Success requires the ability to outthink an opponent and ruthlessly exploit the opportunities that come from positions of relative advantage. The side that best understands an operational environment, that learns and adapts more rapidly, and that acts more quickly, is most likely to win.

***ADP 3-0,* Operations**

Introduction

Within the Department of Defense's (DoD's) human intelligence (HUMINT) enterprise, foundational training for HUMINT collectors is conducted by the individual services, whereas professional development training is conducted by a joint element—the HUMINT Training Joint Center of Excellence (HT-JCOE). When deployed, HUMINT-trained service personnel generally operate in a joint environment, under a geographic combatant command and component-delegated HUMINT authorities. HUMINT collectors provide operational and intelligence reporting in a joint intelligence information report, which is described in the Defense HUMINT Enterprise Manual 3301.002. Joint certification of service HUMINT training ensures a common operational language and common standards for HUMINT collectors when they deploy or when they attend joint HUMINT professional development courses.

HUMINT Training and Joint Certification

Each individual service initially trains its respective personnel in HUMINT collection under the service's train, man, and equip responsibilities. The U.S. Army's 35M10 HUMINT course trains Soldiers in interrogation, debriefing, and military source operations. The Marine Corps has a Marine Air-Ground Task Force Counterintelligence/HUMINT Course to train military occupational specialty (MOS) 0211 Marines; and the Navy trains its Navy enlisted classification 3913 Sailors in interrogation, debriefing, military source operations, and counterintelligence operations. The HT-JCOE, headquartered at Fort Huachuca, Arizona, delivers follow-on professional development training for these HUMINT disciplines. The HT-JCOE offers additional courses for skill identifiers in debriefing (Defense Strategic Debriefing Course), in source operations (Source Operations Course and Defense Advanced Tradecraft Course), and in specialized functional and topical courses.

DoD Instruction (DoDI) 3305.15, *DoD Human Intelligence (HUMINT) Training and Certification*, establishes the requirement to develop HUMINT training standards and to provide oversight of training. The Joint Coordination Element (JCE) was chartered under the auspices of the Defense Intelligence Agency and the Joint J-7 staff to meet the requirements of DoDI 3305.15. JCE's mission is to certify training and standards through the joint certification process. Subject matter experts from each service conduct the comparative review of service MOS and the Universal Joint Task List; review lesson plans; and observe, verify, and validate the conduct of HUMINT training. Each service has used the joint certification process to validate its own foundational training course and to ensure the consistency of tasks and training standards with the DoD's HUMINT enterprise.

Joint certification of service and HT-JCOE HUMINT training courses has enabled the development of a shared operational vocabulary and has better prepared 35M Soldiers, 0211 Marines, 3913 Sailors, and Navy intelligence debriefers to operate under joint authorities and to report in a commonly understood joint format when operationally employed and deployed. Personnel from each service are already exposed to Universal Joint Task List standards. They are also conditioned toward success when participating in professional development and advanced HUMINT training at HT-JCOE or throughout the HUMINT enterprise, and they are able to perform to common standards when deployed.

Conclusion

Joint certification provides a valuable external technical review to ensure the Army's foundational 35M10 HUMINT course is consistent within the DoD's HUMINT enterprise for technical tasks and operational doctrine. This ensures the Army's HUMINT Soldiers are prepared to operate effectively under joint and geographic combatant commander authorities, both in deployed and in garrison environments.

CW5 Joseph P. Lancaster is a senior human intelligence (HUMINT) collector with 31 years of service as a HUMINT collector, interrogator, and debriefer at U.S. Forces Command, U.S. Army Intelligence and Security Command, U.S. Army Training and Doctrine Command, and U.S. Special Operations Command. He previously served as the 35M course officer in charge at the U.S. Army Intelligence Center of Excellence.

Devil Strike Paratroopers: Winners of the Major General Oliver W. Dillard Award for FY 2017

by Major Jason M. Elphick

The MG Oliver W. Dillard Award honors the most outstanding company-size military intelligence (MI) unit assigned to a brigade combat team. Although MG Dillard was an infantry officer during the Korean and Vietnam Wars, he was a decorated battalion S-2 in Korea and became U.S. Army Forces Command's (FORSCOM's) first Deputy Chief of Staff for Intelligence (G-2) in 1973. He continued his service as an infantry officer within an MI functional area, and as the senior intelligence officer in U.S. Army Europe from 1975 to 1978 he promoted the use of intelligence Soldiers and units at the tactical level. MG Dillard received the Thomas W. Knowlton Award for Intelligence Excellence and is a member of the Army's Military Intelligence Corps Hall of Fame and the Alabama Military Hall of Honor. MG Dillard symbolizes the promotion of esprit de corps and professionalism in MI units throughout FORSCOM.

COL Ryan M. Janovic, FORSCOM Deputy Chief of Staff, G-2, officially designated Delta Company, 127th Airborne Engineer Battalion, 1st Brigade Combat Team, 82nd Airborne Division, at Fort Bragg, North Carolina, as the MG Oliver W. Dillard Award recipient for fiscal year (FY) 2017. Under the leadership of CPT Miguel A. Urbina and 1SG Harold E. Jarrell, the Soldiers of Delta Company demonstrated excellence in training and support to operations in both garrison and deployed combat environments.

Delta Company paratroopers spent half of FY17 maintaining their focus on individual and unit readiness through their participation in multiple company, battalion, and brigade-level training exercises. While maintaining a high training operational tempo, Delta Company paratroopers provided the bulk of all-source and geospatial intelligence to the brigade intelligence support element, providing daily support and situational understanding to the 1st Brigade Combat Team, 82nd Airborne commander. Additionally, the Tactical Unmanned Aircraft System Platoon was the first in FORSCOM to complete the 600-flight-hour proficiency requirement.

In June 2017, Delta Company deployed to Afghanistan in support of Operation Freedom's Sentinel. Delta Company task-organized themselves to better support operations and enable aerial intelligence, surveillance, and reconnaissance in four geographically dispersed locations while continuing to man the Kandahar Intelligence Fusion Center. In so doing, Delta Company paratroopers ensured intelligence was effectively nested with operations and enabled increased force protection of U.S. and coalition forces.

The Devil Strike paratroopers of Delta Company, 127th Airborne Engineer Battalion, 1st Brigade Combat Team, 82nd Airborne Division, serve as role models for other FORSCOM intelligence professionals. The company epitomizes esprit de corps and professionalism in the MI Corps and is designated the most outstanding company-size MI unit assigned to a brigade combat team in FY17.

MAJ Jason Elphick is the Army National Guard advisor to the U.S. Army Forces Command (FORSCOM) G-2. Since 2015, he has worked to integrate and operationalize Army National Guard intelligence equities within FORSCOM. He holds a bachelor's degree from Brigham Young University and a master's in business administration from Webster University in St. Louis, MO.

Seek and Disrupt Battalion: Winners of the Brigadier General Roy M. "Bud" Strom Award for FY 2017

by Major Jason M. Elphick

The BG Roy M. "Bud" Strom Award honors the most outstanding company-size military intelligence (MI) unit assigned to an expeditionary-MI brigade or theater support battalion. BG Strom was commissioned as an artillery officer in 1954 and transitioned to MI assignments after his attendance at the Gunnery School at Fort Sill, Oklahoma. He commanded the 519th MI Battalion, 525th MI Group, in Vietnam and subsequently took command of the 4th MI Battalion, 525th MI Group, responsible for intelligence operations in the Delta region. BG Strom's third command was the 18th MI Battalion, 66th MI Group, in Munich, Germany. A graduate of the Industrial College of the Armed Forces, he also commanded the 500th MI Brigade, Intelligence and Security Command, at Camp Zama, Japan. In 1982, BG Strom returned to Washington, DC, to become the Army's Deputy Assistant Chief of Staff for Intelligence. His final assignment was to serve as U.S. Army Forces Command (FORSCOM) Deputy Chief of Staff, Intelligence, until his retirement in 1985.

COL Ryan M. Janovic, FORSCOM Deputy Chief of Staff, G-2, officially designated Bravo Company, 109th Expeditionary MI Battalion, 201st Expeditionary MI Brigade, at Joint Base Lewis-McChord, Washington, as the inaugural BG Roy M. "Bud" Strom Award winner for fiscal year (FY) 2017. Under the leadership of CPT Bryan J. Nesbitt and 1SG Marvin J. Meertens, the Soldiers of Bravo Company, 109th Expeditionary MI Battalion, demonstrated an exceptional commitment to the high standards of the MI Corps while serving in training and operational environments.

The centerpiece to any expeditionary MI battalion is its collection capability. Bravo Company achieved the distinction as "top team" in two installation MI master gunner events. Their multifunction teams went on to validate their skills during two brigade combat team rotations through the National Training Center at Fort Irwin, California. The teams earned accolades from both rotational commanders for their operational contributions. Bravo Company expanded on these training achievements by providing over 740 hours of real-world full motion video processing, exploitation, and dissemination in support of Operations Inherent Resolve and Pacific Eagle.

Bravo Company's influence extends beyond its military mission and includes a commitment to each other, the community, and their families. The Bravo Company command team emphasized family readiness through support to the family readiness group and by maintaining steady communication between them and the families. The family readiness group hosted many events, including a barbecue, a "pie-in-the-face" fundraiser, and a springtime Sports Day that included a running clinic. They also won third place in the Joint Base Lewis-McChord Commander's Cup bowling tournament. Bravo Company Soldiers continue to build unit cohesion and demonstrate their commitment to excellence.

The leaders and Soldiers in Bravo Company, 109th Expeditionary MI Battalion, serve as role models for other FORSCOM units and U.S. Army intelligence professionals. The company epitomizes esprit de corps and professionalism in MI and is the most outstanding company-size MI unit assigned to an expeditionary-MI brigade or theater support battalion in FY17.

MAJ Jason Elphick is the Army National Guard advisor to the U.S. Army Forces Command (FORSCOM) G-2. Since 2015, he has worked to integrate and operationalize Army National Guard intelligence equities within FORSCOM. He holds a bachelor's degree from Brigham Young University and a master's in business administration from Webster University in St. Louis, MO.

Distinguished Members of the Military Intelligence Corps

The Honorary Officers and the Distinguished Members of the Corps are essential to the accomplishment of the Corps' purpose—to establish a sense of espirit de corps within military intelligence (MI), unifying MI Soldiers and Civilians in a common bond of mission and fellowship. Living legends of MI, they link today's intelligence Soldiers and Civilians with our proud past. These special appointees represent every aspect of the MI profession. The Honorary Colonel, Honorary Chief Warrant Officer, and Honorary Sergeant Major of the MI Corps each serve for 3-year terms (renewable once), and then they become Distinguished Members. The tenure of the Distinguished Members in indefinite.

Outgoing Honorary Colonel

Colonel Alfred H. Elliott, III
U.S. Army, Retired
Honorary Colonel of the MI Corps (2012-2018)

COL Elliott was commissioned a second lieutenant in infantry in 1969, and the following year, he completed helicopter flight training. He served as a helicopter pilot in Vietnam for 16 months. He subsequently was assigned to the 2nd Armored Cavalry Regiment where he began his long association with Army intelligence, serving as a border reconnaissance troop commander and flying surveillance and reconnaissance missions along the inner-German border. Later COL Elliott was awarded an alternate skill specialty as a signals intelligence officer and, upon graduation, received his first true intelligence assignment with the Joint Electronic Warfare Center.

While assigned as Chief, Requirements Branch, Deputy Chief of Staff for Intelligence, U.S. Army Europe and Seventh Army (USAREUR), COL Elliott was a major force behind the successful development and restructuring of the USAREUR intelligence strategy and associated architectures for post-Cold War Europe. Among his most significant contributions were the fielding of the Tactical Radar Correlator System and assisting in concept and architecture development for deploying the first TROJAN SPIRIT to the Gulf War. COL Elliott's final job in Europe was Deputy Commander of the 66th MI Brigade.

COL Elliott then spent three years at the U.S. Army Intelligence Center, first as Director of Combat Developments and then as Garrison Commander. His final assignment was Chief, Intelligence and Electronic Warfare Division on the Army Staff. COL Elliott retired from the U.S. Army in 1999. He was inducted into the MI Hall of Fame in 2003 and has served as the Honorary Colonel since 2012.

Incoming Honorary Colonel

Colonel James V. Slavin
U.S. Army, Retired
Honorary Colonel of the MI Corps (29 June 2018)

Commissioned through the U.S. Military Academy in 1975, COL Slavin's first intelligence assignment was as an infantry battalion S-2 and infantry company commander for the 506th Infantry Battalion (Currahee), 101st Airborne Division. He then served as detachment commander, watch officer, and battalion S-3 at Field Station Augsburg in Germany.

After a year instructing at West Point, he was assigned as the Operations Officer for the 525th MI Brigade at Fort Bragg, followed by positions as S-3 and Executive Officer for the 519th MI Tactical Exploitation Battalion. He then served consecutively as Assistant G-2 of Operations and Deputy G-2 of the 7th Infantry Division at Fort Ord, California, where he instituted the first counterdrug intelligence preparation of the battlefield methodology.

After an assignment as the Regional Division Commander, Joint Intelligence Center, Atlantic Command, in Norfolk, Virginia, COL Slavin returned to Fort Bragg as the Director of Intelligence for Special Operations Division, Delta Force. From there, he went to Camp Zama as the G-2 of U.S. Army Japan. Selected to command the U.S. Support Group (East Timor), COL Slavin deployed just days after the terrorist attacks on 11 September 2001.

In 2003, COL Slavin became Director of Joint and Allied Doctrine for Training and Doctrine Command. His last active duty assignment was as a strategic planner for the Coalition Provisional Authority, Baghdad, Iraq. He retired from the U.S. Army in 2005 after 30 years of service.

COL Slavin was inducted into the MI Hall of Fame in 2012.

Outgoing Honorary Chief Warrant Officer

Chief Warrant Officer 5 Rex A. Williams
U.S. Army, Retired
Honorary Chief Warrant Officer of the MI Corps
(2014-2018)

CW5 Williams enlisted in 1971 as an imagery analyst. He served in the 2nd MI Battalion, Aerial Reconnaissance Support, at Zweibrucken Air Force Base, Germany; the 1st MI Battalion, Aerial Reconnaissance Support, at Fort Bragg; and the 704th MI Detachment, Aerial Surveillance, in Pyong Taek, Korea.

Appointed as a warrant officer in 1978, he was assigned to the Intelligence Center's Directorate of Combat Developments as an action officer for imaging systems, unmanned aerial vehicles, the Joint Surveillance Target Attack Radar System, and all airborne radars. After tours as the Chief, All-Source Production Section, 2nd Infantry Division, in the Republic of Korea, and principal threat instructor for the MI Officer Basic and Advanced courses at Fort Huachuca, CW5 Williams moved to the Pacific Command. He led a 19-member inter-service consolidated order of battle section that published intelligence products for the Defense Intelligence Agency (DIA). In 1989, his section was honored as the DIA Intelligence Producer of the Year.

Aside from an assignment as the Chief of the Intelligence Production Branch at the Joint Intelligence Center, U.S. Central Command, CW5 Williams spent the rest of his career at the Army Intelligence Center. From 1999 until 2001, he served as the first Chief Warrant Officer of the MI Corps. His final assignment was technical advisor to the Chief, Concepts, Architectures, and Requirements in Combat Developments. He retired from the U.S. Army in 2003 and was inducted into the Hall of Fame in 2005. He has served as the Honorary Warrant Officer since 2014.

Incoming Honorary Chief Warrant Officer

Chief Warrant Officer 5 Richard L. Swarens, Jr.
U.S. Army, Retired
Honorary Chief Warrant Officer of the MI Corps
(29 June 2018)

CW5 Swarens enlisted in the U.S. Army as a counter-intelligence (CI) assistant in 1982. He completed tours at the 311th MI Battalion and 902nd MI Group before being appointed a CI warrant officer in 1988. He returned to the 311th MI Battalion as a CI technician and battalion S-2 and deployed the first tactical CI team into Saudi Arabia during Operation Desert Shield.

In 1992, while assigned to the 18th MI Battalion in Germany, CW5 Swarens created and implemented security procedures for a new human intelligence computer architecture and became a driving force behind the automated data processing security field. After a year as the Operations Officer of the CI Detachment, he deployed as the only American CI officer in the combined task force in support of Operation Provide Comfort in Northern Iraq and Turkey. He was then selected to command a CI detachment providing support to the Netherlands, Belgium, Northern Germany, and Luxembourg.

CW5 Swarens spent two years as Chief of the CI Training Committee at the U.S. Army Intelligence Center and then transferred to the Third Army G-2 Section. He deployed in support of Operation Bright Star in Alexandria, Egypt, and became the lead security interface with Egyptian forces on 11 September 2001. In 2002, CW5 Swarens was chosen as the Deputy Director of Security in the White House Military Office. He retired from active duty in 2008 after 26 years in uniform.

CW5 Swarens was inducted into the MI Hall of Fame in 2012.

Distinguished Members of the Military Intelligence Corps

Outgoing Honorary Command Sergeant Major

Command Sergeant Major James A. Johnson
U.S. Army, Retired
Honorary Sergeant Major of the MI Corps
(2012-2018)

CSM Johnson enlisted in the Marines in 1965, serving a 17-month tour in Vietnam. After joining the Army in 1970, he was assigned first to the 400th U.S. Army Security Agency Special Operations Detachment (SOD) in Okinawa, and then to the 402nd SOD at Fort Devens, Massachusetts, where he was part of the initial cadre that developed the concept of direct MI support to special forces.

In 1982, CSM Johnson served as Operations Sergeant and First Sergeant with the Support Battalion, U.S. Army Field Station Augsburg. He then became the First Sergeant of the 519th MI Battalion, 525th MI Brigade, before being selected as the Command Sergeant Major of the 3rd MI Battalion (Aerial Exploitation), Republic of Korea.

As the Command Sergeant Major of the 111th MI Brigade at Fort Huachuca in 1989, CSM Johnson administered a program to support and monitor drill sergeants, and he established a training program to prepare the newly formed unmanned aerial vehicle platoon for deployment to Operation Desert Storm. In 1991, CSM Johnson was selected as the Command Sergeant Major of the U.S. Army Intelligence Center and Fort Huachuca, which also made him the Command Sergeant Major of the MI Corps.

CSM Johnson's last assignment was Command Sergeant Major of the Intelligence and Security Command in 1993. He retired from the U.S. Army in 1995. CSM Johnson was inducted into the MI Hall of Fame in 2005 and has served as the Honorary Sergeant Major since 2012.

Incoming Honorary Command Sergeant Major

Command Sergeant Major Franklin A. Saunders
U.S. Army, Retired
Honorary Sergeant Major of the MI Corps
(29 June 2018)

CSM Saunders entered the U.S. Army in 1983 and spent the first 10 years in field artillery and special forces. He then reclassified as a 96U, Tactical Unmanned Aerial Vehicle (UAV) Operator. His first intelligence assignments were as an intelligence analyst with the 7th Special Forces Group; platoon sergeant for Company D, 304th MI Battalion; and then First Sergeant of the Army's first tactical UAV company at Fort Hood, Texas.

During his 27-year career, CSM Saunders served in a variety of leadership and staff positions, including squad leader; platoon sergeant; battalion operations sergeant; first sergeant; brigade operations sergeant major; battalion command sergeant major; brigade command sergeant major; the Army War College and Carlisle Barracks Command Sergeant Major; and U.S. Army Intelligence Center, Fort Huachuca, and MI Corps Command Sergeant Major. He retired in 2010 as the U.S. Army G-2 Command Sergeant Major.

As both a trainer and a leader, CSM Saunders had significant impacts on the MI Corps, and his fingerprints are on many Army intelligence programs of the 21st century, including increased human intelligence training, Distributed Common Ground System-Army across our formations, persistent surveillance platforms, the Every Soldier a Sensor program, company intelligence support teams, and multifunctional teams. When he became the Senior Enlisted Advisor to the Deputy Chief of Staff, G-2, he championed every aspect of the Army G-2's mission and vision to transform and rebalance the Army MI force.

CSM Saunders was inducted into the Hall of Fame in 2013.

Distinguished Members of the Military Intelligence Corps

The Military Intelligence Corps 2018 Hall of Fame Inductees

Colonel Robert Reuss, U.S. Army, Retired

Robert Reuss enlisted in the U.S. Army in 1969 and a year later graduated from the Officer Candidate School with a commission as a second lieutenant in military intelligence (MI). He spent the first decade of his career alternating between operational and institutional assignments. As the 1st Armor Division Artillery S-2, he was one of the first MI officers to serve as a maneuver S-2 in the forward-deployed divisions in U.S. Army Europe (USAREUR). After three years at the U.S. Army Security Agency Training Center and School, Fort Devens, Massachusetts, he served four years as a G-3 electronic warfare officer at VII Corps. He then spent three years at the Command and General Staff College, instructing future senior leaders to embrace intelligence as the first element in operational planning.

In 1987, COL Reuss was assigned as the G-2, 1st Armored Division. One of his most noteworthy achievements was bringing National Training Center force-on-force training standards to USAREUR, significantly influencing combat readiness of European forward-deployed forces. In 1990, he deployed the first divisional MI battalion for Operations Desert Shield/Desert Storm. He commanded the 124th MI Battalion throughout the conflict, providing force protection in advance of the division and working with the Division G-2 to orchestrate air and ground combat intelligence operations in Saudi Arabia and Iraq.

In 1993, COL Reuss became the Deputy Chief of Staff for Intelligence at the U.S. Army Training and Doctrine Command (TRADOC). Applying lessons learned from Operation Desert Storm, he coordinated the integration of intelligence support and capabilities into the Army's long-range planning for Force XXI and Army After Next concepts. He followed his TRADOC assignment with command of the National Ground Intelligence Center (NGIC) from 1995 to 1997. He directed the development of innovative analytical and collaborative tools that enabled NGIC to provide timely and relevant reachback support for deployed forces.

In 1997, COL Reuss deployed as the CJ2 for the Stabilization Force Bosnia. Responsible for more than 450 coalition personnel, he forged an effective team that substantially improved theater surveillance operations; established theater security policy; introduced an analytical capability targeting public corruption; provided tailored intelligence products for Theater Special Operations; and maintained situational awareness of the potentially destabilizing conflict in Kosovo.

COL Reuss's final military assignment was as the DJ2 for U.S. Atlantic Command (later the Joint Forces Command). His experience in Bosnia enabled him to successfully design and field an all-source intelligence team using assets from the Joint Intelligence Center, J-2 staff, and National Agency representatives. Responding to several national crises, he spearheaded a groundbreaking effort to stand up a joint task force for civil support, breaking down many of the barriers between the Department of Defense and national and local law enforcement that had historically impeded progress and transparency.

COL Reuss retired from active duty in 1999 and served an additional 15 years as a defense intelligence senior-level leader at TRADOC, retiring in 2015. COL Reuss's awards include the Defense Superior Service Medal, Legion of Merit, Bronze Star, Meritorious Service Medal, Army Commendation Medal, and Army Achievement Medal.

Lieutenant Colonel Ellis C. Atchison, U.S. Army, Retired (Deceased)

Ellis Atchison enlisted in the Army in 1940 and graduated from the Officer Candidate School in 1942. He was assigned as a radio intelligence officer to the newly constituted 138th Signal Radio Intelligence Company (later redesignated the 1st Army Air Force Radio Squadron, Mobile (J) [RSM]), which was sent to Port Moresby, New Guinea, in 1943. From then until the end of the war in 1945, Atchison led or participated in numerous operations in support of all U.S. Army Air Force units in the Southwest Pacific Area, providing life-saving intelligence to commanders during the campaign to retake the Philippine Islands and later operations on Okinawa.

In addition to his duties as a radio intercept officer, then 1LT Atchison was the designated supply officer charged with supplying, dispatching, and at times commanding small units operating in multiple isolated locations. These units conducted radio intercept, direction finding, cryptanalysis, and traffic analysis of Japan's army, air, and naval forces communications. His unit's successes included the decryption of an enemy message that alerted the Allies to a major concentration of Japanese air strength in Hollandia, New Guinea, where GEN Douglas MacArthur was planning an invasion. In response, the 5th Air Force launched massive raids that destroyed more than 100 enemy planes and ensured American forces could land on the island virtually unopposed. In other instances, Atchison and his men warned units of incoming enemy air attacks and pending ground reinforcements. His squadron also broke the Japanese weather reporting code used by Japanese pilots, which alerted American bomber crews of the weather conditions over their targets. Once in the Philippines, Atchison activated and commanded Detachment 2, the first unit of its kind to operate in the field in a mobile state. Working near the front lines in the Philippines and in Okinawa, the unit was often involved in direct action against the enemy.

In May 1945, the 1st RSM was awarded the Philippine Presidential Unit Citation for its interception, decoding, and direction-finding efforts that led to the elimination of Japanese air activity. In January 1946, the unit was awarded a Meritorious Service Unit plaque by the Commanding General, Pacific Air Command. The citation read, in part, that the unit *"obtained information that was of inestimable value…in the detection of planned enemy air raids far in advance of the actual time of the proposed strike, enabling our forces to effect air interception of the enemy prior [to] his arrival over our installations."*

Following the war, LTC Atchison continued to be in the forefront of signals intelligence. Using the valuable lessons learned during World War II, he assisted in developing and implementing radio intelligence training for the Army Security Agency (ASA). Later, he helped establish the Army Language School and the U.S. Air Force Security Service. In the 1950s, LTC Atchison served as the security officer for three Secretaries of Defense and commanded the 5th ASA Field Station in Helemano, Hawaii. He then served at the National Security Agency until his retirement in November 1960.

LTC Atchison's military awards and decorations include the Bronze Star for his 27 months in the Southwest Pacific and the Army Commendation Medal. LTC Atchison passed away in May 2016 at the age of 100.

Chief Warrant Officer 5 Paul L. O'Meara, U.S. Army, Retired

Paul O'Meara enlisted in the Army in 1981 and served his first nine years as a nuclear weapons specialist. He became a warrant officer in 1988 and then transitioned into military intelligence (MI) as a counterintelligence and human intelligence (HUMINT) agent. For the next 25 years, he held various positions throughout the United States and commanded the field office at Fort Knox, Kentucky, and detachments at the 524th MI Battalion in the Republic of Korea. He also deployed as the operations chief, Combined Task Force J-2, to Bosnia and Herzegovina in 2001; as the U.S. Special Operations Command's project officer in 2001; as the U.S. Special Operations Command's liaison officer to the Federal Bureau of Investigation during Operation Enduring Freedom in 2002; and as the senior HUMINT advisor to multinational forces Iraq in 2005.

Chief O'Meara's most enduring contributions to the MI Corps came during his final assignment as the warrant officer life cycle manager at the U.S. Army Intelligence Center (USAIC) and as the fourth chief warrant officer of the MI Corps from 2006 to 2010. During the course of these five years, his accomplishments had a tremendous and enduring impact on the MI Corps' ability to recruit, retain, manage, and educate the MI Warrant Officer Corps.

First, determined to improve the health of the MI Warrant Officer Corps, he implemented innovative solutions, such as accession and retention bonuses and an increased number of enlisted feeder military occupational specialties (MOSs), and he marketed warrant officer opportunities to the enlisted MI community around the world. His efforts led to an unprecedented increase in the number of MI warrant officers from 800 to 1,400 over three years, with every MI warrant officer MOS filled to no less than 89 percent strength.

Second, after dually serving as the chief warrant officer of the Corps and the warrant officer life cycle manager, he successfully fought to separate the two distinct positions in 2008. CW5 O'Meara thus became the first warrant officer to serve solely as the chief warrant officer of the MI Corps. In this position, he advised the commanding general of USAIC on the recruitment, retention, management, and professional development of the MI Warrant Officer Corps. Amid concerns that the curriculum at USAIC lacked relevancy, he recruited the very best warrant officers with recent combat experience to instruct and then overhauled the course material within Warrant Officer Professional Military Education

courses. He also extended the Warrant Officer Advanced Course from four to six weeks to incorporate focused training on the complex technical skills within each respective MOS.

Finally, CW5 O'Meara changed the culture of the MI Warrant Officer Corps by emphasizing the Army's decision to transition warrant officers from specialists to commissioned officers within the greater officer corps. Circulating among the force, he challenged the warrant officer community not only to be technical specialists but also to redefine their role and embrace their leadership position within the force.

CW5 O'Meara retired in 2010, culminating his 29-year military career. He continues to support the intelligence community in HUMINT collection operations for the Department of Homeland Security's central region.

CW5 O'Meara's military awards include the Combat Action Badge, Legion of Merit, Bronze Star, Defense Meritorious Service Medal, Meritorious Service Medal, Joint Service Commendation Medal, Army Commendation Medal, and Army Achievement Medal.

Command Sergeant Major Dennis M. Rydell, U.S. Army, Retired

Dennis Rydell began his military career as a Marine in 1977. By 1980, he had transitioned to the U.S. Army, had completed signals intelligence (SIGINT) training, and was serving as a senior non-Morse intercept operator in Eastern Europe. In 1984, he served as an instructor at the Naval Technical Training Center in Pensacola, Florida. He returned to Eastern Europe in 1987. While serving as the collection noncommissioned officer in charge (NCOIC) at Field Station Berlin in 1989, he and his team collected the first actionable intelligence on the dismantling of the Iron Curtain.

Returning to the United States, CSM Rydell was assigned to the 344th Military Intelligence (MI) Battalion where he served as an instructor and battalion operations noncommissioned officer. He was then reassigned to the 513th MI Brigade, 201st MI Battalion, where he served on the advance party with the relocation of the brigade from Fort Monmouth, New Jersey, and the 201st MI Battalion from Vint Hill Farms, Virginia, to Fort Gordon, Georgia. While assigned to the 201st MI Battalion at Fort Gordon, he forward deployed as the NCOIC of a SIGINT collection team in Bahrain and oversaw the training provided to the Saudi Arabia Ministry of Defense Intelligence Directorate as part of the Theater Security Cooperation initiative. Returning to the 201st at Fort Gordon, he served as the 1SG of A Company. The next year, he became 1SG of D Company, which established the first regional technical control and analysis element inside the Gordon Regional SIGINT Operations Center, which enhanced the Army's national to tactical integration and partnership with the National Security Agency.

In 1997, CSM Rydell arrived at Menwith Hill Station, England, as the 1SG of a Headquarters and Operations Company, 713th MI Group, where he earned the Award of Excellence in Leadership presented by the Director of the National Security Agency.

From 1999 to 2005, CSM Rydell served with the 504th MI Brigade at Fort Hood, Texas. After a year as the brigade operations sergeant major, he was assigned as the III Corps senior intelligence sergeant, analysis and control element. Returning to his position as the 504th MI Brigade operations sergeant major, he was crucial in the activation and mobilization of B Company, 321st MI Battalion (Reserve), and

ensuring the battalion was prepared for its mission to stand up the Guantanamo Bay detention camp in 2002.

From 2002 to 2005, CSM Rydell served as the 15th MI Battalion (Aerial Exploitation) command sergeant major, during which time he deployed twice in support of Operation Iraqi Freedom. In August 2005, he was selected as the command sergeant major of the 470th MI Brigade at Fort Sam Houston, Texas. His team provided intelligence products to support the Global War on Terrorism, U.S. Army South (USARSO), and U.S. Southern Command missions.

After a five-month assignment as command sergeant major, USARSO, CSM Rydell returned to the 470th to stand up the Army's first Joint Interrogation and Detention Center, 201st MI Battalion.

CSM Rydell retired in 2007, culminating a 30-year military career. He continues to support Army intelligence as the senior civilian advisor in the 116th MI Brigade at Fort Gordon, Georgia. CSM Rydell's military awards include the Legion of Merit, Bronze Star, and Meritorious Service Medal (4th Award).

Mr. Michael T. Warnock, Chief Warrant Officer 3, U.S. Army, Retired (Deceased)

Michael Warnock enlisted in the Army in 1968. After initially training as a personnel specialist, he transitioned to military intelligence in 1972, becoming a counterintelligence (CI) agent. He was one of the first automated data processing focused CI agents and used those skills to develop a CI/terrorist threat database that drove the Allied Command Europe capability to counter emerging threats. Appointed a warrant officer in 1980, he was selected to serve as a CI agent with 1st Special Forces Operational Detachment-Delta in 1982. He deployed during Operations Urgent Fury in Grenada and Just Cause in Panama, and for Scud suppression operations during Desert Storm in Iraq.

CW3 Warnock retired from the Army in 1991 and immediately embarked on a 21-year career as a Department of the Army Civilian with the Joint Special Operations Command (JSOC). His Civilian service included multiple combat deployments to Bosnia and Somalia, and eight separate deployments to Afghanistan. During every deployment, he consistently provided accurate and timely human intelligence (HUMINT) to tactical and operational commanders. During his deployment with Task Force Ranger (Operation Gothic Serpent) to Mogadishu, he proved fundamental to the success of CI operations, HUMINT support, low-level source operations, and operational security of the deployed forces. He mentored and led local law enforcement personnel during high-risk operations and personally caused the capture of over $4 million in U.S. currency intended to support the revolutionary faction.

In the spring of 2004, he deployed for the first time in support of Operation Enduring Freedom in Afghanistan, where he served as the task force CI coordinating authority for a Joint Special Operations Task Force (JSOTF) working directly for the National Command Authority. He also managed nascent JSOTF detainee operations. Between 2005 and 2011, Mr. Warnock deployed seven more times to Afghanistan as the JSOTF J2X. He adeptly managed HUMINT collection teams at 12 remote locations throughout Afghanistan. By teaming analysts with HUMINT collectors, he ensured a significant increase in the quantity and quality of HUMINT reporting. The intelligence collected by his case officers resulted in the capture/kill of numerous Taliban and al-Qaida personnel. He also led the force protection and CI support during the successful mission to kill Osama bin Laden.

In addition to repeated combat deployments, Mr. Warnock drove the command's force protection operations in the United States. He was the primary interface between JSOC, the Federal Bureau of Investigation, and the intelligence community during a high-profile investigation that resulted in the conviction of a U.S. service member for attempting to spy for China.

Finally, Mr. Warnock was one of the primary architects and a plank owner for the JSOC J2X established in 2005. The organization he built to expand CI and HUMINT collection and analysis within JSOC continues to support the national mission force more than 10 years later.

Mr. Warnock passed away in May 2012 while preparing for his ninth deployment to Afghanistan. His military awards include the Legion of Merit, Bronze Star, Meritorious Service Medal, Joint Service Commendation Medal, Army Commendation Medal, Joint Service Achievement Medal, and Army Achievement Medal. As a Civilian, he received the Meritorious Civilian Service Medal, Superior Civilian Service Medal, Joint Civilian Service Commendation Award, Commander's Award for Civilian Service, and Armed Forces Civilian Service Medal.

Doctrine Corner

Multi-Domain Operations

Editor's Note: This article is an excerpt from Draft Publication FM 2-0,* Intelligence. *This publication represents a significant update to Army intelligence doctrine, as it addresses the fundamentals and tactics associated with intelligence during large-scale combat operations.

The interrelationship of the air, land, maritime, space, cyberspace, the information environment, and the electromagnetic spectrum (EMS) requires cross-domain situational understanding of the operational environment. Commanders and staffs must understand friendly and enemy capabilities and vulnerabilities that reside in each domain. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for the best effects. Since many capabilities are not organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations. Intelligence plays an important role in situational understanding across all domains.

The Army conducts operations across all domains and the information environment. All Army operations are multi-domain operations. A multi-domain approach to operations is neither new to the Army nor to national to tactical intelligence. Rapid and continued advances in technologies and the military application of new technologies to the space domain, the EMS, and the information environment (particularly cyberspace) require special considerations in intelligence, planning, and converging effects from across all domains.

Army operations and battles will invariably involve challenges across multiple domains. Examples of Army multi-domain operations and activities include airborne and air assault operations, air and missile defense, fires, aviation, cyberspace electromagnetic activities (CEMA), information operations, space operations, military deception, and information collection. Key considerations for operating in multiple domains include—

- Mission Command.
- Protection.
- Reconnaissance in depth.
- Sustainment.
- Mobility.
- Information operations.
- Cross-domain fires.
- CEMA.
- Tempo and convergence of effects.

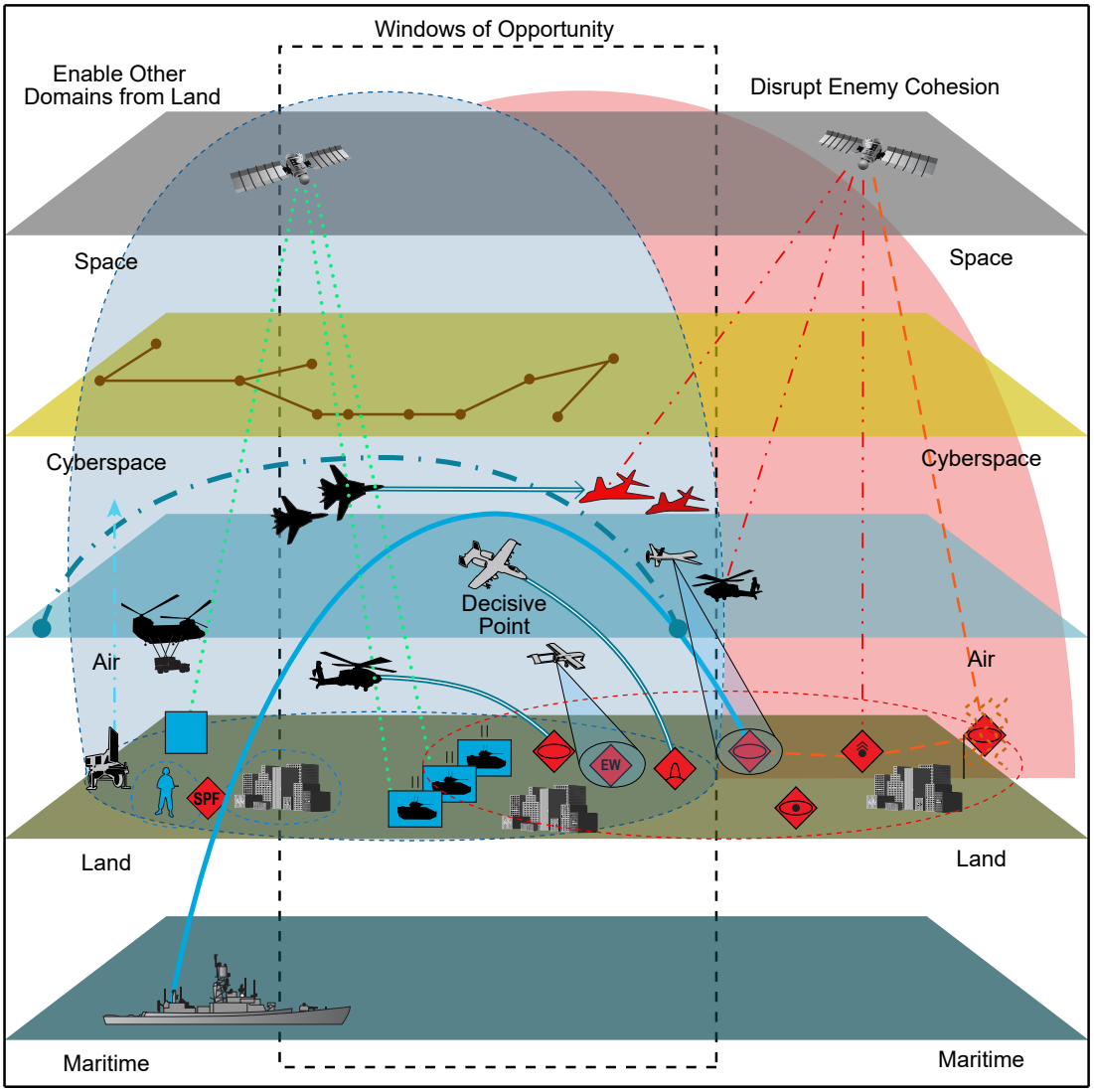
Army forces may be required to conduct operations across multiple domains to gain freedom of action for other members of the joint force. This is similar to other members of the joint force operating across multiple domains to assist in providing ground forces with a position of relative advantage. Examples of these operations include neutralizing enemy integrated air defenses, destroying long-range surface-to-surface fires systems, denying enemy access to an area of operations, disrupting enemy command and control, protecting friendly networks, conducting tactical deception, or disrupting an enemy's ability to conduct information warfare. All of these operations are enabled by precise and detailed intelligence on threat vulnerabilities.

Every echelon is affected by the multi-domain extended battlefield; each should consider time, geography, decision making, the EMS, and the other domains differently. However, not every echelon is able to effectively conduct operations across multiple domains. Brigade combat teams and lower echelons focused on fighting in the close area generally lack the time and ability to effectively plan and employ multi-domain capabilities other than those already under their control. These echelons focus on fundamental operational aspects such as mobility, lethality, and protection. The division is the first echelon able to effectively plan and coordinate for the employment of all multi-domain capabilities across the operational framework. Theater army and corps echelons have a broader perspective, better focus, and far more capabilities to orchestrate and converge multi-domain activities and operations in time and space. Through these activities and operations, intelligence is critical in assisting friendly forces to effectively identify and exploit windows of opportunity across the domains to create and exploit temporary windows of superiority.

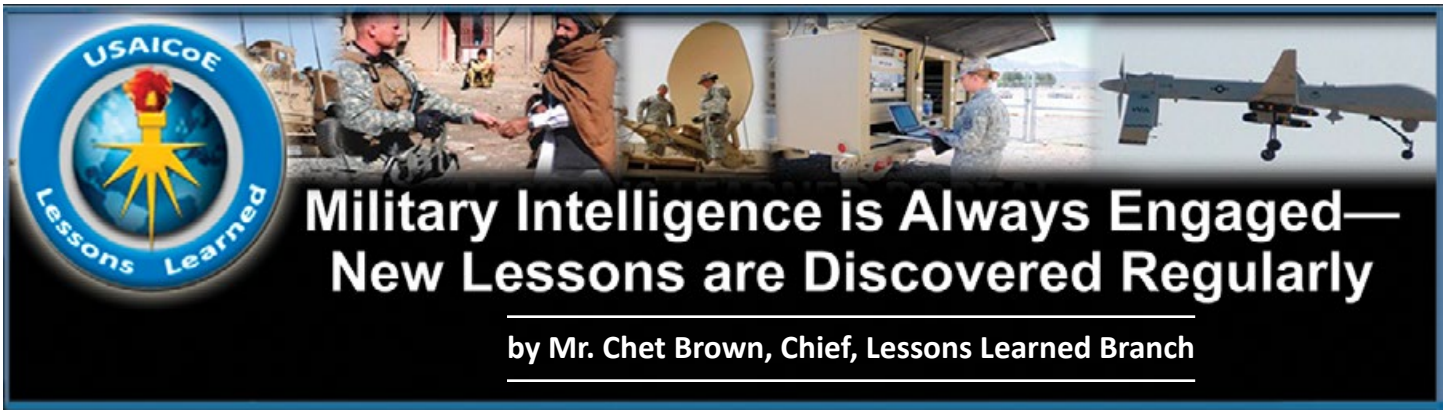
Although there are many possible techniques for conducting operations in and across all of the domains, multi-domain operation against a peer threat requires continuous situational understanding to see opportunities, seize

the initiative, and exploit enemy vulnerabilities or windows of friendly superiority. Seeing and understanding when and how the joint force will isolate portions of the operational environment in one or more domains to allow a portion of the joint force to establish a decisive point for the cross-domain convergence of capabilities must be supported by continuous intelligence operations across the domains. During large-scale combat operations against a peer threat, ground-force commanders may be required to conduct tactical activities, such as a deliberate attack, to shape the environment to gain a position of relative advantage for activities, such as joint fires, within the other domains. Once that position is achieved, operations would continue to increase the position of advantage in order to create a longer window of superiority to facilitate follow-on missions and operations across the domains. The figure below depicts a multi-domain operation in which friendly ground forces neutralized enemy integrated air defenses, thus creating a window of superiority for joint fires capabilities across multiple domains. They achieved this through aggressive information collection and focused intelligence analysis.

During intelligence preparation of the battlefield (IPB), each staff element provides input in order to provide a holistic view of the operational environment. Subsequently, the IPB effort aids in identifying domain windows of opportunity to exploit threat vulnerabilities. For example, the air defense artillery staff element's input to IPB about enemy integrated air defense system capabilities and vulnerabilities may present the friendly commander with recommended timeframes and locations to conduct suppression of enemy air defense or deep strike. Additionally, the gaps identified during mission analysis and IPB will drive information collection requirements. The results of information collection may also identify domain windows of opportunity. (See ATP 2-01.3 for more information on IPB.)



Windows of Opportunity in a Multi-Domain Operation



Military Intelligence is Always Engaged—New Lessons are Discovered Regularly

by Mr. Chet Brown, Chief, Lessons Learned Branch

The intelligence organizations, units, and capabilities of the U.S. Army Intelligence and Security Command (INSCOM) are always engaged—operating worldwide every day. With continuous operations comes a corresponding increase in the potential for INSCOM personnel to discover lessons and best practices.

Many of the lessons and best practices that INSCOM identifies receive validation from subject matter experts within the intelligence disciplines in which they were discovered. The first to benefit from newly discovered lessons and best practices are the personnel and leaders at INSCOM's regional, functional, training, and support elements. Unit and organizational leaders within INSCOM integrate pertinent lessons and best practices into operations, which sometimes result in revising existing tactics, techniques, and procedures. INSCOM leaders also highlight key lessons and best practices, as well as their associated operational impacts, through a variety of internal synchronization venues and information exchanges. The rapid dissemination of lessons and best practices within the command and its subordinate organizations contribute to immediate application (as appropriate) with a corresponding increase in performance.

INSCOM personnel exchange lessons and best practices with personnel at the U.S. Army Intelligence Center of Excellence (USAICoE) who work in the military intelligence (MI) proponent's capability development areas of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). These direct exchanges of validated lessons and best practices enable their rapid integration, and the identification of any issues that require solutions or mitigating measures. Lessons learned by INSCOM personnel, who are involved in emerging and leading-edge technologies, inform current DOTMLPF development and contribute to efforts toward building the Army of the future.

As INSCOM and USAICoE personnel work together to effect positive changes in the DOTMLPF capability areas, so too do the personnel involved in the Army's lessons learned (LL) enterprise at INSCOM and USAICoE. The formal exchange of lessons and best practices occurs between personnel within the INSCOM G-37 Training and Exercise element, and the USAICoE Directorate of Training LL Branch. LL personnel at these two organizations maintain regular contact in order to provide situational awareness of lessons and best practices as they are discovered or validated. Each LL organization serves as the advocate for continued validation and integration in their respective commands.

The majority of lessons and best practices information that INSCOM provides to USAICoE is contained in INSCOM unit after action report (AAR) documents and briefing products. In return, INSCOM receives USAICoE LL collection reports, lessons and best practices-based information products, and information presented in the monthly MI LL Forum. Additional exchanges of lessons and best practices result from recurring collaboration, which often begins with INSCOM identifying opportunities for USAICoE to observe INSCOM units and personnel in the operational environment. Observing operations and exercises inherently leads to collecting lessons and best practices that satisfy the specified LL information collection requirements assigned by the USAICoE commanding general to the LL Branch.

Reporting lessons and best practices to satisfy the commanding general's LL information collection requirements is the primary purpose of any LL collection mission. The secondary purpose is to identify lessons and best practices that impact, or may impact, the DOTMLPF or intelligence warfighting function performance. Each USAICoE LL collection mission conducted in partnership with INSCOM has been successful in identifying lessons and best practices information of value to the intelligence community. Two of these missions resulted in identifying key issues affecting the Army. As this *Military Intelligence Professional Bulletin* issue goes to press, INSCOM and USAICoE are finalizing the coordination of two separate LL collection visits to operational INSCOM units. The limiting factor of providing LL

coverage is the availability of resources to perform the mission. Selecting which INSCOM capability, unit, or event to observe is often determined by a cost-benefit analysis that evaluates the probability of identifying pertinent lessons and best practices with the impact on available resources.

Sometimes we are unable to attend INSCOM operations that provide opportunities to learn. When we are not able to observe operations ourselves, we rely on a unit's AAR to identify lessons and best practices suitable for inclusion in the Army Lessons Learned Program (ALLP), in accordance with AR 11-33. INSCOM, as a direct reporting unit (DRU), complies with the specified task in AR 11-33 to each DRU to "enable the ALLP. . .by collecting lessons and best practices before, during, and following unit deployments."[1] AR 11-33 continues its instruction by identifying the Joint Lessons Learned Information System (JLLIS) as the Army portal through which lessons and best practices undergo validation, integration, and assessment. Access to the JLLIS allows us to review information the unit identified as a lesson or best practice. When INSCOM posts an AAR to the JLLIS that has information with the potential to address an LL information collection priority, the USAICoE LL Branch will attempt to define the full context in which the lesson or best practice originated. USAICoE LL personnel first enlist the assistance of the INSCOM Training and Doctrine Support (ITRADS) detachment colocated with USAICoE at Fort Huachuca, Arizona. ITRADS personnel are often able to provide the mission or operational variables at the time a specific lesson or best practice was observed or identified. ITRADS is also able to provide further assistance in the rare instances in which additional research or contact with specific INSCOM personnel is required.

The strength of the LL partnership between INSCOM and USAICoE is dependent upon effective communication, collaboration, and coordination. These attributes transform into techniques employed by the LL community in order to learn as much as possible from INSCOM personnel while not distracting them away from, or disrupting, intelligence operations. Just as MI is always engaged, so too are those who seek to learn from the experiences of MI Soldiers and leaders.

Endnote

1. Department of the Army, Army Regulation 11-33, *Army Lessons Learned Program* (Washington, DC: U.S. Government Publishing Office, 14 June 2017), 2.

by Ms. Angela Aube

Introduction

The Army is building Security Force Assistance Brigades (SFABs) with highly qualified Soldiers who will serve as combat advisors, working closely with our partner nations, to meet security needs of the assigned theater. These SFABs are "purposefully built to help combatant commanders accomplish theater security objectives by training, advising, assisting, accompanying and enabling allied and partnered indigenous security forces."[1]

In August 2017, the 316th Cavalry Brigade and the Maneuver Center of Excellence at Fort Benning, Georgia, stood up the Military Advisor Training Academy (MATA) to prepare SFAB Soldiers to deploy as combat advisors. In addition to focusing on the characteristics, roles, and duties of an advisor, a critical component of the curriculum is training Soldiers to develop cultural competency skills to help accomplish their mission objectives.

Communicate and Build Trust

Advisors must be able to build rapport with their counterparts by establishing trust and relationships that allow them to function more effectively in their role. In order to build rapport, communication skills are vital. In an age of dwindling face-to-face interactions, effective communication has become an increasingly endangered skill. And those who cannot communicate will find themselves hard-pressed to build a productive professional relationship with others. Of course, job competence is important, but even the most competent person can experience difficulty connecting with counterparts if they do not know how to communicate and build trust. Most people have witnessed supervisors or peers who, while fully capable of doing their job, have difficulty in creating robust relationships with their subordinates and peers. This inability to connect can be a costly detriment to a career. In particular, advisors have limited positional power and must rely on their communication and engagement skills to influence their counterparts in a meaningful way. Advisors must be able to connect and engage every day on a one-to-one level.

In partner support to the MATA program, the U.S. Army Training and Doctrine Command Culture Center (TCC) created curricula and provided culture-focused instruction to MATA students. From August to October 2017, the TCC was on the ground at Fort Benning to support this important effort by providing culturally focused lessons designed to bolster critical advisor skills. During this time, the MATA Soldiers focused on not only understanding what culture is and what it means to them but also on communication, rapport building, and influence processes. A lot of culture training focuses on the specifics within a region (e.g., Afghanistan or Iraq), the cultural dos and don'ts, how to shake hands, and how to greet others. While this is an important component of culture training, it is not the only component.

Gaining a fundamental understanding of the communication process allows the advisor to explore all the factors that impede communication beyond not speaking the same language and to develop plans for how to mitigate those impediments. Breaking down the process of building rapport into the human factors that cause others to like or trust us helps advisors to engage in a more thoughtful process of interaction with their counterparts. Understanding the

principles of influence enables advisors to develop specific strategies to better persuade their counterpart and move him or her toward the advisor's objectives.

As Soldiers and leaders, we communicate, build (or break) relationships, and influence those around us every day. The question is whether or not those efforts are successful and whether they move us toward, or away from, our objectives. Having this baseline knowledge allows us to take a critical look at reading the "human map," so to speak. We then build upon this by providing opportunities to learn the specifics of the region or culture on which we are focused. This regional overlay of the human map provides us details that we can then use to shape our planning process and our actual engagements.

Key Leader Engagement Process and Negotiation Techniques

At the MATA, we didn't just stop at the understanding or "information" portion of these topics. In addition to the baseline knowledge and skillset described above, we also examined the key leader engagement process and negotiation techniques, because advisors typically find themselves in these situations. We focused on providing functional how-tos for each topic and on providing opportunities to practice these skills. After all, if a Soldier can't use the culture information and skills, then it is of limited utility. The goal of culture education and training in this context isn't to make a cultural anthropologist; it is to build everyday skills that allow advisors to accomplish their mission as efficiently and effectively as possible and come home safely. For this, we need advisors who are strong thinkers, planners, and doers.

To support this goal, MATA students conducted a series of key leader engagements and negotiation role-playing during which they were asked not only to use an interpreter but also to put all of their cross-cultural engagement skills into practice. For example, were they able to—

- ✦ Master their body language?
- ✦ Shape their communication approach to better resonate with their counterpart?
- ✦ Convey that they were trustworthy through body language, words, and actions?
- ✦ Notice nonverbal communication cues to better read their counterpart?
- ✦ Use what they knew about their counterpart to better shape their plans and approach?
- ✦ Maintain patience when frustrated?

The ability to do these things well greatly enhances success in engagements of any kind.

The Football Analogy

From the outside, it may seem simple to conduct a leader engagement or negotiation, especially if we spend our time just thinking and planning. However, mastery of these skills is a lifelong effort and must also be demonstrated in actions.

Compare this to football. Start with your understanding of the fundamentals—the player positions, the layout of the field, and the scoring. Then study the plays that the coach designs and know them by heart. Study your opponent and see what they have done in the past. Also, study the preferred plays and who you should focus on blocking. All of this occurs off the field. This is your thinking and planning. But, come game day, put on the helmet and stand on the field: that's when it gets real. If you're at the right spot on the field at the right time but can't catch the football, your days as a wide receiver are certainly numbered.

Conclusion

The ability to execute (i.e., to DO), in addition to thinking and planning, is a necessary component of success. In the case of culture and the advisor, the practice of people skills in a variety of contexts is critical to building a functional level of cultural competence that benefits not only advisors but also Soldiers and leaders of all kinds.

The culture education and training provided at the MATA was the first step in this lifelong process. Advisors will certainly be put to the test as they deploy and further implement their knowledge and abilities, but having these culture skills in their repertoire will help them to achieve the goals of the U.S. Army and the advisor mission.

Endnote

1. John May, "Military Advisor Training Academy Prepares 1st SFAB as Combat Advisors," *U.S. Army Worldwide News,* November 27, 2017, https://www.army.mil/article/197404/military_advisor_training_academy_prepares_1st_sfab_as_combat_advisors.

Ms. Angela Aube is the team lead for cross-cultural competency/professional military education and the lead for training development at the U.S. Army Training and Doctrine Command Culture Center (TCC). In support of the Security Force Assistance Brigades program and the Military Advisor Training Academy (MATA), Ms. Aube led the team responsible for designing, developing, and instructing the culture block for the MATA and served as a primary instructor during TCC's support to the MATA in 2017. Before joining the TCC in 2004, Ms. Aube was an Arabic language cryptologic linguist.

Moments in MI History

The Belfort Ruse, August-September 1918

by Lori S. Tagg, USAICoE Command Historian

My dear General Pershing: I hear from everywhere, and especially from the armies and civil authorities of the east, that, in their generous enthusiasm on account of the prospect of a great success over the enemy, numerous American officers and soldiers have talked in a public way of the projects of the High Command in the Woëvre….It is impossible that the enemy should not be forewarned.

–General Henri Philippe Pétain, Commander-in-Chief, French Army

The date was 19 August 1918. After 15 months of preparation, planning, and training, the American Expeditionary Forces (AEF) were finally ready to launch their first large-scale military operation of World War I. The early September offensive would pit the U.S. First Army and more than 100,000 French troops against 11 German divisions at the St. Mihiel salient in northeastern France. The French were worried, and rightly so. Inexperienced American soldiers and officers, who certainly should have known better, were egregiously violating operational security.

General John J. Pershing, commander of the AEF, was no stranger to the importance of negative intelligence—keeping information from the enemy. Chagrined that his own troops were exhibiting such carelessness, Pershing replied to Pétain on 22 August: "the importance of the considerations which you have set forth relative to the necessity for secrecy in all operations had not escaped me. I keenly regret that indiscretions may have been committed, and I consider, with you, that we must attempt to deceive the enemy upon the actual directions [of] the attack."

Pershing directed the Information Division within his G-2 section to devise and execute, in very short order, a plan to mislead the Germans as to the true location of the American attack. The chief of the division was CPT (later COL) Arthur L. Conger, Jr., a Harvard graduate, instructor at Fort Leavenworth, and German linguist familiar with the German Army. Conger, however, was a reluctant intelligence officer. Reportedly difficult to work with, he had been passed over by other AEF staff officers and ended up "stuck" in the G-2. After the war, Conger told a group of new intelligence officers, "I was one of those people in Intelligence who felt that they were in the wrong place all during the war and wanted very much to be someplace else." Despite his wishes, Conger was second in command to MAJ (later MG) Dennis Nolan, the AEF G-2.

Although unhappy about the assignment, Conger attacked it with vigor. To prevent further security breaches, he limited knowledge of the deception plan to Pershing, his chief of staff, and the AEF G-3. Conger had the G-3 issue a confidential order to the VI Corps commander to establish a headquarters in Belfort, France, a small town near the German border, and to expect seven divisions for an attack on the city of Mulhouse through the Belfort Gap, 125 miles southeast of St. Mihiel. Staff officers from the corps and each of the named divisions converged on Belfort to arrange for lodging and administrative space to support this large force. Conger also traveled to Belfort, a hotbed of German sympathizers and spies, where he dropped hints to local inhabitants and conveniently left "confidential" papers in plain sight. He arranged for reconnaissance flights over enemy lines, sent borrowed French tanks to drive around open fields, and dispatched agents to scout rail lines, roads, and hospital facilities. Signal units set up large antennas and proceeded to dispatch a flurry of messages.

Throughout the execution of his deception plan, Conger expressed pessimism on its chances for success, doubting "that the enemy takes this reconnaissance very seriously; ...[he won't] be deceived by a mere 'paperwork' demonstration or reconnaissance of officers, unaccompanied by actual preparations of guns, munitions, materiel, and subsistence." And he was right. German intelligence officers doubted the legitimacy of the information they received out of Belfort but felt it was too important to ignore completely. After all, Belfort might very well have been the true site of the upcoming attack and the American preparations at St. Mihiel the ruse.

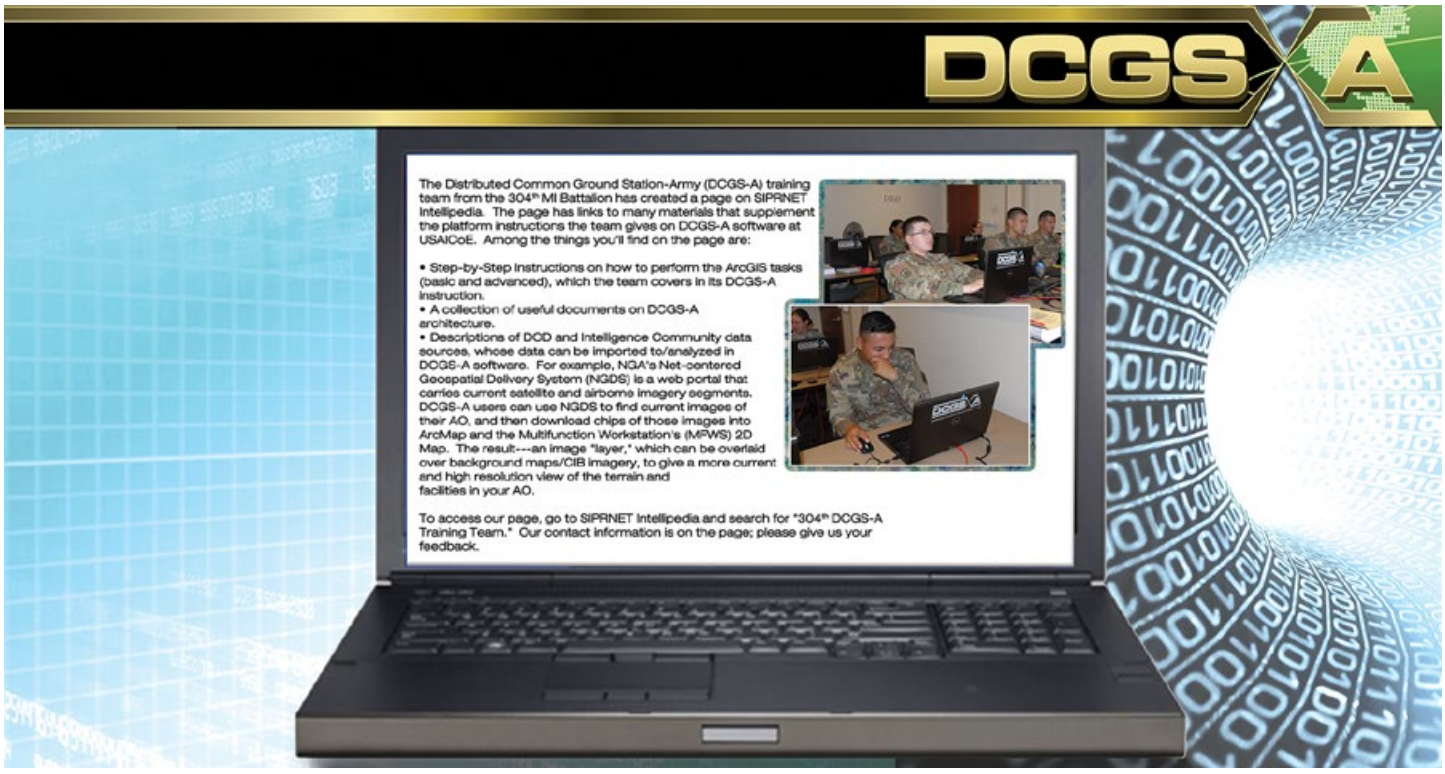
Ultimately, the Belfort Ruse had little impact on the offensive at St. Mihiel; however, it did sow enough confusion

and concern within the German forces for them to divert resources, time, and effort that could have been more effective elsewhere. Pershing believed the ruse successful enough to request additional deception operations to keep the enemy uncertain and distracted.

After the war, Conger stated, "Of course, it is as old as the history of war for false information to be given to the enemy." Indeed, examples, both successful and not, can be found throughout U.S. Army history. Used to counteract a serious security leak or to mislead the enemy, deception operations can help a commander preserve that all-important principle of war—security.

Photo courtesy of the Library of Congress

The U.S. First Army moves forward to its first offensive of World War I at the St. Mihiel salient, September 1918.

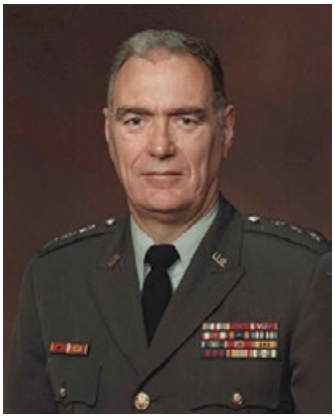


VIGILANCE ALWAYS

A Tribute to Military Intelligence Legend Lieutenant General James Arthur Williams

by COL Nichoel E. Brooks and CPT Jessica A. Tarsa

Lieutenant General (Retired) James Williams passed away on 31 October 2017 following a remarkable life defined by a passion for learning, humbling generosity, and distinguished service to the United States Military Intelligence Corps.



LTG Williams commenced his life in uniform at the U.S. Military Academy at West Point in 1950. He commissioned four years later as an air defense artillery officer with a bachelor of science in engineering. In 1957, he was detailed to the Counter Intelligence Corps, beginning his career as an intelligence professional.

Over the next 20 years, he accrued a wealth of experience overseas and with the State Department. He served with the 470th and 471st Counter Intelligence Corps Detachments in the Panama Canal Zone and Puerto Rico, as an assistant Army attaché in Venezuela, and as Commander of the 1st Military Intelligence (MI) Battalion (Provisional), 525th MI Group, in Vietnam. Following his graduation from the National War College in 1971, he became Director of Political/Military Affairs, Bureau of Inter-American Affairs, at the State Department. In 1974, he served briefly as the Chief, Counterintelligence and Collection Division, for the Assistant Chief of Staff, Intelligence, before taking command of the 650th MI Group at the Supreme Headquarters Allied Powers Europe in Belgium.

In 1976, LTG Williams returned to the United States to serve at the Defense Intelligence Agency (DIA) as the Chief, Missile Forces, Strategic Arms Limitation Branch, Soviet/Warsaw Pact Division, then later as the Deputy Director for Estimates. He pinned his first star in 1980 as Deputy Chief of Staff, Intelligence, U.S. Army, Europe. He would earn two more stars as DIA's seventh director from 1981 to 1985.

During his tenure as Director of DIA, LTG Williams refocused its efforts on how to best support the warfighter—creating the systems and structure required to provision real-time intelligence from the strategic echelon to the tactical edge. Guided by his vision, DIA designed and implemented the National Military Intelligence Support Team and the Military Intelligence Integrated Data System, which provided commanders down to the corps/division level access to standardized national to tactical intelligence. He also established a crisis management center, facilitating all-source support to the National Military Intelligence Center and combatant commands. Retired MG Barbara Fast recalls LTG Williams as, "among the first leaders to marry technology with human analytic brainpower…he was able to combine nationally derived intelligence with regional/operational intelligence. This distributed intelligence approach…now is part of our military intelligence doctrine and reaches all the way to the tactical edge."

LTG Williams is also remembered for his remarkable ability to adapt and remain current. These traits enabled him to conceptualize technological solutions to long-standing and emerging problem sets, resulting in many firsts in our intelligence community: the first formal use of imagery from civilian satellites; the first computerized threat methodologies for the Department of Defense; the first threat validation system for the defense acquisition life cycle; and the initiation of widespread usage of open-source foreign scientific and technical information to aid analysis. His leadership also steered DIA to better confront Cold War challenges, escalating tensions in Nicaragua, and a significant increase in terrorist activity. He helped create the *Soviet Military Power* series to inform the American public about the Soviet threat. To better combat foreign espionage operations, he oversaw a major expansion in the Agency's Counterintelligence Division. The first all-source fusion cell specifically for terrorism analysis was established, as was the Central America Joint Intelligence Team to help U.S. Southern Command monitor the growing insurgency in Central America. In 1985, LTG Williams concluded his 31 years of formal government service. Reflecting on his tenure at DIA, he said, "I have altered the Agency's basic philosophy of whom it exists to serve."

After retirement, he continued his selfless service as a senior consultant for the Arms Control and Disarmament Agency; member of the Board of Visitors of the Joint Military Intelligence College; senior fellow at the Joint Forces Staff College; and Chairman of the National Military Intelligence Association. Despite his impressive accomplishments, retired MG Fast considers LTG Williams's greatest legacy "the mentorship and leadership that he provided to generations of military and civilian personnel. He was always the teacher, the coach, and the confidant for both professional and personal matters. He was humble, but forceful in his love for our Nation, for our Intelligence Corps, and our people. And, we will miss him." LTG Williams lives on in the legions of intelligence officers inspired by his grace, relentless curiosity, and humility.

LTG Williams's awards and decorations included the Defense Superior Service Medal, Legion of Merit (1 Oak Leaf Cluster), Bronze Star (V Device and 1 Oak Leaf Cluster), Meritorious Service Medal (2 Oak Leaf Clusters), Air Medals, Joint Service Commendation Medal, and Army Commendation Medal. He was inducted into the MI Hall of Fame in 1987 and served as the first Honorary Colonel of the MI Corps from 1987 to 1990. He continued to serve as a Distinguished Member of the Corps until his death in October 2017.

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

INSCOM

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

PIN: 203547-000