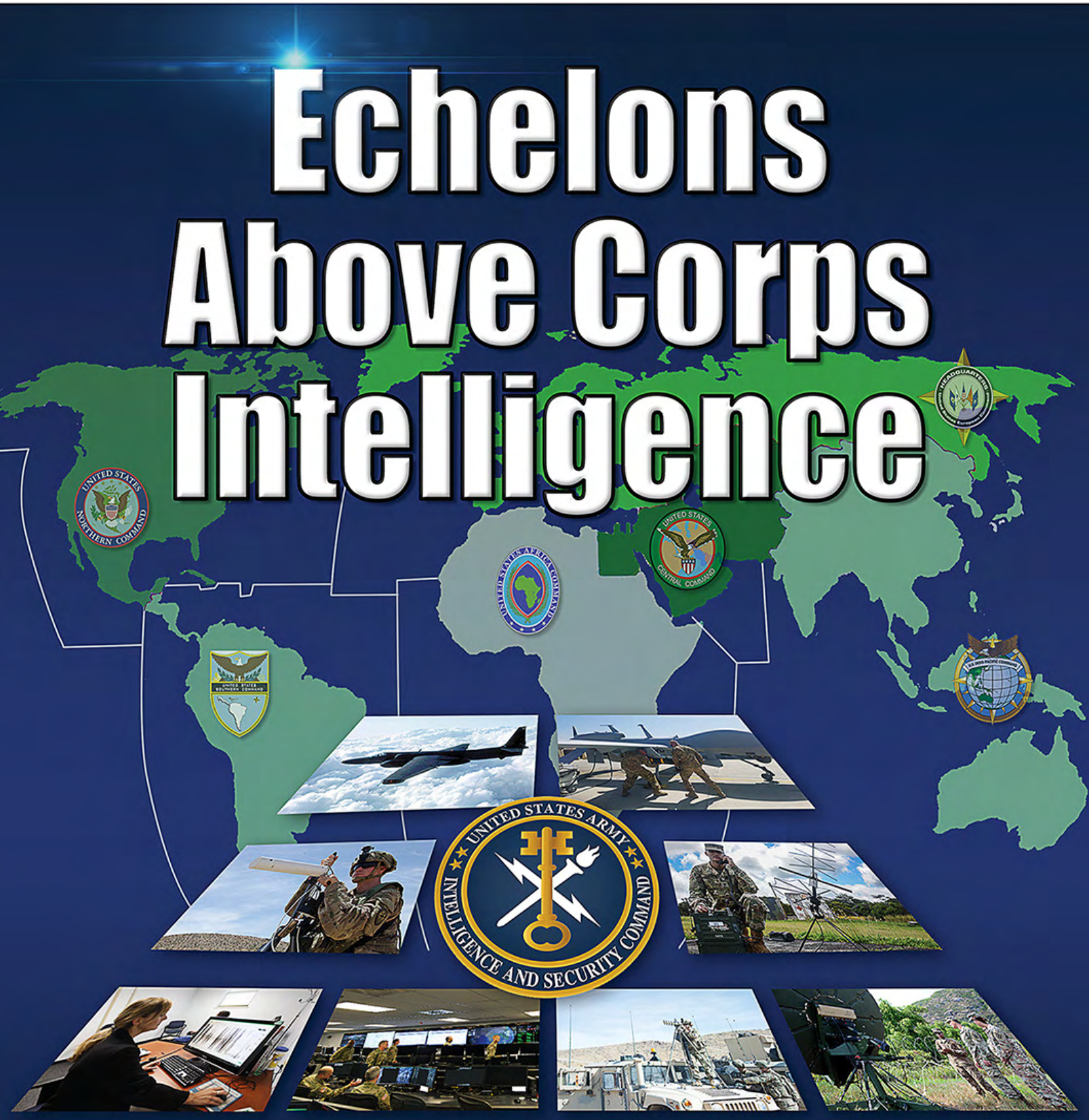
MI Professional Bulletin
January–March 2020
PB 34-20-1

Echelons Above Corps Intelligence



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

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

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

Our mailing address: MIPB (ATZS-DST-B), Dir. of Doctrine and Intel Sys Trng, USAICoE, 550 Cibeque St., Fort Huachuca, AZ 85613-7017

Commanding General
MG Laura A. Potter

Chief of Staff
COL Peter J. Don

Chief Warrant Officer, MI Corps
CW5 David J. Bassili

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
Emma R. Morris

Military Staff
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:

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

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1931007

From the Editor

The following themes and deadlines are established:

July–September 2020, *Collection Management*. This issue will focus on how the intelligence staff executes the tasks of collection management in support of information collection. Deadline for article submission is 3 April 2020.

October–December 2020, *Peer and Emerging Threats*. This issue will focus on developing an understanding of current and potential threats facing U.S. forces. Deadline for article submission is 1 July 2020.

January–March 2021, *Our Intelligence Disciplines.* This issue will focus on new, critical, and refocused aspects of all the intelligence disciplines and complementary intelligence capabilities. Deadline for article submission is 30 September 2020.

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

If you would like to receive a notification email when new MIPB issues become available on Intelligence Knowledge Network and/or when new intelligence doctrine is published, send an email to usarmy.huachuca.icoe.mbx.mipb@mail.mil or usarmy.huachuca.icoe.mbx.doctrine@mail.mil requesting to be added to USAICoE Doctrine Division's announcement distribution list.

For us to be a successful professional bulletin, we depend on you, the reader. Please call or email me with any questions regarding article submissions or any other aspects of MIPB. We welcome your input and suggestions.

Tracey A. Remus
Editor

MI Professional Bulletin

January–March 2020
PB 34-20-1
Volume 46 Number 1

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.

We would like to sincerely thank the U.S. Army Intelligence and Security Command (INSCOM) for allowing us to leverage their expertise as the "stakeholder" for this issue. We are especially grateful to COL Eric Heist, Director, Enterprise Task Force, and Mr. MyRon Young, Chief, INSCOM Public Affairs Office.

FEATURES

DEPARTMENTS

Always Out Front

by Major General Laura A. Potter
Commanding General
U.S. Army Intelligence Center of Excellence

In my first few months of command, I have met with every organization within the U.S. Army Intelligence Center of Excellence (USAICoE) and with several of the tenants on Fort Huachuca. I am extremely impressed with what our team is accomplishing in order to evolve military intelligence to meet the Army's operational and force modernization demands in support of multi-domain operations, and to ensure that our Soldiers are receiving the best training and education. Intelligence drives operations, and what we accomplish at USAICoE directly corresponds to the quality of intelligence we provide commanders at all echelons.

In last quarter's *Military Intelligence Professional Bulletin* (MIPB) issue, we discussed the National Defense Strategy (NDS) and how USAICoE is changing its course curriculum and programs of instruction to meet the modernization needs and priorities listed in the NDS. This quarter's theme is intelligence at echelons above corps (EAC). One of those lines of effort listed in the NDS is "strengthening alliances as we attract new partners."[1] This priority is critical, especially when setting the theater at the EAC level. ADP 4-0, *Sustainment,* defines setting the theater as "a continuous shaping activity [that] is conducted as part of steady-state posture and for contingency or crisis response operations. Setting the theater describes the broad range of actions conducted to establish the conditions in an operational area for the execution of strategic plans." [2] In accordance with this doctrinal definition, military intelligence plays a key role in setting and assessing the conditions and requirements for Army, joint, and combined campaigns and operations in theater. The combatant commands, which are responsible for warning intelligence and 24-hour-a-day situational awareness, are the largest consumers of operational and strategic theater-level intelligence that the Service components and the Service intelligence centers produce. The rapid changes in the operating environment, including the increasingly global activity of our peer competitors, increase the demands and complexity of our EAC intelligence mission and how we support the combatant commands, the U.S. intelligence community, and our allies and partners.

In competition and conflict, we must work closely with our joint, interagency, and multinational partners to see ourselves and see the enemy across all domains in our theater operational environment. Across the intelligence community problem sets, there are information and capability gaps that our foreign partners can bridge. Our allies and partners provide us with analysis, expertise, and capacity necessary to characterize the current environment and prepare to compete and prevail in conflict. To benefit from this invaluable resource, setting the theater must include—

- The right coalition architecture to share our data and ingest the data from our allies and partners.
- An approach that embraces their contributions.
- A collection strategy that includes "REL" requirements and demands writing for release.
- Adequate foreign disclosure policies.
- A knowledge management process that proactively shares releasable intelligence.

Once we share our different perspectives and integrate capabilities, we can establish a common sight picture necessary to set the theater and prepare for a peer fight and large-scale ground combat operations.

At EAC, it is our military intelligence brigades-theater, our strategic intelligence units, our intelligence professionals in Special Operations, and our Service intelligence center—the National Ground Intelligence Center—that contribute to this common intelligence picture across multiple domains. In this edition of MIPB, the authors of

"Building the Base: Using the Army's Intelligence Program of Analysis to Drive Foundational Intelligence" explain foundational intelligence—how we established it, how we define it, and how it can affect our missions. They also talk about how we analyze our lessons learned to form and evolve our intelligence to meet the needs of the mission and ensure the combatant commanders have a complete and vivid picture of the adversary. In order to maintain this foundational intelligence and constantly improve it, we rely on our Service intelligence centers. At the EAC level, our Service intelligence centers collect information to provide a complete sight picture of our adversaries so that our commands are properly equipped and possess the right capabilities and understanding to make informed decisions during a peer fight.

The recently signed Army Intelligence Plan lays out the Army intelligence enterprise priorities as people, readiness, modernization, and reform. As the intelligence community conducts the planning and preparation, we build readiness for our combatant commands to execute their mission. As the operational environment changes, the intelligence community evolves to modernize and reform our equipment and force to be prepared for the expanding battlefield.

Endnotes

1. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America,* n.d., 5, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. Department of the Army, Army Doctrine Publication 4-0, *Sustainment* (Washington, DC: U.S. Government Publishing Office, 31 July 2019), 2-4.

Always Out Front!

Ladies and Gentlemen,

It is my distinct pleasure to announce the selection of CW5 Aaron Anderson to serve as the eighth Chief Warrant Officer of the Military Intelligence Corps. Aaron is a well-respected intelligence professional who brings the right energy, emotional intelligence, and experience necessary to continue shaping and preparing our warrant officers and the greater MI Corps to win in large-scale ground combat operations in a multi-domain environment. Our warrant officers are the technical leaders of our branch and serve as trusted advisors to our commanders and senior intelligence officers around the globe. I have full confidence in Aaron's abilities to execute these responsibilities flawlessly.

We will welcome CW5 Anderson and farewell CW5 Bassili during a Change of Responsibility/Retirement Ceremony in summer 2020.

Please help me in congratulating CW5 Aaron Anderson on his selection.

Always Out Front!

Laura A. Potter
Major General
Commanding General
U.S. Army Intelligence Center of Excellence
and Fort Huachuca

CSM Forum

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

Talent management is a term used by senior leaders all around the Army. "Get the right person to the right place at the right time" is a good bumper sticker, but it is easier to talk about than to actually do. The good news is there is a realization that we must do something that goes beyond the simple development of people and assignment management. Many of us have done some semblance of talent management for years. Although talent management is a moderately common occurrence, what "right" looks like in one career management field, or even unit, may not be the same in another field, and is not always a deliberate and well-thought-out process.

Although several variables deal with talent management, leadership is the key to success. The Army expects leaders to be agile and adaptive, causing us to continually look at how and why we are doing things to remain relevant. Today's society, Army, and Soldiers present some variables we need to take into account when considering talent management. Soldiers from previous generations could be told to do something, and they moved out smartly without requiring a great deal of explanation. Soldiers of the present generation want to feel valued and see value in what they do. Key complaints by Soldiers to the Inspector General are misutilization and poor leadership. Misutilization is inherently contrary to talent management but in reality takes on different meanings depending on whom you are speaking to about this topic. What seems like misutilization to a Soldier may not be how senior leaders see things. Taskings are part of Army life, and some duties are required and even developmental when managed properly. Leaders need to take time to manage talent to maximize the success of mission, Soldiers, and families. Actually, talent management is a line of effort responsibility for noncommissioned officers (NCOs) as prescribed in NCO Strategy 2020.

In talent management's simplest form, leaders should consider the commander's requirements and priorities to determine where the most impact and risk lie and focus the most talented people in those areas. Task, time, and priority management can be just as important here as talent management. Those who are unable to accomplish required missions need to be retrained and counseled appropriately after determining the cause. It is easy to forget that each person has other duties they are responsible for, and not moving responsibilities around appropriately can cause undue stress and burnout for our best people. Even additional duties should be taken into account. Do not limit what you consider for managing talent.

Several elements go into talent management. Capability, career goals, and needs of the Army are some of the key aspects leaders must consider. Leaders must communicate with their Soldiers to ensure Soldiers know the pros and cons to their career based on their decisions. Leaders can see if a Soldier needs to continue building on basic skills before looking for additional responsibilities or stove piping their skillsets and potentially halting their progression. Individual development plans are a great tool to assist with talent management and provide a perfect opportunity for holistic mentoring when considering professional and personal goals and ways to get there.

There is one thing that is often not understood in Career Management Field 35—senior NCOs, in particular Command Sergeant Major/Sergeant Major, must simultaneously understand intelligence and be good leaders. This must emcompass the full scope of the Intelligence Warfighting Function and what every discipline brings to the fight. This takes time and experience, while putting away ego, to fill in gaps of knowledge and understanding. Far too often, senior NCOs decide they are not good at one

or the other and spend time focusing on what they view as their strength. First Sergeants need an understanding of how to oversee training for any intelligence discipline and be the senior advisor to the commander. Sergeants First Class must learn to manage missions, assess training needs, develop plans to fill mission gaps, and lead NCOs and Soldiers. All of this builds toward who will be the most talented individuals to serve in the most senior positions but requires leaders along the way to manage talent. The Office of the Chief of Military Intelligence is painstakingly rewriting the professional development models for each intelligence discipline, and the NCO Academy is organizing its training along these lines.

The Army has taken some key actions in this process by the development of the Talent Management Task Force, initiation of Assignment Interactive Module 2, and emplacement of the Marketplace, to name a few. All of these focus on officers gaining more control of managing their own careers through an assignment selection process that includes a potential agreement between an individual and unit leadership. There are no guarantees, and every valid position will be filled, but officers can attempt to match their wants with Army needs. There is a lot of discussion about this being available to the enlisted force after additional fielding.

Giving NCOs/Soldiers more control over their careers may assist with retention because they can try to obtain assignments with jobs at locations of their choice. This should increase the proficiency of individuals, as Soldiers who are more competitive for promotion will, in theory, be more lucrative for units to choose for jobs at their location. This may become unbelievably important, as today's recruits who fall under the new retirement plan will have more options throughout their career to leave the military. However, there are negatives if this process becomes available to the enlisted force, as each career management field will not work in the same way. Soldiers may choose to continue doing a specific job or remain at a location. Although stability works well for the mission and family, it may not assist the Soldier with career progression and may eliminate opportunities for other Soldiers. Serving in a mix of assignments at the U.S. Army Intelligence and Security Command and U.S. Army Forces Command and with Special Operations Forces builds diversity through experiences leading/working in different environments because the mission, even within the same military occupational specialty (MOS), is executed much differently at each location. Leaders will need to be engaged and look at each circumstance to determine the best way to mentor and develop their Soldiers.

Although talent management is done primarily at the unit level, Human Resources Command (HRC) must be part of the discussion. Manning guidance dictates assignment management, but branches conduct talent management to the maximum level possible to synchronize assignments to meet the larger Army mission. Determining Soldiers eligible for drill sergeant, recruiter, nominative assignments, and more ensures only qualified individuals go to certain jobs. HRC also performs assignment management to ensure we take care of families through the Exceptional Family Member, Married Army Couples, and Joint Domicile Programs when Soldiers move. We want to get the right person to the right place at the right time, but assignment availability and balancing the needs of the force at large are realities in actual talent management. At the end of the day, making full use of the available assets for talent management requires HRC and unit leaders to work together.

Another area for talent management is broadening assignments and obtaining additional skills. This is a great way for NCOs to separate themselves from their peers. Excellence while serving in operational assignments is what gets Soldiers promoted. Broadening assignments are a great way for NCOs to demonstrate they are able to operate at a high level in any environment and hone needed skills to progress in their careers. As an example, drill sergeant is an outstanding way to develop good leadership skills while planning, coordinating, and executing training in conjunction with an MOS committee. Another discriminator for Soldiers is obtaining additional skill identifiers (ASI). An ASI will not get a Soldier promoted, but what the Soldier does with that skill in support of the mission is the positive impact. Leaders need to deliberately assist individuals in making positive decisions so that they do not undercut their potential or put themselves in positions beyond their current capability.

There is still one more important issue to discuss on this topic—we need to train leaders how to manage talent. Spotting, assessing, and developing talent is not a skill everyone has. It is hard and has nothing to do with being friends. Many senior leaders say that everyone in their organization manages talent because they have ensured it is a priority. Too many times senior leaders believe this is such a simple concept. They think it is implied or someone else is doing it, but may not periodically check

whether it is being done. What is simple to some is not simple to all and requires a little inspect versus expect to take care of those top performers in every formation. Truthfully, every organization has people who do talent management well, while others do not do it for multiple reasons. In most instances, if talent management does not happen it is because individuals do not understand the how or why of taking the time to perform this important function. Although the focus for leader development is two levels down, senior leaders may need to go below two levels to ensure a deliberate process exists to manage time, tasks, and priorities and ensure we get the right people to the right place at the right time.

It will be interesting to see what opportunities will be available to enlisted Soldiers, whether managing one's own career or managing the talent of others. Leaders will need to be adaptive and engaged. The only way to ensure this happens is to have leaders at every level develop those below them and ensure talent is managed. It is good to see the Army looking at this important topic and ways to best take care of our number one asset —our people.

Always Out Front!

Another Perspective: EAC at the Tip of the Spear

The United States Army is currently in a serious competition with our peer threats—Russia, China, Iran, and North Korea. At the same time, we continue to support many unique operations across the world outside of that competition. While the Army often discusses the new focus on large-scale ground combat operations, we should not overlook the importance of the daily competition we conduct against our peer threats.

As stated in ADP 3-0, *Operations,* "The Army's primary mission is to organize, train, and equip its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas."[1] That mission starts well before the actual conduct of large-scale ground combat operations. In many ways, our successes and struggles during combat operations will be largely determined during the Army strategic roles of shape operational environments and prevent conflict. Intelligence is at the tip of the spear during competition, and intelligence support is often driven from the top by echelons above corps (EAC). Understanding the value of EAC planning, collection and processing, analysis, and production is important for all military intelligence Soldiers from the national level all the way down to the tactical level.

During the competition phase, the most critical intelligence capabilities and task of establishing the intelligence architecture reside within EAC. EAC intelligence activities build our foundational intelligence, support strategic and operational level planning, protect our force, improve the capabilities of our allies and partners, and help prepare the tactical force as the Army transitions to large-scale ground combat operations. EAC foundational intelligence is critical to so many aspects of Army operations. However, our peer threats continually attempt to conduct deception and hinder our collection efforts. We are literally "fighting for intelligence" even before we conduct combat operations.

To win tomorrow, the intelligence warfighting function must continue to innovate and evolve. EAC intelligence organizations are fully engaged in efforts to find solutions and drive change to solve complex intelligence problems. We must be prepared for the future challenges so that the Army can deter, fight, and win on any battlefield, against any foe, now and into the future.

Endnote

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

Technical Perspective

by Chief Warrant Officer 5 David J. Bassili
Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence

Hello again from the station of choice, home of the U.S. Army Intelligence Center of Excellence, Fort Huachuca, Arizona. As I continue into my final year as your Chief Warrant Officer of the Military Intelligence (MI) Corps, I cannot help but remind everyone what a fabulous duty station this truly is. Sure, it may come off as too small a town for some, but for what it lacks in size, it makes up for in beautiful sunrises and sunsets and near year-round cloudless skies. It also offers boundless professional opportunities to build the foundation of our corps through capability development, training, and education of the entire Army MI force. Now that the Army's Talent Alignment Program is in full swing, each of you has greater influence in determining your ability to join the team on America's western frontier.

Foundation building is apropos to the focus of this quarter's *Military Intelligence Professional Bulletin* (MIPB)—intelligence at echelons above corps (EAC). It also harkens back to the MIPB edition on large-scale combat operations (January–March 2019). Our EAC intelligence formations and staff positions at the operational and strategic echelon arguably serve as the greatest contributors in our Army's effort to shape and compete against peer and near-peer adversaries across the globe in support of the National Defense Strategy. This may entail generating intelligence requirements against theater or combatant commander contingency plans; conducting intelligence operations against those requirements; or building relationships, placement, and access with host-nation security organizations. Whatever the situation, many of the MI Corps core competencies against peer adversaries are executed in real operational environments 365 days a year. Much of this work is done outside the spotlight and with little fanfare from the unaware. For example, the all-source analyst who updates order of battle entries based on the latest information available, or the human intelligence collector who generates a report on the military load capability of bridges along route Y in country X, while building partner-nation capacity. As it relates to success in large-scale ground combat operations, the contributions of the all-source analyst and the human intelligence collector count as much as, if not more than, an armored brigade combat team battalion's qualification on Table XII or a division's ability to conduct a wet-gap crossing. These are but a few examples, but the foundational, pre-conflict, deep understanding of the threat and operational environment is paramount through all phases of conflict, and this responsibility is executed primarily at EAC within the intelligence warfighting function.

While much of the discussion of these activities focuses widely on the U.S. European Command and U.S. Indo-Pacific Command areas of responsibility (AORs), most of you already know that our peer and near-peer adversaries similarly enjoy our global reach. Although pertinent to focus future maneuver capacity and capability in these AORs, the intelligence warfighting function should focus on our adversaries' intent, capacity, and capability in all AORs. Although we currently no longer enjoy the force structure within our MI brigades-theater that we did when our main peer competitor was the Soviet Union, our technological capabilities are far superior. While it certainly feels like "doing more with less," our access to data and our ability to process and exploit that data today are far ahead of where we were in the 1980s and will only continue to improve. The real challenge is balancing the daily operational requirements of the theater and combatant command against unique AOR challenges not specifically focused on peer and near-peer adversaries, while attempting to synchronize limited theater resources against likely lower priority requirements.

I know that those who have served in the AORs of U.S. Northern Command, U.S. Southern Command, and U.S. Africa Command understand this challenge. Having personally endured these challenges in all three AORs, I can say that what they do offer is the ability to hone your influence, creativity, and leadership skills to find solutions, regardless if those efforts produce gainful insight during your assignment or after you depart. Shaping and competition for MI is the long fight—what we do today enables success in the future.

This issue's contributing authors share valuable insight and tactics, techniques, and procedures at EAC and potential solutions for the challenges you face in your current unit or organization. As always, thank you all for your dedicated service and continued sacrifice to the Nation.

Always Out Front!

Another Perspective: One Team, One Fight

FM 2-0, *Intelligence,* discusses intelligence support across the Army strategic roles and describes specific analytical and collection capabilities across echelons. Echelons above corps (EAC) intelligence organizations and units flex their capabilities to meet operational requirements from multiple theaters across the globe. Theater armies shape areas of responsibilities and improve operational-level positions of relative advantage. Theater army intelligence cells manage intelligence collection, production, dissemination, disclosure, and counterintelligence requirements. Military intelligence brigades-theater provide regionally focused collection and analysis to support theater army requirements and specific joint operations. EAC support is sometimes even downward reinforcing to the tactical level. In all cases, EAC databases, information feeds, and intelligence products support tactical operations down to the battalion level and sometimes even lower through the intelligence architecture. Through these capabilities, EAC organizations and units are the cornerstone for intelligence collection, production, and dissemination.

Although EAC is the cornerstone during competition, it is not the only ingredient to a successful intelligence warfighting function. It is the responsibility of military intelligence (MI) Soldiers at all echelons to support each other, collaborate, and work cohesively—one team, one fight. It is important for officers, warrant officers, and noncommissioned offers of every rank to develop Soldiers who can understand the role and value of each echelon. Within the intelligence warfighting function, it is important to know how to access and use all intelligence and intelligence capabilities. Understanding intelligence across echelons starts with understanding EAC intelligence.

The good news is that our MI force is ready to answer the many challenges of providing intelligence during the competition phase. The intelligence warfighting function comprises various disciplines, inherently competes across multiple domains and the information environment, and supports the entire continuum of operations. Today, MI Soldiers are excelling at EAC organizations and units across each specialty and intelligence discipline. MI Soldiers are true Army professionals, disciplined, and technically and tactically proficient. ADP 6-22, *Army Leadership and the Profession,* discusses how the trust within an organization enables influence up and down the chain of command. Trust is critical for intelligence. The entire intelligence warfighting function is built on trust. We must continue to trust each other and work as one team, collaborating with all echelons vertically and laterally.

ATP 2-19.1,
Echelons Above Corps Intelligence Organizations: Why the Update?

by Mr. Jerry Jones and Ms. Terri Lobdell

Introduction

ATP 2-19.1, *Echelons Above Corps Intelligence Organizations,* is the Army's doctrinal publication on the roles, responsibilities, and capability of intelligence organizations at echelons above corps (EAC). Last published in 2015, ATP 2-19.1 discusses doctrinal capabilities, organization, and structure for EAC intelligence organizations. While the U.S. Army Intelligence Center of Excellence (USAICoE) is the doctrinal proponent for ATP 2-19.1, the publication was not developed in isolation. Instead, USAICoE used a teaming approach with the U.S. Army Intelligence and Security Command (INSCOM). The INSCOM Training and Doctrine Support (ITRADS) Detachment, as INSCOM's representative, worked closely with the USAICoE Doctrine Division throughout the development process.

Recently, the Army updated its foundational doctrine to focus on large-scale ground combat operations against a peer threat. ADP 3-0, *Operations,* dated 31 July 2019, discusses the foundations, tenets, and doctrine of unified land operations. It is the core of Army doctrine, and it guides how Army forces contribute to unified action.[1] FM 3-0, *Operations,* dated 6 October 2017, introduces the Army strategic roles (shape, prevent, large-scale combat operations, and consolidate gains) and clearly emphasizes and focuses on conducting large-scale ground combat operations against a peer threat.[2] This paradigm shift, as well as updates to EAC intelligence capabilities, organizations, and structure, was a driving force behind the update to ATP 2-19.1. In order to maintain relevancy and consistency with validated Army doctrine, ATP 2-19.1 includes the following discussions—

- EAC intelligence organization support to the warfighter through the Army's strategic roles.
- EAC intelligence organization support to setting the theater.
- Updated verbiage to ensure consistency with operations doctrine and terminology.

Program Directive

The project to update ATP 2-19.1 began in August 2018 with the development of a program directive. A program directive is the official document that establishes a doctrine development requirement.[3] The program directive was staffed worldwide, and the validated comments concerning the content were incorporated into the document before command approval. The USAICoE Commanding General approved the program directive on 17 September 2018. The U.S. Army Combined Arms Doctrine Directorate validated it on 27 September 2018.

Initial Draft

ITRADS was the lead agent for developing the initial draft. In order to accomplish this task, ITRADS facilitated the update and revision of all sections of the publication. Each lead organization identified in ATP 2-19.1 was designated as the primary author for their chapters and/or sections. Their objectives were to—

- Understand the Army's major trends and intelligence challenges and their applicability with regard to updating ATP 2-19.1.
- Think about complex operational environments and the effect they have on EAC intelligence organizations.
- Acquire an understanding of how EAC intelligence organizations can address a complex operational environment across all relevant aspects within and across each domain.

Project Handoff

The ITRADS Detachment provided the initial draft to the USAICoE Doctrine Division at the end of September 2019. With such a solid draft to work with, Doctrine Division expects minimal development and editing will be required before staffing. We anticipate worldwide staffing will occur during the 2nd quarter of fiscal year 2020, with final publication mid to late summer 2020.

Endnotes

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

2. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), foreword. Change 1 was issued on 6 December 2017.

3. Department of the Army, Training and Doctrine Command (TRADOC) Regulation 25-36, *The TRADOC Doctrine Publication Program* (Fort Eustis, VA: TRADOC, 21 May 2014), 81.

Mr. Jerry Jones began his Army career in 1970 as an Armor officer in the 1st Armored Division and the 1st Cavalry Division at Fort Hood, TX. A veteran of Vietnam, Operation Desert Storm, and the Balkans conflict, he served at multiple echelons during his 30 years on active duty. He currently serves as the Director, U.S. Army Intelligence and Security Command Training and Doctrine Support Detachment.

Ms. Terri Lobdell is the Chief, Keystone Doctrine and Doctrine Integration Branch, Directorate of Doctrine and Intelligence Systems Training, U.S. Army Intelligence Center of Excellence at Fort Huachuca, AZ. She is a retired military intelligence warrant officer with 24 years of active and reserve Army service. During her tenure, she served in various intelligence assignments from company to echelons above corps. She holds a master's degree in public administration from the University of Nebraska–Omaha.

Doctrinal Proficiency and Doctrinal Assistance

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

- Answer -

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

Want to be in the doctrinal know?

USAICoE doctrine maintains an email notification list to announce —

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

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

Editor's Note: The following text is from FM 2-0,* Intelligence, *6 July 2018, Chapter 4, "Intelligence Staffs and Units."

National and Joint Intelligence Support

National intelligence organizations employ specialized resources and dedicated personnel to gain information about potential adversaries, events, and other worldwide intelligence requirements. National intelligence organizations routinely provide support to the joint force commander while continuing to support national decision makers. However, the focus of these national intelligence organizations is not evenly split among intelligence customers and varies according to the situation and competing requirements. During large-scale combat operations against a peer threat, intense competition for intelligence resources at every level requires efficient use and availability of Army information collection units and capabilities.

The Army, in response to validated requirements, may provide the theater and joint force with intelligence capabilities resident within [U.S. Army Intelligence and Security Command] INSCOM. INSCOM is a direct reporting unit to the Army Deputy Chief of Staff for Intelligence that conducts and synchronizes worldwide intelligence discipline and all-source intelligence operations. INSCOM also delivers linguist support and intelligence-related advanced skills training, acquisition support, logistics, communications, and other specialized capabilities to support Army, joint, unified action partners, and the U.S. intelligence community. INSCOM's functional brigades and groups may provide general support, general support reinforcing, or direct support to theaters through intelligence reach, or they may be force-tailored for deployment to support the joint force. INSCOM's functional brigades and groups include—

- An aerial intelligence brigade that provides aerial intelligence collection platforms, associated [processing, exploitation, and dissemination] PED, and mission command at forward locations.
- A [counterintelligence] CI group that conducts the full range of CI functions (operations, investigations, collection, analysis and production, and technical services and support activities).
- An Army operations group that conducts global, full spectrum [human intelligence] HUMINT operations.

Theater Army

The Army Service component command (ASCC) of a combatant command is called a theater army. The Army contributes organizational elements and capabilities to joint force commanders to conduct unified action across the range of military operations. Theater army headquarters, with their command posts and their associated theater-enabling commands and functional brigades, can control Army or joint forces for smaller scale contingency operations. (See ATP 3-93.)

The theater army maintains an area of responsibility-wide focus, providing support to Army and joint forces across the region, in accordance with the geographic combatant command's priorities of support. Depending on the region and the geographic combatant command's priorities, the relative emphasis that the theater army places on its operational and administrative responsibilities can vary greatly. The theater army focuses on administrative duties that support those operational requirements supporting the operations to prevent, [to prevail in] large-scale ground combat, and the operations to consolidate gains strategic roles. This frees the theater army to perform those functions that no other Army echelon can perform during those strategic roles:

- Shaping the area of responsibility to improve relative positions of advantage enjoyed by the United States and its allies.
- Protecting against threat actions outside of the operational area.
- Preventing the expansion of conflict unintended by friendly decision makers and senior commanders.
- Detecting and striking enemy capabilities that reside outside of a joint operations area. ***Note.*** During large-scale ground combat, theater army commanders and staffs must not overlook this important operational function.

The theater army enables the combatant commander to employ landpower anywhere in the area of responsibility across the range of military operations. It commands all Army forces in the region until the combatant commander attaches

selected Army forces to a joint forces commander. When that happens, the theater army divides its responsibility between the Army component in the joint operations area and Army forces operating in other parts of the area of responsibility. Each theater army supports the Army's strategic roles—shape, prevent, conduct [prevail in] large-scale ground combat, and consolidate gains—and facilitates the use of landpower in the joint task force to win.

Theater army intelligence operations are continually conducted to provide information and intelligence used to support land forces. Results from these operations are used to provide guidance on plans, policies, and strategic guidance. For the Army's corps, divisions, and [brigade combat teams] BCTs, theater army intelligence operations provide information used in [intelligence preparation of the battlefield] IPB, targeting, situation development, and protection, as well as provide warning intelligence.

The theater army headquarters has a G-2 who assists the commander in processing, analyzing, and disseminating information and intelligence provided by subordinate, higher, and adjacent units. (For more information on the theater army, see ATP 2-19.1 [classified].)

Theater Army G-2

The theater army G-2 is the commander's principal assistant who advises, plans, and coordinates actions of the intelligence warfighting function. The theater army G-2 is the—

- Chief of the intelligence cell.
- Theater army's senior intelligence officer.
- Principal intelligence advisor to the theater army commander.

The theater army G-2 is equipped with intelligence systems and processors that connect to all required networks. These systems are interoperable with the Army's mission command suite of systems and are able to share data with Army organizations at all echelons and organizations within the intelligence community.

The theater army G-2 and its supporting analysis and control element (ACE) provide regionally focused intelligence overwatch. Regionally aligned, assigned, and designated forces must thoroughly coordinate with the supporting INSCOM [military intelligence brigade-theater] MIB–T. This allows regional forces to access theater intelligence, infrastructure, and training opportunities, as well as leverage expertise resident in the theater. Organizations can also interact with INSCOM functional commands to focus organic intelligence capabilities and enhance situational awareness and mission readiness.

Theater Army Intelligence Cell

The theater army intelligence cell is responsible for synchronizing and integrating Army intelligence operations throughout the combatant command's area of responsibility. The cell's staff elements either embed or coordinate with other command post cells to facilitate this synchronization. Specifically, the theater army intelligence cell performs the following tasks:

- Plans, programs, budgets, manages, evaluates, oversees, and integrates all intelligence activities.
- Provides functional oversight of assigned or attached intelligence personnel and units.
- Manages theater army intelligence collection, production, dissemination, disclosure, and CI requirements.
- Coordinates for national intelligence support and executes intelligence engagement and theater security cooperation as required.

The intelligence cell in the theater army command post provides regionally focused intelligence support to Army and joint forces operating in the combatant command's area of responsibility. It is organized as a planning staff that assists the theater army commander in developing the plans required to support the combatant command's operations.

The theater army intelligence cell depends on the MIB–T for intelligence collection, single-source analysis, and all-source intelligence to meet the theater army's intelligence needs. With augmentation, the intelligence cell can conduct operational intelligence collection and analysis to support theater army operations or operate in direct support of a corps or other subordinate headquarters.

Military Intelligence Brigade-Theater

MIB–Ts are assigned to combatant commands and may be attached, [operational control] OPCON, or [tactical control] TACON to the theater army by the combatant commander. As the theater army's permanently assigned ground intelligence organization, the MIB–T can deploy scalable and tailorable intelligence capabilities to meet combatant command, ASCC, and [joint task force] JTF intelligence requirements. However, it is likely that MIB–Ts will be OPCON to the theater army; therefore, this publication discusses MIB–Ts as OPCON to the theater army.

MIB–Ts provide regionally focused collection and analysis to support theater army daily operations requirements and specific joint operations in the area of responsibility. MIB–Ts provide the theater army with its foundational capabilities to set the theater for the intelligence warfighting function. As such, MIB–Ts serve as intelligence anchor points for deploying forces. As anchor points, they provide intelligence

system and intelligence personnel support related to combatant command-specific operational environments. MIB–Ts also provide expertise on joint [intelligence, surveillance, and reconnaissance] ISR and Army information collection, intelligence resources, cultural knowledge of the theater, and the threat, as well as access to theater and national intelligence architectures and data that support intelligence operations.

Deployed MIB–T forces leverage secure communications networks to access nondeployed MIB–T, higher echelon Army, joint, and intelligence community capabilities through intelligence reach. MIB–Ts can provide or coordinate the following support and enabling services to ground forces deploying to, operating in, or otherwise supporting the theater:

- **Intelligence:**
  - Intelligence assessments.
  - [Common operational pictures] COPs and intelligence graphic products.
  - Persistent intelligence overwatch (for example cultural, language, area subject matter experts).
  - Federated intelligence production and coordination on behalf of the ASCC G-2.
- **Integration:**
  - Information technology integration.
  - Data services (COPs and intelligence pictures, theater foundation geospatial data, data sharing, access to the combatant command's distributed integrated backbone [also called DIB], and knowledge management).
  - Data ingest services (data push and pull, data formatting, and Distributed Common Ground System-Army [DCGS–A]-to-mission command systems population).
  - Architecture management services (secret, sensitive compartmented information, and multinational communications networks; regionally aligned forces DCGS–A connectivity; theater geospatial data and services across all network classification domains; and data routing services provided or coordinated by Ground Intelligence Support Activity information technology operations).
- **Training:** Live environment training, mobile training teams, and subject matter expertise.

The organization and capacity of each MIB–T differ in relation to enduring theater requirements and relative prioritization within the Defense Planning Guidance. Although tailored to the unique circumstances of the theater to which it is assigned, a MIB–T's standard baseline design is—

- A multicomponent brigade headquarters that includes Regular Army and Army Reserve elements.
- An operations battalion that serves as the theater army G-2's ACE. This battalion may also be task-organized as a theater intelligence center. The battalion may also send a task-organized intelligence support element as part of a forward deployment of a theater army headquarters command post/element and/or other ground intelligence forces.
- A forward collection battalion that may possess CI, HUMINT, and [signals intelligence] SIGINT capabilities.
- An Army Reserve [military intelligence] MI battalion-theater support (known as MI BN–TS) that is assigned to the Military Intelligence Readiness Command but regionally aligned to the theater, which can mobilize to provide surge and an extension of intelligence capability and capacity to the MIB–T to support ground force requirements in theater.

Theater Army-Level Intelligence Collection Capabilities

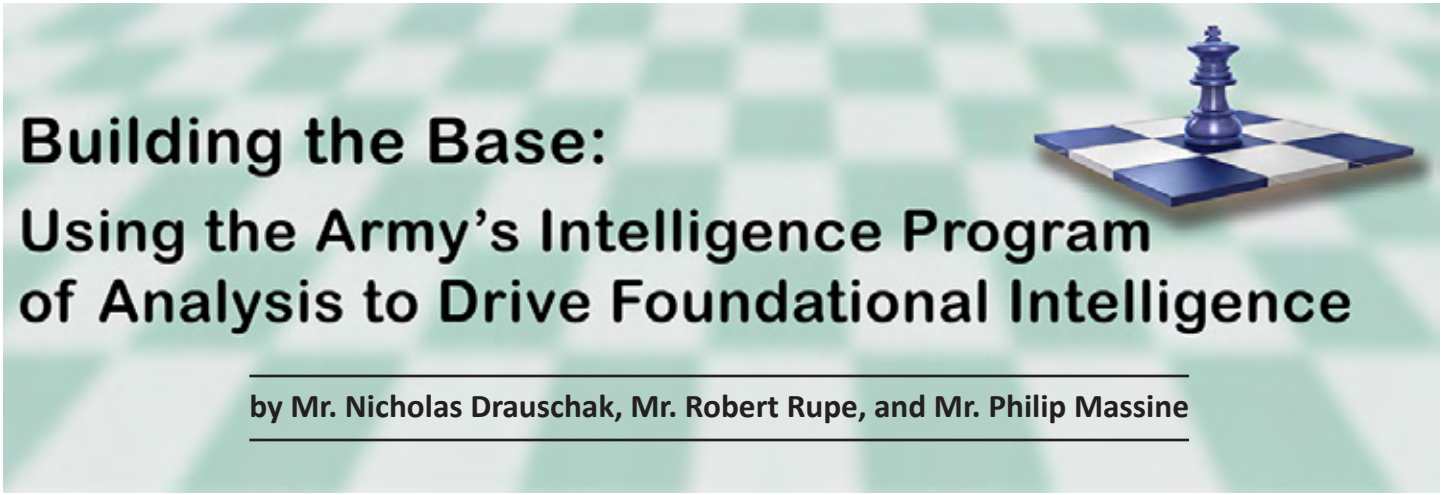
Since every theater and specific operation is different, the theater army G-2 will build an intelligence architecture, receive augmentation and higher-level support, and task-organize organic intelligence units based on the specific operation. The intelligence architecture will reflect how many MI capabilities are employed forward as well as the capabilities provided through reachback.

Note. Generally, at each echelon there are more requirements than intelligence analytical and collection capacity.

Theater Army-Level All-Source Intelligence Capabilities

All-source intelligence support at the theater army level consists of robust and sophisticated capabilities focused on analyzing a broad range of operational and mission variables across all domains. The analytical focus is at the strategic and operational levels. This all-source support occurs across all theater army command posts and is a key component of the intelligence architecture. All-source intelligence support includes the various elements of the theater army intelligence cell, the MIB–T operations battalion, and the regionally aligned Army Reserve theater support battalion.

The primary all-source analytical element supporting the theater army is the ACE. Most theater army ACEs do not deploy forward. However, tailored analytical elements deploy forward to support the theater army command post structure.



Building the Base:
Using the Army's Intelligence Program of Analysis to Drive Foundational Intelligence

by Mr. Nicholas Drauschak, Mr. Robert Rupe, and Mr. Philip Massine

If you're an inch off on landing, no big deal. If you're an inch off on take-off, you miss the moon by a million miles.

—Neil Armstrong

Introduction

Construction engineers understand the value of a solid foundation and the dangers associated with a foundation of questionable quality. A solid base can support skyscrapers of more than a hundred stories, reinforce bridges across the most turbulent waters, and sustain coastal communities through hurricane-force winds. Similarly, military operations require information composed of foundational intelligence gathered, analyzed, and disseminated far in advance of engagement. This article will—

- Clarify how foundational intelligence is used, drawing on Army foundational intelligence for examples.
- Discuss historical case studies of its success and failure on the battlefield.
- Describe the role of the National Ground Intelligence Center (NGIC) as a Service intelligence center in the acquisition, analysis, and distribution of foundational intelligence.
- Describe the process used to organize information into a series of documents that drive production within NGIC.[1]

The foundational intelligence for military operations is defined as the detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics required to plan for and execute unified land operations in a complex, dynamic, multi-domain operating environment.[2] Foundational intelligence encompasses knowledge of foreign armed forces, including the detailed analysis and cataloging of order of battle, infrastructure, and environmental knowledge to support military plans and operations.[3] Foundational intelligence is analyzing and testing an enemy's artillery weapons to gauge their effective range to keep allied units out of harm's way. It is knowing how long it takes to refuel and re-arm enemy helicopters to understand the window of time available to maximize an adversary's losses during a counterattack. Foundational intelligence makes up most of the doctrinal threat characteristics that tactical units require to begin planning and preparation of the battlefield—including composition, strength, combat effectiveness, doctrine/tactics, support relationships, electronic technical data, capabilities and limitations, and biometric and forensic data.[4] Though every operation should begin with a review of this foundational intelligence, one cannot assume that the information will always be readily available and in a consumable format. Figure 1 (on the next page) shows foundational intelligence elements as they relate to intelligence preparation of the battlefield (IPB) setup.

Foundational Intelligence: Historical Perspectives

The impact of a lack of foundational intelligence can be illustrated by failures and lessons learned during the 25 October 1983 invasion of the island nation of Grenada. Elements of the United States Army, Navy, and Marine Corps embarked upon Operation Urgent Fury to rescue deposed Grenadian Governor General Paul Scoon and several hundred American medical students held by soldiers and revolutionary forces from Cuba and Grenada. The rapid escalation of the situation exposed weaknesses in the foundational intelligence required to plan and execute the operation.

Senior leadership at Fort Bragg, North Carolina, in charge of the 82nd Airborne Division assumed that orders to prepare for deployment related to an overwhelming retaliation for the 23 October 1983 bombing of the Marine barracks in Beirut, Lebanon, that killed 241 American Service members. Maps and diagrams in nearly every briefing room at Fort Bragg all related to Beirut and Lebanon; even though two battalions of U.S. Army Rangers elsewhere had received a warning order days earlier about invading the

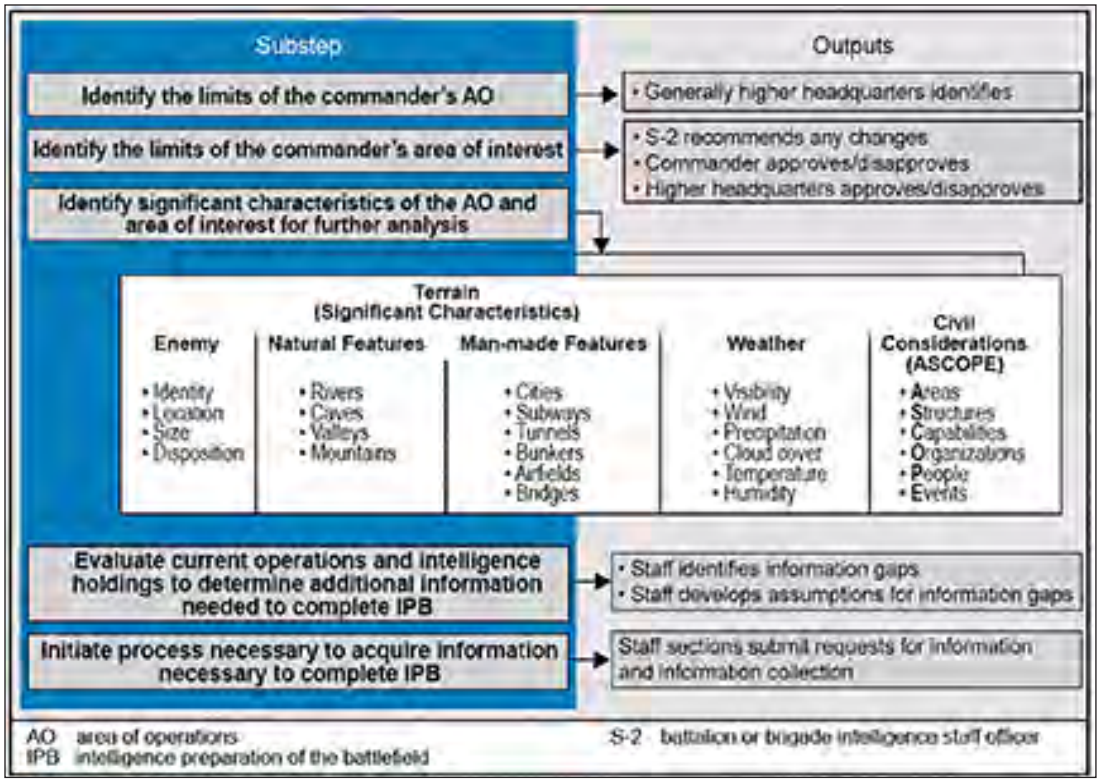


Figure 1. ATP 2-01.3: Substeps and Outputs of IPB Process[5]

Caribbean island. Leadership at Fort Bragg had minimal information available regarding the composition of opposition forces on Grenada, the country's topography, or the key facilities involved. Most of the information on the island nation was gleaned from articles found in a recent issue of *The Economist* magazine.[6] Invading Soldiers; Sea, Air, and Land Forces (SEALs); and Marines were provided outdated tourist maps of Grenada with superimposed military grids that contained no detail regarding topography or key facilities.[7] Deploying Joint Special Operations Command personnel were forced to use overhead photographs with hand-drawn key features, which severely limited artillery, naval gunfire, and air strikes.[8]

The lack of verified ground intelligence led to costly mistakes. Discrepancies in map coordinates, size and location of drop zones, facility identification, interoperability of communication equipment, and targeting systems led to the deaths of U.S. Service members and the unintentional targeting of a civilian mental hospital. Although the invasion ultimately succeeded—owing to the adaptability, ingenuity, and superiority of U.S. forces—the invasion resulted in 125 American casualties, of which 19 were killed and 106 injured.[9]

At its best, foundational intelligence enables rapid and unprecedented success within the operational environment. The 1991 Gulf War presented a number of critical intelligence support lessons that became highly relevant to future U.S. Army operations.[10] The surprise invasion of Kuwait by the Iraqi military, the rapid and massive initial deployment of coalition troops, and the growing international support for combat operations placed a large burden on the United States intelligence community. Given its comprehensive understanding of the adversary, the intelligence community was equipped and capable of responding with "decisive, aggressive, and perhaps most importantly, innovative collection, analysis, production, and dissemination measures" to support the operational environment.[11] The accurate breadth and depth of detail accumulated on the Iraqi chemical warfare program, the intelligence gathered regarding the Iraqi order of battle, and the identification of a multitude of structures scattered throughout Iraq as having military and strategic significance have all been identified as having critical foundational importance—without which the air war would never have been the success it was.[12]

Despite various operational dilemmas, such as a lack of cover and concealment, and the harshness of the desert environment, this intelligence facilitated the development of vastly improved tactics, techniques, and procedures for operating in an environment as austere as the Iraqi desert—lessons that would be perfected and used a little more than a decade later. Through knowledge gained regarding the lack of technological advancements of Iraqi armored and infantry units, the United States capitalized on the vast difference in night vision capabilities to "own the night" and conduct operations with relative impunity. Unit commanders and vehicle drivers used image-enhancement scopes and goggles and infrared and thermal-imaging systems to identify enemy vehicles using heat signatures developed years before through exploitation of foreign materiel.[13] Furthermore, knowing that Iraqi units did not possess similar technology allowed United States armored divisions to successfully fire on and destroy the enemy from a range at which those units neither exposed themselves to harm nor were close enough for the enemy to determine their

position.[14] The success of the foundational intelligence gained during Operation Desert Storm can best be summed up by the Department of Defense (DoD) report to Congress, which stated that "no combat commander has ever had as full and complete a view of his adversary as did our field commanders …This success reflected investments in technology and the efforts of thousands of U.S. intelligence professionals."[15]

Service Intelligence Centers

In 2017, GEN Joseph Dunford wrote, "The speed of war has changed, and the nature of these changes makes the global security environment even more unpredictable, dangerous, and unforgiving…Our decision-making processes and planning constructs must also be flexible enough to deliver options at the speed of war."[16] To generate decisions at the "speed of war," foundational intelligence must be sound, and current threat characteristics for the most likely, and even possible, adversaries are mandatory. At the forefront of maintaining today's foundational intelligence are members of the Defense Intelligence Enterprise. This enterprise, led by the Defense Intelligence Agency, comprises general and specialized intelligence centers focused on the production and maintenance of critical intelligence products and databases. The enterprise includes the Missile and Space Intelligence Center, the National Center for Medical Intelligence, and the Nation's Service intelligence centers. Uniquely positioned at the crossroads between the operational force and the intelligence community, four Service intelligence centers represent each branch of Service: National Air and Space Intelligence Center (Air Force), Office of Naval Intelligence (Navy), Marine Corps Intelligence Activity (Marine Corps), and NGIC (Army).

Service intelligence centers fulfill two primary roles: direct intelligence support to their Service and production of foundational intelligence on foreign military service capabilities and operational art. The Service intelligence centers leverage their unique understanding of their particular Service's mission and capabilities to address intelligence requirements and support mission command throughout the force. Direct support may include the provision of expertise to operationally deployed forces or support to senior decision makers within the Pentagon. In addition to this specific support to the Service, the Service intelligence center is also responsible for a layer of foundational data. This foundational layer consists of authoritative assessments regarding threat characteristics, future force projections, emerging capabilities, foreign force organization, and other topics. It represents a more general level of support not only to their Service but also to the DoD and the broader intelligence community.

NGIC, for example, is an Army military intelligence brigade that provides foundational all-source and geospatial intelligence on ground force capabilities and related military technologies while integrating with mission partners to ensure Army, DoD, joint, and national-level decision makers maintain decision advantage to protect U.S. interests at home and abroad. NGIC provides general military intelligence and the associated scientific and technical intelligence on foreign ground forces from the operational through small-unit level, maintaining detailed knowledge of current ground force capabilities and doctrine, as well as projecting 5, 10, and even 20 years into the future. The scope of this mission requires not only a specialized workforce but also a deliberate collection and prioritization of requirements from customers who rely on NGIC's assessments.[17]

The NGIC workforce composition reflects the need for deep expertise and mission continuity. At NGIC, civilians make up most of the workforce and enable the center to maintain deep regional and functional understanding. NGIC employs not only civilian general military intelligence specialists but also chemists, computer scientists, mathematicians, and engineers in diverse fields from aeronautics to robotics, as well as modelers, simulation experts, and other technical specialists who evaluate capabilities and performance data.[18] The Army also assigns active duty personnel to NGIC as a broadening assignment for intelligence noncommissioned officers, warrant officers, and officers, as well as a number of officers from other Service branches. These Soldiers bring recent operational experiences and perspective to NGIC, while gaining a greater depth of knowledge of analytic tradecraft and an understanding of the broader intelligence community. Finally, NGIC leverages a contract workforce that brings critical skills and capability not readily available within the civilian and military population.

Organizing the Effort to Maintain a Solid Foundation

Since 2014, NGIC has used the Director of National Intelligence's Program of Analysis process as a means to organize and prioritize its analytic focus. Each of the 17 members of the intelligence community produces a Program of Analysis that identifies where the member will focus analysis over a defined period. Each year, on behalf of the Army G-2, NGIC collects requirements from its customers across the Army Service component commands, the Army acquisition community (e.g., including Army Futures Command), Training and Doctrine Command, Forces Command, combatant commands, and elements of Special Operations Command. NGIC conducts extensive coordination with these organizations and brings representatives together to

establish priorities for each community of interest. The results are then compiled and organized around key intelligence questions that represent focus areas for intelligence collection and analysis. The key intelligence questions are also assessed to ensure they are assigned to the appropriate production agencies, both inside the Army and across the Defense Intelligence Enterprise. The resulting document is published as guidance for intelligence organizations across the Army. At NGIC, the Program of Analysis and the priorities expressed in it guide the development of a detailed production plan to address the specific requirements and areas for knowledge development.[19]

Though this process is repeated annually, many of the focus areas are enduring and remain part of the plan for more than just one year. The process has been continually refined, and NGIC has been able to look beyond each fiscal year and consider multiyear efforts.[20] This evolution has allowed NGIC to look more holistically at an issue and plan a series of products intended to build the solid foundation required to answer complex questions. The Program of Analysis process has also highlighted opportunities for integration with other intelligence partners, as well as additional information and organizational dependencies. Ultimately, it will set conditions for more efficient use of resources and more holistic answers to intelligence requirements.

This iterative process of planning and production is used to ensure the foundation for Army and joint planning remains strong and, more importantly, accessible. Although each accomplishes the mission differently, the Service intelligence centers and other foundational intelligence producers go to great lengths to ensure their work is published in a form that commanders and their staffs need. NGIC uses the Army Knowledge Gateway across multiple networks to share intelligence assessments as they are produced and catalogued.

Using Foundational Intelligence

Foundational intelligence provides operational customers, capability developers, and senior decision makers with the information they need to make informed decisions and avoid surprise. The depth of analysis provided by NGIC is most applicable to three Army intelligence support phases: IPB, current operations, and future acquisition. As the Army iterates IPB in response to current or potential crises, NGIC's analysis of ground and irregular forces provides a baseline understanding of foreign forces and associated operating environments that is necessary to predict adversary courses of action. As conflict progresses to current operations, NGIC provides situational updates on the threat and potential opportunities as they emerge. Looking 5 to 20 years into the future, NGIC provides foresight of foreign technology acquisition to inform Army capabilities developers of emerging adversary capabilities to mitigate technology surprise. NGIC is an important partner and provider to the Army through these critical phases of intelligence support.[21] Figure 2 shows foundational intelligence elements as they relate to IPB step 3 (evaluate the threat).

The 2018 National Defense Strategy signals that we are entering an era of dynamic force employment during which the Army must be prepared to respond to threats ranging from near-peer adversaries to violent extremist organizations. To achieve success in this global arena, Army units will rely heavily on the foundational intelligence provided by NGIC.[22] For example, the basic capabilities of opposition forces must be understood to calibrate force posture. A baseline understanding of coalition force capabilities must exist in order to prepare the operational environment and build partner capacity and interoperability, while

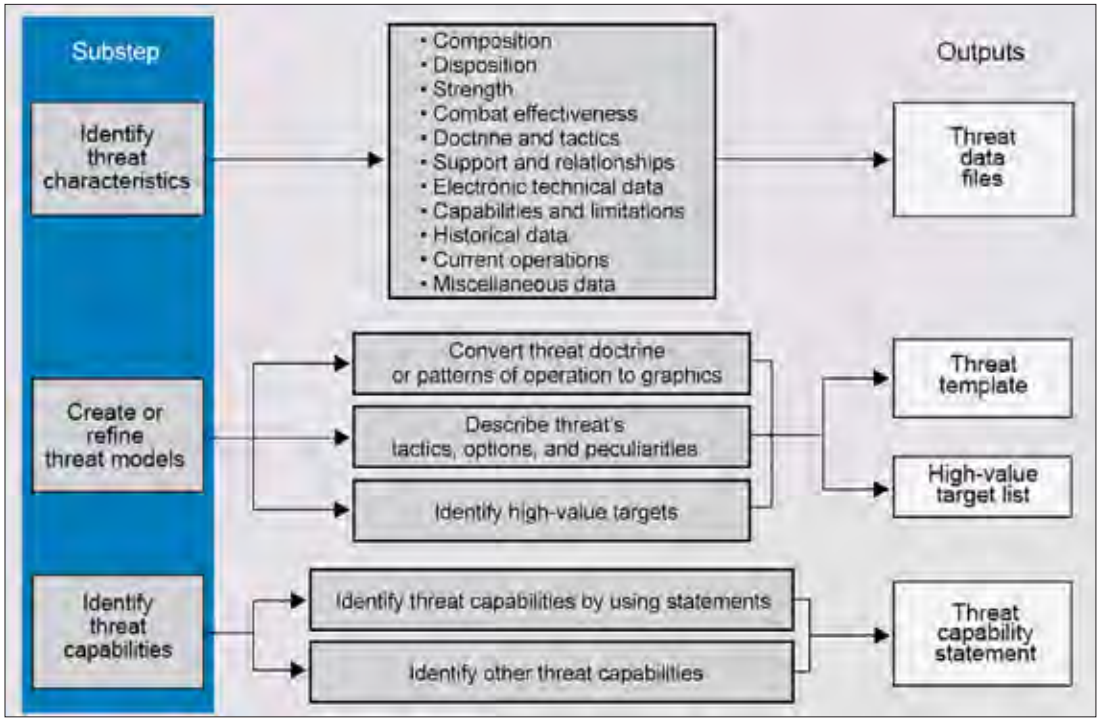


Figure 2. ATP 2-01.3: Substeps and Outputs of Step 3 of the IPB Process[23]

simultaneously enhancing coalition forces' abilities to defeat increasingly sophisticated enemy unconventional and information warfare. As was clearly demonstrated in Operation Desert Storm, the intelligence regarding opposition vehicle and personnel electronic and heat signatures was imperative to achieving tactical and strategic success.[24] Enemy reconnaissance, strike, combined-arms, and unconventional warfare capabilities must be understood, and vulnerabilities must be identified to converge joint force abilities in highly contested environments.[25] Finally, Service intelligence centers, such as NGIC, must maintain and make available to their customers any and all available information that can be leveraged for situational advantage, including data from national, joint, commercial, and Service repositories and libraries or directly from collection assets.[26]

Putting It All Together

The Army is called on to respond to threats to national interests worldwide, both conventional and asymmetric. This global mission carries with it an inherent risk: operational forces may be tasked to operate in theaters with little knowledge of the environment. NGIC's role is to reduce this risk by steadily monitoring the foundational enemy characteristics and environmental concerns of complex, dynamic, and multi-domain operating environs to enable decision advantage should military force be needed. NGIC does this by—

- ✦ Understanding the importance of foundational intelligence to the field.
- ✦ Taking critical lessons learned from a historical perspective.
- ✦ Finding its place as a Service intelligence center.
- ✦ Employing the Army's Program of Analysis to drive production.

In this way, NGIC supports the modern warfighter by providing, as its motto so aptly puts it, "intelligence today for tomorrow's fight." In his initial message to the Army team, incoming Chief of Staff GEN James C. McConville cited the need to "transform all linear industrial age processes to be more effective, protect our resources, and make better decisions."[27] Through close partnership between NGIC and the operational force, NGIC will continue to acquire, analyze, and disseminate foundational intelligence to maintain the decision advantage necessary to respond to current and future threats in an ever-changing global threat environment.

Epigraph

Seth Wickersham and Michael Rothstein, "Inside the Short, Unhappy Life of the Alliance of American Football," NFL, ESPN, Enterprises Inc., June 13, 2019, https://www.espn.com/nfl/story/_/id/26957796/inside-short-unhappy-life-alliance-american-football.

Endnotes

1. Rita C. McIntosh, "Intelligence Center Leads Army Program," *U.S. Army Worldwide News*, December 16, 2015, https://www.army.mil/article/160033/intelligence_center_leads_army_program.

2. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office [GPO], 6 July 2018).

3. Defense Intelligence Agency, *2016 Defense Intelligence Agency Strategy*, n.d., accessed 4 October 2019, https://www.dia.mil/Portals/27/Documents/About/2016_DIA_Strategy.pdf.

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

5. Ibid., 3-2.

6. Sharon Tosi Lacey, "How the invasion of Grenada was planned with a tourist map and a copy of 'The Economist,'" Military Times website, October 25, 2018, https://www.militarytimes.com/veterans/military-history/2018/10/25/how-the-invasion-of-grenada-was-planned-with-a-tourist-map-and-a-copy-of-the-economist/.

7. Marvellous Ojo, "US Invasion of Grenada—Successes and Failures," War History Online, September 13, 2018, https://www.warhistoryonline.com/history/us-invasion-of-grenada.html.

8. Keith Nightingale, "How Grenada Changed How America Goes to War," *Small Wars Journal*, October 25, 2013, https://smallwarsjournal.com/jrnl/art/how-grenada-changed-how-america-goes-to-war.

9. Ojo, "US Invasion."

10. John J. Bird, *Analysis of Intelligence Support to the 1991 Persian Gulf War: Enduring Lessons* (Carlisle, PA: U.S. Army War College, 3 May 2004), 2, https://apps.dtic.mil/dtic/tr/fulltext/u2/a423282.pdf.

11. Ibid.

12. Ibid.

13. Frank N. Schubert and Theresa K. Kraus, eds., "One Hundred Hours," in *The Whirlwind War: The United States Army in Operations DESERT SHIELD and DESERT STORM* (Washington, DC: U.S. Army Center of Military History, 1992), 174-206, https://history.army.mil/books/www/WWW8.htm.

14. Ibid.

15. Department of Defense, *Conduct of the Persian Gulf War: Final Report to Congress* (Washington DC: U.S. GPO, April 1992), quoted in Bird, *Analysis of Intelligence Support*, 2.

16. GEN Joseph Dunford, Jr., "From the Chairman: The Pace of Change," *Joint Force Quarterly* 84 (1st Quarter, January 2017): 3.

17. "National Ground Intelligence Center," U.S. Army Intelligence and Security Command website, updated June 19, 2019, https://www.inscom.army.mil/MSC/NGIC.aspx.

18. Ibid.

19. Rita McIntosh, Kelly Nelson, and Crissana Shackelford, "The Army Intelligence Program of Analysis," *Military Intelligence Professional Bulletin* 44, no.3 (July–September 2018): 25-28.

20. Ibid.

21. "National Ground Intelligence Center."

22. Ibid.

23. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield,* 5-4.

24. Schubert and Kraus, "One Hundred Hours."

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

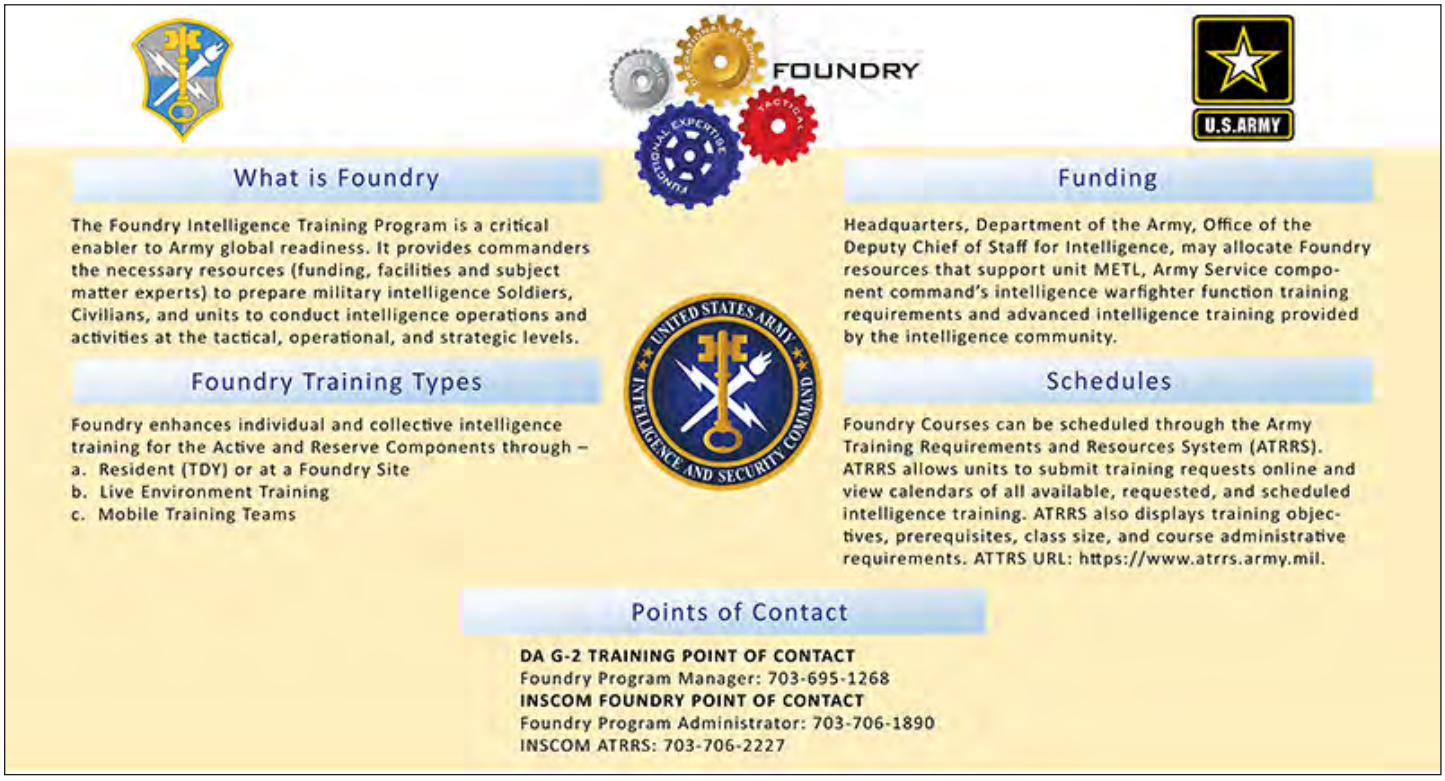
26. Ibid.

27. U.S. Army, "40th Chief of Staff of the Army Initial Message to the Army Team," *U.S. Army Worldwide News*, August 12, 2019, https://www.army.mil/article/225605/40th_chief_of_staff_of_the_army_initial_message_to_the_army_team.

Mr. Nicholas Drauschak currently serves as a program manager with the National Ground Intelligence Center (NGIC) Production Planning and Evaluation Branch. Prior to his role at NGIC, he served as an intelligence analyst with the Virginia Fusion Center and as a strategic emergency planner for the National Capital Region. Mr. Drauschak holds a bachelor of interdisciplinary studies from the University of Virginia, and he is currently pursuing a doctoral degree in fire and emergency management administration.

Mr. Robert Rupe currently serves as the NGIC Branch Chief for Production Planning and Evaluation. Before his retirement from active duty as a chief warrant officer 5, he served as the NGIC senior military technician and the senior all-source technician at Combined Joint Task Force–Operation Inherent Resolve G-2, International Security Assistance Force (ISAF)-ISAF Joint Command, Army North, Army Central, and Army Europe. He holds a master of science in strategic intelligence from the National Intelligence University.

Mr. Philip Massine currently serves as a production planner with the NGIC Production Planning and Evaluation Branch. He has more than 15 years of experience as an infantryman, military intelligence officer, and Army Civilian intelligence analyst. Mr. Massine is a certified defense all-source analyst and holds a bachelor of science in cognition and a master of business administration.



Army G-2X Support to Army Readiness and Modernization Priorities

by Lieutenant Colonel Marcus O'Neal

The National Defense Strategy emphasizes the reemergence of long-term, strategic revisionist powers—China and Russia—resulting in the Army's focus on improving readiness, force projection, and overmatch in multi-domain operations (MDO) against these peer adversaries in competition and large-scale combat operations.[1] To meet joint force requirements and maintain global land force dominance, the Army is pursuing six modernization priorities:

- Long range precision fires.
- Next generation combat vehicles.
- Future vertical lift.
- Network.
- Air and missile defense.
- Soldier lethality.

The Army's modernization strategy requires a transition from the Industrial Age to a technology-enabled Information Age.[2] The Army G-2's vision of multi-domain intelligence illuminates the path forward for Army intelligence enterprise innovation and modernization to fight and win through speed, precision, and accuracy of the intelligence process. Army counterintelligence (CI), human intelligence (HUMINT), foreign disclosure, and security are critical multi-domain intelligence capabilities. The Headquarters, Department of the Army G-2X[3] and the CI, HUMINT, foreign disclosure, and security professionals across the Army will ensure the successful execution of missions to collect intelligence and protect essential friendly information and assets, understand changes in the operating environments, strengthen partnerships, and mitigate threats.

Accomplishment of the G-2X, foreign disclosure, and security mission sets will enable force projection and provide decision advantage to policy makers and commanders to take action ahead of the adversaries' decision cycles. The Army G-2X formulates policy, plans, and programs resources; conducts oversight; and represents functional requirements in Headquarters, Department of the Army, Department of Defense, and the intelligence community. The Army G-2X supports Army readiness and modernization by increasing capability and capacity across CI, HUMINT, and security formations to support multi-domain intelligence and operations in both competition and conflict.

Army G-2X is reforming Army CI and re-focusing Army HUMINT, foreign disclosure, and security to support modernization priorities and to protect critical technologies while countering insider threats. The Director, Army G-2X, with the support of three senior advisors for CI, HUMINT, and security, is implementing a strategy to realign the CI, HUMINT, and security community to meet Secretary of the Army's readiness and modernization priorities through multi-domain intelligence to ensure dominance in MDO. The Army G-2's number one priority in multi-domain intelligence is CI reform. Other Army G-2X primary efforts include achieving HUMINT readiness through adaptation and establishing intelligence security as an intelligence discipline.

Army G-2 Priority Effort: Counterintelligence Reform

Army CI is reforming to counter the foreign intelligence entities of peer rivals—Russia and China—and regional threats, including Iran and North Korea. The Army CI enterprise is postured for a post-Cold War and War on Terrorism environment that prioritized the security of Army tactical and operational forces against terrorism and force protection threats. The Army's modernization priorities, Army Campaign Plan 2019, and The Army Intelligence Plan address aggressive and technologically empowered China and Russia as the dominant future threats. The Army must deliver uncompromised major defense acquisition programs and other enabling capabilities to the future force. The uncompromised delivery of these future strategic capabilities requires a unified and technologically superior Army CI force executing centrally managed and globally synchronized CI activities that deny foreign intelligence entity abilities to operate in the land and cyberspace domains against Army modernization priorities.

Currently, the Army CI enterprise's force posture is optimized to address CI threats of the late 20th century or counterterrorism threats, not current foreign intelligence entity threats. To meet this challenge, the Army must reform the CI enterprise to leverage all available forces to actively counter current and emerging CI threats, while sustaining validated CI requirements for combatant commanders. Achieving this goal will require adjustments of Army CI available resources to focus on current and emerging threats, and improve force skills and authorities. The Army G-2X is leading comprehensive initiatives to update Army CI doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P). This initiative includes input from relevant stakeholders and subject matter experts to apply a wide range of experience and viewpoints to CI reform.

Achieving Human Intelligence Readiness through Adaptation

Building readiness and supporting MDO requires a restructuring and refocus of Army HUMINT to increase operations during competition phases and better prepare the operational environment to ensure dominance over our adversaries. In the multi-domain battlespace against peer and near-peer adversaries, whoever has the ability to sense, understand, decide, and act faster than their opponent will enjoy decisive advantage. Army HUMINT must increase capabilities and capacity as well as accelerate tempo to meet the demands of MDO. The challenges of HUMINT operations in a global and competitive environment with the constant threat of peer conflict differ from the operational experiences Army HUMINT collectors have acquired from a decade plus of counterinsurgency operations occurring largely in Iraq and Afghanistan.

To be competitive against peer and near-peer adversaries, Army HUMINT must adapt to rapidly enable the intelligence warfighting function to support commanders during all phases of joint, multi-domain, high intensity conflict and during competition short of armed conflict. Army HUMINT must rapidly provide the information and intelligence required to enable commanders to clearly understand the adversary and the operating environment and to inform their decision-making processes. Adapting to MDO drives an increased emphasis on HUMINT collection as a deep sensor intelligence, surveillance, and reconnaissance platform for immediate support to fires, maneuver, and force protection; early warning across the range of military operations; and in advance of direct conflict. To be successful, the Army must better man, organize, train, equip, develop, and most importantly, use its HUMINT Soldiers to rapidly provide HUMINT capabilities that increase the lethality and survivability of U.S. forces.

U.S. Army photo by CPT Benjamin West

A platoon leader briefs adjustments to the planned field interrogations at the objective rally point during a training exercise in Cache Valley National Forest, August 11, 2019.

HUMINT must increase the pace of operations and emphasize the development of capabilities in advance of conflict to uniquely provide intelligence in a degraded, intermittent, and limited bandwidth environment when other sensors are degraded or compromised. Source identification, acquisition, and communication must occur during the competition phase and in advance of need to support commanders' requirements now and in combat. To fulfill the mission of setting the theater, shaping, and deterring while in a competitive environment and in advance of conflict, Army HUMINT collectors must be actively involved in identifying, engaging, and collecting from HUMINT sources to prepare the operating environment. They must maintain HUMINT readiness before the conflict phase upon which HUMINT will rely to provide coverage in deep areas targeting enemy forces and capabilities in support of corps, division, and brigade echelons. This will require a partnership between national agencies, foreign counterparts, Service-level assets, theater intelligence brigades, and regionally aligned forces. HUMINT operations collecting on the deep fires areas are preparatory intelligence activities that contribute to setting the theater with the necessary activities to establish and maintain conditions to seize the initiative and retain freedom of action for the specific theater.

Maximize Human Potential

The Army builds and sustains multi-domain formations through the selection, training, and education of the leaders, Soldiers, and teams in them. Employing multi-domain capabilities requires the Army to attract, retain, and employ leaders and Soldiers who collectively possess a significant breadth and depth of technical and professional expertise. The Army must exercise careful talent management to make the most of these high-quality personnel and integrate them into trusted teams of professionals who are able to thrive in ambiguity and chaos. Improving the resilience of leaders and Soldiers—the Army's most valuable capability—requires training, educating, equipping, and supporting them to execute Multi-Domain Operations in all of its intensity, rigor, and complexity.

—TRADOC Pamphlet 525-3-1[4]

Additionally, the Information Age provides opportunities to increase the speed of reporting to answer intelligence requirements and support key decision points. Intelligence consumers require structured-data HUMINT reporting that directly feeds mission command systems and feeds the enemy common operational picture at the speed of mission. The production of intelligence information reports through a national publication system for "pull" by commanders and analysts fails to support timely situational awareness and battlefield visualization required by maneuver operations. A bridging approach to reporting via a mechanism that is more enduring than a SALUTE Report, is more responsive than an intelligence information report, and feeds mission command systems and the digital common operational picture is necessary. Systems must feature one-time data entry and enable tipping and cueing of collection and direct support to fires and maneuver operations to produce HUMINT reporting that is relevant to commanders' needs. Furthermore, Army HUMINT must seek opportunities to use material solutions and employ automation and artificial intelligence to support source identification, targeting, and HUMINT collection and operations management. These processes must be continuous and reviewable in real time and use big data and social media to exploit opportunities at the speed of conflict.

Establish Intelligence Security as an Intelligence Discipline

The security of programs, personnel, technology, information, and facilities is critical as the Army shifts its focus to the modernization of warfighting capabilities to fight and win against peer and near-peer adversaries. Threats to Army capabilities and decisive advantage are active now and rapidly increasing. Foreign threats, especially China and Russia, pose a direct threat to United States Government and industry systems. Army intelligence security professionals support the National Security Strategy, National Defense Strategy, Army Strategy, and modernization priorities. Army G-2X is reshaping intelligence security execution to meet the recent and rapidly emerging need to confront national security threats at the organizational level. This reshaping to meet the mission command approach will play out in three main phases: rebalance, consolidation, and realignment. Intelligence security professionals are the front line of defense against adversaries currently operating against the Army. They are proactively denying access to information, personnel, or facilities, based on known or reported threat indicators and are often the first to identify and report information related to CI threats. Empowering subordinate leaders with the required resources will help ensure effective reform and improved security posture across the Army.

Professionalizing the Security Workforce to Meet Army Priorities

At the close of 2018, the Army G-2 issued implementation guidance for a professional certification requirement for our security employees. This readiness imperative will cultivate Army Civilians who provide commanders with the intelligence support they require to plan, fight, and win decisively across all domains. Investments in training, education, and professional progression must focus on current and future

mission needs, enhance tradecraft, and address competencies with the intent to close existing gaps. This comprehensive talent management effort will develop and sustain the skillsets our workforce requires to provide intelligence support to commands with increased speed, precision, and accuracy. The Army will continue to leverage smart and bold institutional reform to its security workforce, refine processes and modernize systems to address the increasing threats, and ensure protection against threat actors who are pilfering our information and compromising the Army's capabilities today. The Army security workforce is the first line of defense against relentless adversaries daily threatening the Army's current and future capabilities.

Way Ahead

Moving forward, Army intelligence, specifically the G-2X enterprise, must build upon and evolve hard-won lessons from the counterinsurgency fight to ensure victory in a large-scale ground combat operations environment contested by a global peer or near-peer adversary. To achieve this, the Army needs a fully capable, tailorable, scalable, adaptable, doctrinally sound, well-trained, well-equipped, professional CI, HUMINT, and security force to mitigate insider threats and risk to force projection. This force will also provide warning intelligence, along with situational understanding to commanders, in order to enhance the lethality and survivability of U.S. forces. As part of this, CI and HUMINT organizations and operations will be tailorable and flexible, manned, and equipped with modular, scalable, interoperable, and deployable teams and systems capable of deploying in the first lift in concert with the Army tenet of "fight tonight."

The primary differences from the counterinsurgency fight and great power competition concerning peer or near-peer conflict include increased emphasis on threat gray-zone activities. This involves increased espionage activities in the competition phase and a need to prepare for transition to fast-paced missions involving screenings of refugees or displaced persons. It also includes a large number of interrogations for enemy combatants on a continuously evolving battlefield, in addition to the missions of debriefings and source operations that will be expected during the conflict phase. CI forces must enable the Army's modernization by being "left of theft" and protecting our supply chains to deliver uncompromised capabilities to the future force as well as defend our critical infrastructure to support force projection efforts. HUMINT operations must be aggressive, persistent, enduring, and continuous in nature with the requirements tailored and adjusted to meet commanders' and decision makers' operational needs. Army HUMINT must identify and develop sources now, in advance of need, to set the theater during competition short of armed conflict, provide warning intelligence of adversary intentions and actions, and increase lethality during large-scale ground combat operations. Army HUMINT operations must have the capability to penetrate deep networks within complex operating environments where adversaries have increased capabilities to detect and counter our efforts.

Furthermore, Army HUMINT must be prepared to operate within multiple domains and employ materiel modernization to leverage artificial intelligence/fusion capabilities to reduce cognitive burden on analysts. The Army G-2X enterprise must adapt to meet the readiness demands of great power competition by ensuring our CI, HUMINT, and security personnel are prepared to deploy, fight, and win across the spectrum of conflict. Through modernization, the Army G-2X enterprise must be able to build an agile CI, HUMINT, and security force that fully embraces the Information Age, including leveraging technology to reduce cognitive burdens on the force and deliver intelligence at the speed of mission.

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://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. Department of the Army, *2019 Army Modernization Strategy: Investing in the Future,* n.d., 3, https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf.

3. The G-2X is the U.S. Army counterintelligence and human intelligence staff element.

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

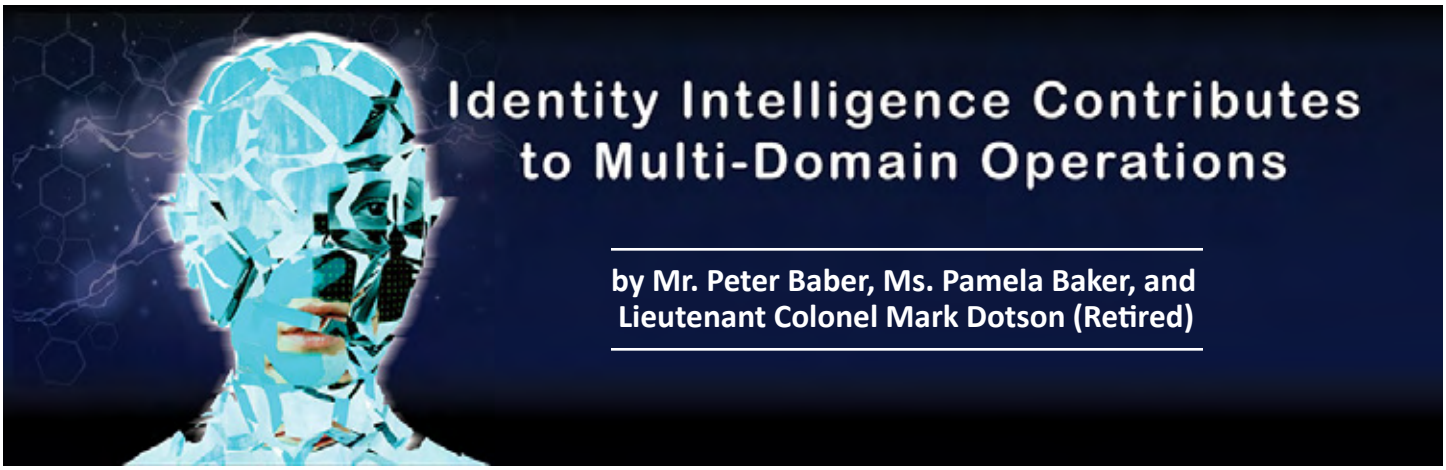
LTC Marcus O'Neal is the Senior Plans Officer for the Headquarters, Department of the Army, Counterintelligence, Human Intelligence, Disclosure and Security Directorate, Army G-2. He holds a bachelor of arts in political science from Southern University and a master of science in strategic intelligence from the National Intelligence University. His previous assignments include Intelligence Planner, XVIII Airborne Corps; Operations Officer, 519th Military Intelligence Battalion; and Executive Officer and later Operations Officer, 525th Military Intelligence Brigade.

Contributors:

Mr. Greg Smietanksi, Army G-2X Human Intelligence Division Chief.

Mr. Michael Schellhammer, Army G-2X Counterintelligence Division Chief.

Mr. Ryan Mower, Security Specialist, Army G-2 Security Division.



Identity Intelligence Contributes to Multi-Domain Operations

by Mr. Peter Baber, Ms. Pamela Baker, and Lieutenant Colonel Mark Dotson (Retired)

Introduction

U.S. Army identity intelligence (I2) is a capability to identify foreign persons of military interest. It distinguishes individuals from each other; discovers new threats and links them to other people, places, and things; and characterizes individuals, entities, groups, networks, and populations of interest. I2 fuses data and information with behavioral, reputational, biometrics, forensics, and other associated identity signatures in order to identify military threat persons of interest. The Army's I2 capability has evolved beyond the counterterrorism and counterinsurgency operational environment (OE) into an "all-threats" enduring requirement. In today's era of multi-domain operations (MDO), I2 provides the Army with an unprecedented insight into potential and existing threats and their plans, intentions, and networks. I2 also supports the force on the battlefield. The Army maintains and sustains its I2 capability at echelons above corps, through Headquarters, Department of the Army, G-2, and the U.S. Army Intelligence and Security Command, primarily at the National Ground Intelligence Center.

Capabilities of Identity Intelligence

I2 identifies and monitors foreign threat-based persons, groups, and networks of military interest and their supporting relationships that are critical to the success of weapons, plans, strategy, and operations; it also identifies and monitors their development, proliferation, and deployment. I2 provides the foundational intelligence that enables the development of a common operational picture (COP) of the OE human layer, determining friend or foe. This includes the ability to maintain situational awareness of connections and changes of key persons of interest of great power competitors, rogue states, violent extremist organizations, and transnational criminal organizations, as well as their proxies, associates, and allies. I2 also identifies individuals and populations that are either vulnerable to malign influence or receptive to building partner-nation capacity.

Imperative to the success of I2 in the conflict phase is conducting I2 operations "left of conflict" (i.e., early in an engagement) by establishing foundational capabilities, including driving collections, and conducting engagements that leverage foreign-partner and U.S. interagency relationships. This includes forensic, intelligence, and biometric partnerships, practiced in joint-combined exercises and executed in cooperative operations, thereby building partner-nation capacity and enriching foundational intelligence. Some means include—

- Developing the environment to establish foreign partner information and intelligence sharing and leveraging current agreements.
- Conducting and collaborating on activities to collect, analyze, and disseminate information about foreign individuals and networks of military interest and their capabilities.
- Collaborating with foreign and U.S interagency partners to monitor foreign persons of military interest.
- Driving collections, evaluating, and analyzing identity and biometric-match information.
- Confirming the identity of non-attributed foreign individuals and forces of military interest, monitored and disseminated via I2 analytical applications, such as the Biometric Identity Intelligence Resource/Identity Intelligence Analytic Resource and the Department of Defense (DoD) Biometrically Enabled Watchlist, to establish the foundational layer of military threat persons of interest, the COP of the OE human layer.
- Using weapons technical intelligence to collect, exploit, analyze, and disseminate information on foreign persons of military interest and their capabilities and attribute them to threat-based devices.
- Tracking adversaries' and other actors' surreptitious activities, in particular malign influence efforts.

Multi-Domain Operations

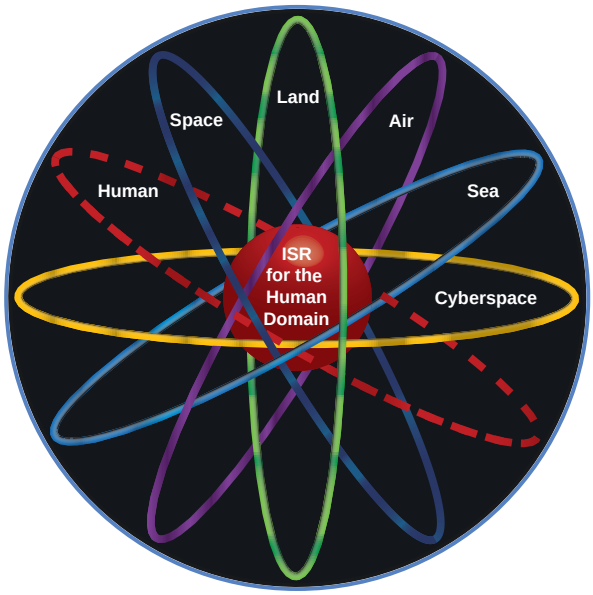
LTG Eric J. Wesley, U.S. Army Futures Command Deputy Commanding General and Director, Futures and Concepts Center, describes MDO as "how the Army envisions a joint warfighting concept that will bring to bear all of the firepower, both kinetic and non-kinetic, to help the U.S. military regain superiority in what is increasingly becoming a contested, access-denied world of near-peer competitors such as China and Russia."[1] U.S. Army Training and Doctrine Command (TRADOC) describes MDO as "designed to achieve U.S. strategic objectives articulated in the National Defense Strategy, specifically deterring and defeating China and Russia in competition and conflict."[2] MDO optimizes effects from across multiple domains identified in joint Service doctrine—land, sea, air, space, and cyberspace—as well as the electromagnetic spectrum and the information environment. A shared trait among the domains, electromagnetic spectrum, and information environment is people—the human element. Humans make decisions and make mistakes. Humans design, deploy, and operate weapons and war plans. According to MDO, "at some point, all the abstract elements (cognitive, virtual, informational, and human) demonstrate their effects physically at a place or in an area through a system or people,"[3] and those systems are designed, proliferated, deployed, and operated by people. Identity intelligence—

- Provides the "so what" that distinguishes individuals from each other (identity resolution).
- Discovers new threats (identity discovery) and links them to other people, places, and things (identity/device attribution).
- Characterizes an individual or network for kinetic and non-kinetic outcomes, supporting the National Defense Strategy and Army's strategic roles.

JP 5-0, *Joint Planning,* states that the OE is the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander, encompassing physical areas and factors of all domains. Included within these areas are the adversary, friendly, and neutral actors relevant to a specific joint operation. The OE includes the human element because a human aspect is present in each domain. Understanding the OE, including the human aspect of the domains, helps the commander to better identify the problem; anticipate outcomes; understand the results of various adversary, friendly, and neutral actions; and understand how these actions affect the military end state.[4]

Identity Intelligence (I2) is the ISR for the "Human Domain"

There is a human aspect to every domain: land, sea, air, space, cyberspace, the electromagnetic spectrum, and information environment



Humans make decisions; make mistakes; design, deploy proliferate, and operate weapons and war plans

Army I2 identifies foreign persons of military interest; it distinguishes individuals from each other, discovers new threats, links them to other people, places, and things, and properly characterizes the human element, sometimes non-doctrinally characterized as the "human domain"

Although MDO is a new and evolving operational warfighting concept, in 2012 the 38th Chief of Staff of the Army retired GEN Raymond Odierno stated, "The world has always been defined by uncertainty and change, but in reality the fundamental nature of war remains the same—a struggle to influence key terrain, populations and governance. Preventing conflict is better than reacting to it, and to prevent it you must understand its causes, but understanding is best gained through presence, presence on the ground. Understanding the human dimension and human domain… We must never forget that conflict in any form at its core is a human endeavor."[5] Army I2 properly characterizes the human element, sometimes non-doctrinally characterized as the human domain.

TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* states that to be successful in the complex, lethal, and chaotic MDO environment, the Army must build trusted teams of professionals that thrive in ambiguity and chaos. These teams are empowered through a doctrine

of mission command to rapidly react to threats and opportunities based on a commander's intent.[6] I2 can identify—

- Foreign individuals critical to adversarial success in MDO.
- Personalities who author, define, and field military plans and doctrine.
- Commander's intent.
- Personalities who successfully thrive in ambiguity and chaos.

Identity Intelligence Addresses the Multi-Domain Problems

According to TRADOC, we must solve five multi-domain problems to meet the strategic objectives of MDO. I2 can contribute to resolving each of these problems.

The first problem is competing to defeat aggression short of armed conflict and to deter conflict. Great power competitors and rogue states continue to use gray-zone tactics (political, economic, and hybrid warfare) short of armed conflict. These tactics include exploiting economic and diplomatic levers, conducting information confrontation, and using proxies and associates to undermine and fracture U.S. partnerships and U.S. access globally. Rather than reacting late, we must recognize that the early identification and monitoring of malign actors and the identification of other individuals driving these initiatives are critical to the success of MDO and will contribute to defeating aggression and deterring conflict.

The second and third problems are penetrating and later dis-integrating enemy antiaccess and area denial (A2AD) systems to enable tactical, operational, and strategic maneuver. Crucial to success against these problems in the armed conflict phase of MDO is the application of I2 before conflict (during the competition phase). This involves building partner-nation capacity and enriching foundational intelligence by establishing a foundational layer of military threat persons of interest and the COP of the OE human layer.

The fourth problem is exploiting freedom of maneuver to defeat the enemy and achieve U.S. strategic objectives. I2 identifies foreign individuals critical to adversarial success in MDO, including personalities who define and establish adversarial plans and doctrine, effectively execute commander's intent, and thrive in ambiguity and chaos.

The fifth problem is re-competing to consolidate gains and expand the competitive space to enable policy makers to resolve the conflict. For almost 18 years, the Army has effectively applied its I2 capability to stability operations in alignment with the re-compete phase.

Multi-Domain Problems

Phases of Multi-Domain Operations

MDO has three phases: competition, armed conflict, and return to competition. To be successful, we must defeat adversaries and achieve strategic objectives in all three.

Competition. The application of I2 before conflict (during the competition phase) is key to identifying the individuals and networks of interest who are critical to adversarial success in MDO, including understanding their development, proliferation, and deployment of weapons, plans, and strategy. In the competition phase of MDO, the joint force expands the competitive space through active engagement to counter malign influence, unconventional warfare, and information warfare directed against partners. These actions simultaneously deter escalation, defeat attempts by adversaries to "win without fighting," and set conditions for a rapid transition to armed conflict. LTG Wesley said, "If there's a word that you want to remember in terms of identifying the challenges we face within the pacing threats, it is the word 'standoff.'...We talk about this in two periods. The competition period and the conflict period, and what we find is our peers are fully engaged in the first layer of standoff by investing in efforts of democratic elections. Not only U.S. elections but Brexit, Catalonia and others, and that becomes the first layer of standoff."[7] "Deterrence should be the first available option but 'is challenged' because the threat of massive retaliation loses its values if adversaries are achieving their operational and strategic objectives left of conflict."[8]

Early engagement is a key aspect not only of MDO success but also of the success of I2 in MDO, both for the United States and its adversaries. According to TRADOC Pamphlet 525-3-1, since war is fundamentally and primarily a human endeavor, the United States must work with partners to address the cognitive aspects of political, human, social, and cultural interactions to achieve operational and national

objectives. Establishing capabilities early in an engagement (i.e., "left of conflict") is crucial to I2 success in MDO, including integrating I2 into concept plans and operation plans. This includes leveraging foreign-partner relationships "left of conflict" for forensic, intelligence, and biometric partnerships. These foreign-partner relationships are practiced in joint-combined exercises and executed in cooperative operations, to build partner-nation capacity and enrich foundational intelligence. Also important is establishing the foundational layer of military threat persons of interest and developing the COP of the OE human layer (foreign persons of military interest in the "human domain" of the OE) executed by I2 operations and disseminated through Biometric Identity Intelligence Resource/Identity Intelligence Analytic Resource and the DoD Biometrically Enabled Watchlist. Army I2 plays a key role in identifying great power competitor malign influence actors and activities. The ability to identify individuals, groups, and populations either vulnerable to malign influence or receptive to building partner-nation capacity can defuse the effects of great power competitor malign influence and information warfare.

Armed Conflict. In the conflict phase of MDO, the joint force defeats aggression by optimizing effects from across multiple domains at decisive spaces to penetrate the enemy's strategic and operational A2AD systems, dis-integrate the components of the enemy's military system, and exploit freedom of maneuver necessary to achieve strategic and operational objectives that create conditions favorable to a political outcome.

Once again, establishing I2 capabilities "left of conflict" is crucial to I2 success in MDO. We can do this by building partner-nation capacity and enriching foundational intelligence by establishing the foundational layer of military threat persons of interest, the COP of the OE human layer. "Left of conflict" identity discovery of foreign intelligence and special operations personnel who may operate in friendly or allied spaces during conflict is included in that layer. A body of evidence states our adversaries are effectively using engagements to shape the field and are establishing their I2 foundational layer "left of conflict." If we wait until armed conflict to establish the I2 foundational layer, it will be too late.

Army FM 3-0, *Operations,* describes armed conflict with great power competitors as intense, brutal, complex, and chaotic. This conflict will include noncombatants and will likely be in and around large cities, with adversarial use of terror, criminal activity, and information warfare.[9] Warfare results in the movement of civilians and stresses the resources of nations. Current counterterrorism and counterinsurgency (non-great power competitor) conflicts, according to the United Nations, have resulted in the highest number of people fleeing conflict since World War II. Refugee sites are exploited to harbor terrorists and to radicalize and recruit new members. I2 can support the rule of law and security to identify friend or foe, to verify individuals authorized to enter refugee and internally displaced persons sites, and to identify and exclude threat personalities (criminal and radical) attempting to exploit those sites. In a similar manner, we can use I2 to support noncombatant evacuation operations. We have used I2 effectively at coalition counterterrorism and counterinsurgency detention facilities, and similarly we should use I2 for enemy prisoners of war to establish a baseline identity, confirm identity, and identify deceptive individuals.

The United States will be required to penetrate and disintegrate enemy A2AD systems to enable tactical, operational, and strategic maneuver in armed conflict. Again, we can address this through the application of I2, "left of conflict." I2 has the ability to provide insight on adversarial force modernization that threatens Army and DoD modernization priorities, supports the protection of U.S. critical technology, deters the theft of technologies, and potentially slows or prevents the integration of DoD technology into adversarial systems.

Return to Competition. In this phase, the joint force consolidates gains and deters further conflict to allow the regeneration of forces and the re-establishment of a regional security order aligned with U.S. strategic objectives. While the Army's I2 capability has evolved beyond counterterrorism and counterinsurgency applications, we have applied it liberally and effectively to stability operations in alignment with the re-compete phase. The ability to identify individuals, groups, and populations vulnerable to malign influence or receptive to building partner-nation capacity will enable commanders and policy makers to capitalize on gains, stabilize and resolve conflicts, and return to competition.

Conclusion

The Army's I2 capability has evolved beyond the counterterrorism and counterinsurgency OE to an "all-threats" enduring requirement relevant to MDO. I2 has been characterized as intelligence, surveillance, and reconnaissance for the "human domain." I2 also contributes to intelligence preparation of the battlefield in relation to the "human domain." As the Army further develops MDO, intelligence leaders should reflect on how I2 can be a force multiplier across multi-domain operations. LTG Wesley addressed the importance of getting "left of conflict" and the ability of actions in the competition phase to positively affect the

armed conflict phase or deter conflict. Intelligence leaders should explore how to incorporate I2 into the development and experimentation of MDO. Human aspects are present in each domain. Humans make decisions and make mistakes. Humans design, deploy, and operate weapons and war plans. Intelligence leaders should explore how I2 can present multiple dilemmas to the adversary in the competition phase. They should also explore how to incorporate I2 into the multi-domain task forces and how to use the Intelligence, Information, Cyber, Electronic Warfare, and Space detachments to support I2 operations.

Endnotes

1. Todd South, "This 3-star Army general explains what multi-domain operations mean for you," *Army Times,* August 11, 2019, https://www.armytimes.com/news/your-army/2019/08/11/this-3-star-army-general-explains-what-multi-domain-operations-mean-for-you/.

2. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Fort Eustis, VA: TRADOC, 6 December 2018), 24.

3. Ibid., C-2.

4. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 16 June 2017), IV-10.

5. U.S. Army, "Gen. Raymond T. Odierno addressing the USMA class of 2013," *U.S. Army Worldwide News,* November 5, 2012, https://www.army.mil/article/90671/gen_raymond_t_odierno_addressing_the_usma_class_of_2013.

6. Department of the Army, TRADOC Pamphlet 525-3-1, *Multi-Domain Operations 2028*.

7. Jed Judson, "US Army capabilities integration chief talks multidomain ops," *Defense News,* October 8, 2018, https://www.defensenews.com/digital-show-dailies/ausa/2018/10/08/us-army-capabilities-integration-chief-talks-multidomain-ops/.

8. Scott King and Dennis Boykin, "Distinctly Different Doctrine: Why Multi-Domain Operations Isn't AirLand Battle 2.0," Association of the United States Army website, February 20, 2019, https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn%E2%80%99t-airland-battle-20.

9. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 6 October 2017), 1-2. Change 1 was issued on 6 December 2017.

Mr. Peter Baber is a program manager for identity intelligence with the Department of Defense. He served on a joint duty assignment as the Chief of the Identity Intelligence Project Office in the Defense Combatting Terrorism Center and deployed in support of establishing Combined Joint Task Force–Operation Inherent Resolve's identity intelligence capability. He served as a branch chief for the U.S. Army Identity Intelligence Division, a plank owner who deployed with, and later led, the Counterinsurgency Targeting Program.

Ms. Pamela Baker is currently in the Identity Intelligence Division with the Department of Defense. She provides analysis and production oversight and lends strategic support to the intelligence community. She has 15 years' experience in the identity intelligence enterprise.

LTC Mark Dotson (retired) is currently the Defense Forensic Science Center Technical Representative for the U.S. Army. While assigned to the Army, he led a team of intelligence planners implementing a portfolio of programs that evolved into identity intelligence capabilities supporting warfighters and later served as current operations officer for the identity intelligence program. Additionally, he deployed operationalizing biometrics and forensics capabilities as nontraditional intelligence, surveillance, and reconnaissance enablers.

Military Intelligence Brigade-Theater Support to Multi-Domain Operations in the Indo-Pacific Strategic Environment

by Colonel David P. Elsen, Major Travis Tyler, Major R. J. Custodio, and Major Michael A. Glover

Introduction

Today, the U.S. military faces dynamic challenges in the Indo-Pacific area of responsibility (AOR). The operational environment is arguably more complex than ever before. This complexity begins simply with demographics. The region contains 36 countries spread across 16 time zones. The region contains more than half the world's population, houses 24 of the 36 megacities (population centers with more than 10 million people) on Earth, and covers more than half the world's surface area. Three of the world's largest economies, seven of the largest militaries, and five of the United States' seven mutual defense agreement partners are all located in this theater.[1] The region is also extremely prone to severe weather patterns such as devastating tsunamis, volcanoes, and catastrophic earthquakes. When demographics are coupled with the unpredictable weather effects in the region, the complexity of the environment increases rapidly. These demographic, economic, and meteorological dynamics, combined with the rapid rate of technological change, add to the region's political and military complexity.[2]

Key Challenges and Threats in the Indo-Pacific

The 2018 U.S. National Defense Strategy emphasized four of the five national security threats reside in the Indo-Pacific region. These threats, particularly China and Russia, actively contest and leverage every domain to achieve great power status and reduce or eliminate United States influence within their near abroad. "Global proliferation of advanced military technology has eroded, to some degree, the advantage the U.S. and its military partners have held for decades, allowing adversaries to threaten use of the air, sea, land, space, and cyberspace domains."[3] Both states are actively competing against the U.S. military in an effort to achieve strategic standoff. Dramatic technological shifts created by unmanned capabilities, machine learning, artificial intelligence, nanotech, biotech, and big data are expanding military *hyper*-competition

The U.S. Indo-Pacific Command area of responsibility.

Map courtesy of U.S. Indo-Pacific Command

between geopolitical rivals. Much of these new technological tools depend on digital connectivity—with 8 billion devices connected to the internet in 2018 and a projected 50 billion by 2020—only increasing the already dangerous situation in cyberspace and its dependence on space assets for connectivity. Without a doubt, future conflict will be increasingly complex and distributed, involving actions across multiple domains by multiple military services, and at times simultaneously.[4]

It is evident that our strategic competitors have taken the information they learned through the study of our military doctrine and recent military operations to develop and employ capabilities that mitigate areas in which our military has enjoyed overmatch and that place our people, systems, and critical infrastructure at risk. They accomplish this through the employment of a wide array of layered antiaccess and area denial systems across all domains that provide standoff and limit our joint force's freedom of maneuver.[5]

In response, the U.S. Army unveiled its multi-domain operations (MDO) concept and rapidly evolved and adapted its doctrine to address this newly framed great power competition. Through MDO, the Army and the joint force seek to regain the ability to project forces into the theater and achieve convergence across all domains to defeat our adversaries. Furthermore, on 6 December 2018, the Army published TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028,* which provides guidance on how the Army must build capacity and capability to enable MDO by:

- Continuing to update the MDO concept and subsequent doctrine.
- Developing a modernization strategy that nests with the MDO concept and synchronizes with a joint approach to force development.
- Identifying and driving rapid solution development across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.
- Improving the operational integration of general-purpose forces and special operations forces, and with allies and partners.[6]

The introduction of MDO has provided the Army and its warfighting functions a blueprint on how to organize their formations, develop and integrate new capabilities, and train those formations. For example, the intelligence warfighting function is heavily invested in MDO through its support for the Intelligence, Information, Cyber, Electronic Warfare, and Space (I2CEWS) detachment; publishing of new doctrine; investment in deep sensing; and introduction of machine learning powered analytics. Within the intelligence warfighting function, the military intelligence brigade-theater (MIB–T) continues to be the Army Service component command's primary intelligence organization at the theater level and the focal point of the Army's multi-domain intelligence support throughout both the competition and the conflict phases.

500th MIB–T Support to Multi-Domain Operations

As an element of the joint force, Army forces conduct MDO to prevail in competition; penetrate and dis-integrate enemy antiaccess and area denial systems when necessary; and exploit the resultant freedom of maneuver to achieve strategic objectives (win) and force a return to competition on favorable terms.[7] The MIB–T is postured to provide multi-domain intelligence support to Army, joint, and coalition forces within a theater of operations[8] through collection and analysis across the intelligence disciplines, such as through the use of human intelligence/counterintelligence platforms, open-source intelligence, forward-deployed signals intelligence assets, and national collection. The MIB–T is equipped with a unique set of capabilities to support MDO and help set conditions by improving and developing required Army capability sets. The MIB–T is equipped to set the theater for intelligence and establish the intelligence, surveillance, and reconnaissance (ISR) dynamic forward posture. It stands ready to provide multi-domain intelligence.

Set the Theater for Intelligence

Doctrinally, MIB–Ts "provide the theater army with its foundational capabilities to set the theater for the intelligence warfighting function."[9] They do this in a number of ways, to include providing—

- intelligence (assessments, support to the combined operational/intelligence picture, graphic products, and persistent intelligence overwatch),
- integration (theater intelligence architecture and data sets),
- training (live environment training, mobile training teams, and subject matter experts), and
- support to the Army Service component command's theater security cooperation program and engagements.[10]

The 500th MIB–T assists the U.S. Army Pacific (USARPAC) G-2 in setting the theater for intelligence in all areas, enabling multi-domain intelligence support. Some key focus areas include the provision of the theater intelligence architecture backbone; the role of the theater analysis and

control element (ACE), to include providing the common intelligence picture; support to partner nation engagements; and the provision of discipline-specific theater entry requirements.

Intelligence Architecture Backbone. The 500th MIB–T, in coordination with the USARPAC G-2, maintains the Army Indo-Pacific intelligence architecture to provide consistent readiness for the Pacific theater of operations. The MIB–T serves as the architecture backbone of the intelligence enterprise in theater. These efforts connect rotational, aligned, and assigned forces entering the U.S Indo-Pacific Command (USINDOPACOM) AOR to the theater intelligence enterprise. They also provide forces with the ability to leverage U.S. Army Intelligence and Security Command capabilities in support of MDO. This enhances commander's decision making through access to timely, predictive intelligence and shared understanding of the multi-domain threat. Units deploying into the AOR rely on intelligence reach to access intelligence from joint forces, combatant commands, and the national intelligence community. The 500th MIB–T integrates regionally aligned, assigned, and rotational units early, in both exercise and operational planning cycles, to support shared understanding, streamline information sharing, and maintain readiness within the Pacific theater.

Theater Analysis and Control Element, Common Intelligence Picture, and Partner Nation Engagement. The 500th MIB–T, in coordination with the USARPAC G-2, provides the theater analytic capabilities in the form of the ACE. The ACE serves as the integration mechanism fusing intelligence across every intelligence discipline and every domain, across federated sites throughout the USINDOPACOM AOR. The analytic capabilities the MIB–T offers include the deployment of an expeditionary, configurable deployable intelligence support element in support of combined and joint operations while still maintaining analytic capabilities in both strategic support and operational support areas. The elements within the ACE maintain the common intelligence picture that feeds the joint operational picture, leveraging federated intelligence to include Reserve and National Guard units. Additionally, with web-based applications on both the SECRET Internet Protocol Router and the Joint Worldwide Intelligence Communications System, intelligence production is available using relatively minimal bandwidth. The MIB–T further provides support to building partner nation capacity and capabilities through subject matter expert exchanges and increasingly complex joint and combined exercises.

Photo courtesy of COL David Elsen

500th **MIB–T Soldiers provide analysis from the deployable intelligence support element during Exercise Pacific Sentry 19-3, U.S. Army Pacific's Joint Task Force Certification Exercise, June 2019.**

Theater Entry Requirements. As the MIB–T supports the Army and joint forces, specific requirements exist for all forces to connect to the MIB–T intelligence architecture backbone, ensuring units are consuming and benefiting from the daily intelligence produced by the theater ACE, across the multi-domain battlefield from the strategic support areas to the deep fight. The objective is to ensure no cold starts for joint and combined forces both in theater and in support of the theater. Across multiple intelligence disciplines (all-source, geospatial intelligence, signals intelligence, human intelligence, counterintelligence, and open-source intelligence), the 500th MIB–T provides specific theater entry requirements to facilitate connectivity, clear lines of mission and authority, and a continuous intelligence cycle of situational awareness and shared understanding of the threat.

Establish the Intelligence, Surveillance, and Reconnaissance Dynamic Forward Posture

The MDO concept requires the Army to develop or improve required Army capability sets. These capability sets include setting the theater through such activities as establishing basing and access rights, prepositioning equipment and supplies, and conducting preparatory intelligence activities. Additionally, aspects of MDO require the establishment of necessary authorities and permissions normally reserved for conflict or for higher echelons to operate in competition and rapidly transition to conflict. There is perhaps no better example of development and improvement in these capabilities than that of the MIB–T ISR dynamic forward posture.

Focused on the MDO tenet of calibrated force posture, the MIB–T establishes an ISR forward presence, as part of the "contact forces" forward deployed in theater, to provide warning intelligence, maintain an accurate and timely common intelligence picture of the threat across all domains, support competition phase operations in contested spaces/

environments, and be in position in the event of crisis or escalation. For all these reasons, ISR should not be held in reserve but rather be "always out front" in line with the Military Intelligence Corps motto. The ISR dynamic forward posture is supported by established and future basing and access rights and enables the achievement of positional advantage through prepositioned capabilities and support packages. The MIB–T establishes sensor and collection capacity forward to increase situational awareness of threat competitor activities taking place across and through standoff layers before transition to conflict, not after. Additionally, small processing, exploitation, and dissemination nodes positioned forward in theater mitigate the risks associated with monitoring these collection assets in the disconnected, intermittent, limited bandwidth environment expected given current threat capabilities. This initiative focuses on overcoming the challenges of gaining positional advantage and maneuver over strategic distance.

Furthermore, based in part on the geography in the Indo-Pacific theater, any newly established forward presence of ISR creates the requirement for coalition, cross-Service, and cross-domain coordination, breaking through historically stove-piped, domain-federated operational approaches. This coordination is essential in synchronizing collection across national, coalition, and other theater capabilities; in providing the necessary fidelity for the common operational and intelligence pictures; and in moving toward the synergy and convergence required for effective MDO.

Establishment of the MIB–T ISR dynamic forward posture further supports future integration of the multi-domain task force and its I2CEWS detachment through improved theater-wide baselining and situational awareness of adversary placement, posture, and activity.

Stand Ready to Provide Multi-Domain Intelligence

Multi-domain intelligence is the Army intelligence framework that increases the speed, precision, and accuracy of the intelligence process. Within the multi-domain intelligence framework, the MIB–T provides key support in the foundation layer, in managing and synchronizing layered collection, and in intelligence support to multi-domain targeting.

Foundation Layer—Redundant and Survivable Architecture. The MIB–T has a unique ability to collect, analyze, and track threat characteristics, the ground order of battle, and the doctrine of both partner nations and adversaries over many years. Such abilities enable the MIB–T to create and maintain a valuable database of intelligence regarding regional military forces, key military and political leaders, and the evolving doctrine and capabilities of regional military forces. Furthermore, critical to the targeting process is the Cross Domain Solution Suite and combat information needed on collateral networks, which the MIB–T will provide to support lethal and nonlethal effects. Of equal importance is the establishment of an agile, flexible, and converged architecture that leverages the Distributed Common Ground System family of systems.

Photo by U.S. Army SSG Shameeka R. Stanley

A military intelligence systems maintainer/integrator assigned to 715th Military Intelligence Battalion, 500th Military Intelligence Brigade-Theater (MIB–T), briefs the 500th MIB–T command team on communications equipment capabilities during training exercise Lightning Forge on the Island of Oahu, July 24, 2018.

Collection Layer—Layered Intelligence Collection. MDO will require layered, redundant, and complementary collection to enable cross-domain synergy when faced with the challenges of a hyper-contested, communications-degraded environment linking the network of sensors to the web of shooters. This increases the required speed of friendly recognition, decision, action, and reaction. In addition to its organic collection assets, the MIB–T must also leverage joint, coalition, and national assets in coordination with the USARPAC and USINDOPACOM collection plans. The required collection must occur across the terrestrial, aerial, and space layers, across all domains, and must encompass national-to-tactical capabilities. Furthermore, the MIB–T's ability to leverage nontraditional collection, including open-source

intelligence, to tip and cue more traditional sensors will be critical to the joint force success.

Intelligence Support to Multi-Domain Targeting. Intelligence support to multi-domain targeting is a central component of intelligence support to MDO and will help drive MDO writ large. In order for the MIB–T to effectively support targeting, a baseline needs to be established during the competition phase through robust intelligence preparation of the battlefield, determination of the ground order of battle, awareness of threat capabilities and disposition across all domains, and generation of indicators and warnings. Multiple units within the MIB–T perform these functions. These units include the theater ACE, organic TROJAN remote operations facility, composition 2 and 3 elements, and Joint Intelligence Operations Center formations that encompass the combatant command's larger intelligence enterprise, including at echelon corps and below. Key components of effective multi-domain intelligence support to targeting comprise—

- redundant, survivable architecture and communications pathways;
- layered collection;
- timely, often near-real-time reporting;
- focused analysis;
- and closely coordinated and rehearsed sensor-to-shooter battle drills, incorporating both lethal and nonlethal fires and across all phases from competition through conflict.

Conclusion

China and Russia actively contest and leverage every domain to achieve their strategic national objectives and compete against the United States military in an effort to achieve strategic standoff. With the advent of emerging technologies and threat competitor focus on employment of layered antiaccess and area denial systems across all domains, it is imperative that the Army evolve and adapt its warfighting techniques and build ground forces capable of maximizing deterrence and, if necessary, winning future wars. The MDO concept stands as a foundational guide for this iterative process. As part of this process, the MIB–T evolves in order to increase the speed of friendly recognition, decision, and reaction. With a focus on setting the theater for intelligence, establishing the ISR dynamic forward posture, and standing ready to provide multi-domain intelligence, the 500th MIB–T is uniquely equipped and postured to face the evolving threats in the Indo-Pacific theater.

Endnotes

1. Robert B. Brown, "The Indo-Asia Pacific and the Multi-Domain Battle Concept," *Military Review* 97, no. 5 (September–October 2017): 15.

2. Kyle McCreary, *The Multi-Domain Task Force (MDTF) and Intelligence, Cyber, Electronic Warfare, and Space (ICEWS) in US Army Pacific (USARPAC)* (Fort Shafter, HI: U.S. Army Intelligence and Security Command, January 14, 2019).

3. Forum Staff, "Unpredictable Behavior: Joint forces view multi-domain battle as key to future success," *Indo-Asia Pacific Defense Forum* 42, no. 4 (2017): 11.

4. McCreary, *The Multi-Domain Task Force.*

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

6. Ibid.

7. Ibid.

8. Department of the Army, Army Techniques Publication 3-93, *Theater Army Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 26 November 2014).

9. Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: U.S. GPO, 6 July 2018), 4-3.

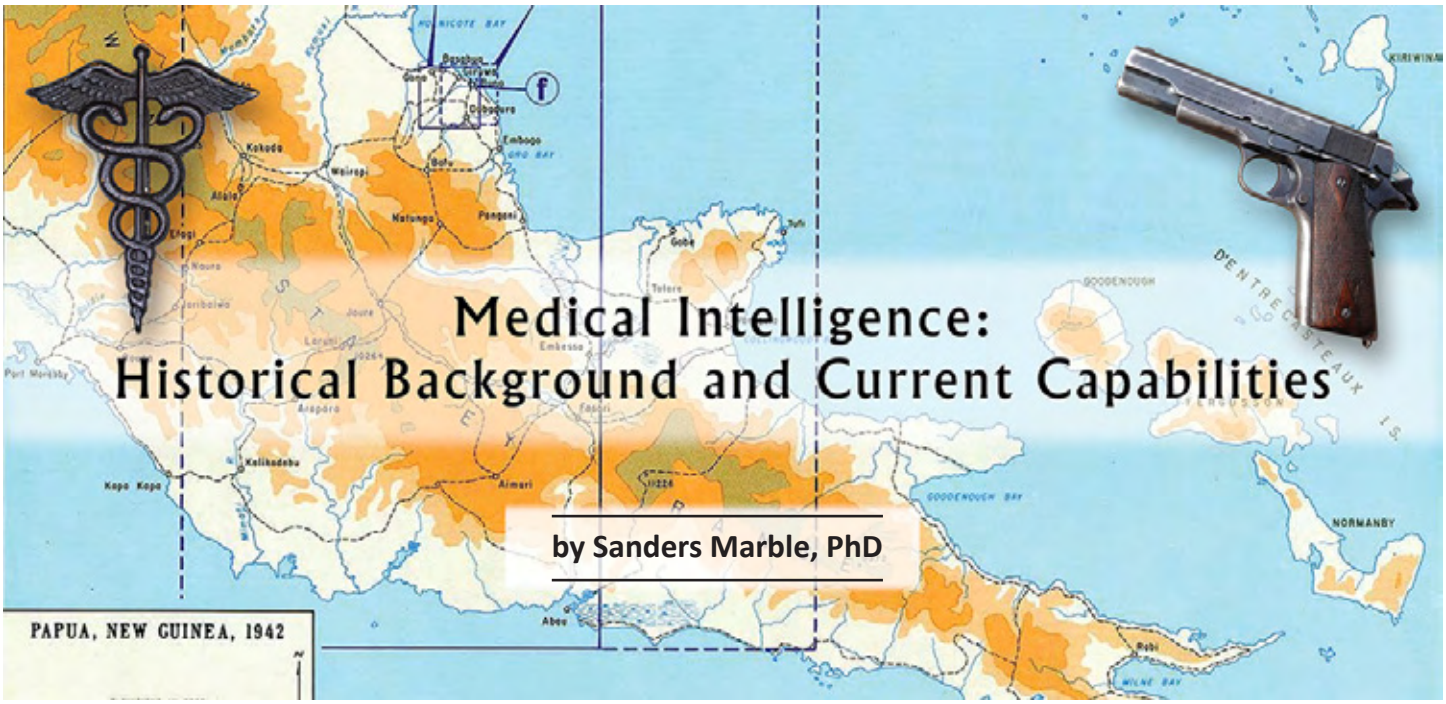
10. Ibid.; and Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019).

COL David Elsen is the Commander, 500th Military Intelligence Brigade-Theater (MIB–T), Schofield Barracks, HI. He has served more than 7 years with units focused on the Indo-Pacific region, including command of the 532nd Military Intelligence Battalion, Camp Humphreys, Republic of Korea.

MAJ Travis Tyler is the Plans and Exercises Chief, 500th MIB–T, Schofield Barracks, HI. He has served more than 4 years with units focused on the Indo-Pacific region and more than 4 years with MIB–T units focused on both the European and Indo-Pacific regions.

MAJ R.J. Custodio is the Executive Officer, 500th MIB–T, Schofield Barracks, HI. He has served more than 8 years with units focused on the Indo-Pacific region.

MAJ Michael Glover is the Operations Officer, 500th MIB–T, Schofield Barracks, HI. He has served more than 9 years with units focused on the Indo-Pacific region.



Medical Intelligence: Historical Background and Current Capabilities

by Sanders Marble, PhD

Introduction

Dr. Edward T. Wolf, sometimes known as E. Trowbridge, was going behind Japanese lines. The Army issued him a Colt .45 and a submachine gun. He wasn't looking to fight; he was hunting mosquitoes to know what diseases they spread. GEN Douglas MacArthur wanted intelligence on the diseases in Northern New Guinea, and men like Trowbridge had to establish the ground truth because, in September 1942, no medical intelligence organization existed to provide it. CPT Wolf boarded a 40-foot wooden fishing boat with five Filipinos as crew and traveled at night from the hastily built base at Milne Bay, on the eastern end of New Guinea, north and west along the coast up to Wanigela Bay and onward. The 32nd Infantry Division was shortly going to land somewhere on that remote jungle coast, and knowledge of endemic diseases and the insects that transmitted them would affect operations.[1]

Trowbridge's dangerous mission was necessary to gather the intelligence because nobody had thought ahead and had prewar medical intelligence.

Starting Medical Intelligence

In April 1941, months before Pearl Harbor, the chief of preventive medicine in the Office of the Surgeon General knew he didn't know enough and got an officer assigned to do medical intelligence work.[2] But nobody was trained for that work, and there was a whole world to cover. Finding people was a challenge. Even with the draft to provide manpower, nobody had any experience. And which part of the world? Priorities were a problem because the enemy had the initiative and the Allies repeatedly had to switch focus areas. They initially focused on the French colonies in the Caribbean because the Vichy French might give the Germans bases there. Next, the United States traded 50 old destroyers to the British in exchange for basing rights on various British islands, and it was necessary to identify the medical threats on those islands because American troops would be at risk. The first officers sent were sanitary engineers who provided detailed information about the water systems but very little about diseases. The Japanese attack on Pearl Harbor compounded these problems: now United States forces would be operating in the Pacific as well.

Despite the problems, the medical intelligence office (which had various titles during the war) contributed to 96 "Strategic Surveys" in 1942 alone, with only seven staff members. They knew the information was patchy, but it was something. They contributed it to the planners but had no idea how it affected operations. In 1943, the number of products dropped as the Allies gained the initiative and plans could be more deliberate instead of reactive. The staff grew, but unfamiliarity with languages remained an obstacle to understanding the worldwide operating environment. The Army worked with the Navy (the Air Force did not yet exist) on Joint Army-Navy Intelligence Studies and firmed up internal operating procedures. They developed a structure of collection, analysis, and dissemination, rather than a geographical one. The approach to sources became a bit more systematic: they combed through open-source medical literature; followed up personal contacts; and got information from the War Department G-2, Allies, prisoners, Office of

The collection, analysis, and dissemination of medical information of importance to our troops operating in all and any parts of the world.
—World War II definition of medical intelligence

Strategic Services, and sometimes operational forces. Only limited information came from the theaters because the intelligence officers there had never worked with medical intelligence, and medical officers had trouble getting on the intelligence staffs or intelligence field teams. They also had to decide how to cover foreign medical developments. Was a new surgical procedure or a new medicine an intelligence matter or a clinical matter? The final decision was that medical intelligence was about disease prevalence, not about how it was treated. The exception was biological warfare, which had such serious implications that intelligence and medical intelligence both covered all aspects: overlap was better than gap.[3]

By 1944, the medical intelligence "product" had changed to Technical Bulletins, Medical, known as TB MEDs. These included a section of recommended ways to safeguard troops' health. With the broad outlines of Allied strategy clear, it was easier to predict locations, and there was less wasted effort. Sometimes the TB MEDs were ready just before an operation (the report on France was printed in May 1944, only 34 days before D-Day), not allowing much time for review and intelligence to influence operations. Yet when the report was ready in time, it didn't necessarily influence operations: TB MED 20, the survey of the Mariana Islands, was ready 90 days before the invasion, and it identified dengue fever as a major risk. But insect-control teams were not prioritized for shipping space, and the invasion forces suffered around 4,000 dengue cases on Saipan alone before the bug-sprayers arrived and promptly broke the epidemic.[4] Intelligence was accurate and timely but might not influence plans.

Getting information to theaters could be as much of a problem as getting information from them. No established channels existed for medical intelligence, either in intelligence staffs or in medical staffs. Potential users did not know about medical intelligence, so they did not know to ask, and even the communication channels were unclear. A TB MED was likely to get to a medical unit, but would it get to the G-2 staff? One novel distribution channel was open-source publishing: since much of the information was public domain, a three-volume set of books titled *A Geography of Disease and Sanitation* was published, which could have been useful if they reached theaters in time.[5]

The Cold War

After World War II, sweeping changes occurred in U.S. defense and intelligence structures; however, the newly established Central Intelligence Agency did not receive the medical intelligence mission. Instead, it stayed with the Army, consolidated on behalf of all the services.[6] However, the office was downgraded: in 1946, the chief went from a lieutenant colonel to a major to a civilian.[7] (To be fair, that probably reflected the reduction in size of the military, and the position has since moved up to colonel.) On the plus side, a medical intelligence course was taught at the Army Medical Field Service School, and with the subject matter being intelligence, the student text was of course classified.[8]

Following World War II, a contingent of United States troops moved to Korea to disarm the Japanese occupation forces and began advising the fledgling Republic of Korea; therefore, the prevalent diseases were fairly well known by 1950 when the Korean War started and there was limited need for that part of medical intelligence. But some medical intelligence derring-do occurred during the Korean War. Communist troops were moving through Manchuria, where bubonic plague (i.e., the Black Death) was endemic. Reports from agents in North Korea of a plague-like outbreak alarmed American leaders because the disease could easily turn into a pneumonic form, spread by coughs and with nearly 100 percent mortality. In February 1951, a three-man team led by BG Crawford Sams, Medical Corps, went ashore behind Communist lines. On-site discussion with an agent cut through miscommunication. The disease was identified as hemorrhagic smallpox rather than bubonic plague, and therefore it was not necessary to get a blood sample from a Communist soldier (dead or alive).[9] Smallpox was bad, but the United States and United Nations forces had effective vaccines, so it would not be a problem.

After Korea, the medical intelligence office continued its desk-based work in Washington, DC. Through the Cold War, the name changed but the mission and manning stayed roughly constant, at around 30 military and civilian personnel, until the mid-1980s.[10] In March 1963, the bulk of personnel transferred to the Defense Intelligence Agency (DIA), with the Army retaining only some liaisons and special projects. Whatever their higher headquarters, the mission was

Photo courtesy of the National Museum of Health and Medicine

WRAIR-FEST entomologist performing field studies in Vietnam.

unchanged. For operations in Vietnam, only so much could be done from Washington. The literature about diseases in Southeast Asia was limited, and field studies (debriefing and blood samples from returning Special Forces personnel) were used during the period when U.S. forces were a limited number of advisors instead of line units engaged in heavy combat.[11] That was recognized as inadequate, and a medical research team was sent, but they were hospital-based and focused on clinical research. Because the counterinsurgency war would be fought in the countryside, a field capability was needed and a small unit with a long name was formed: U.S. Army Special Forces–Walter Reed Army Institute of Research Field Epidemiology Survey Team (Airborne), known as WRAIR-FEST. The Special Forces and Airborne designations were not formalities, and a 17-week training program prepared personnel, which included practical exercises with plague in New Mexico and leptospirosis at Fort Bragg, North Carolina. Deploying in September 1966, they wore green berets and were attached to the 5th Special Forces Group (Airborne), which gave them credibility and ready access to the network of Special Forces camps around Vietnam. While most of their work was determining the causes and transmission routes of diseases, they developed operational intelligence as well. In April and May 1967, they identified a new strain of malaria arriving in the Mekong Delta region of South Vietnam. It was a strain from North Vietnam, and it showed North Vietnamese Army troops were arriving. This medical intelligence arrived before any other intelligence.[12]

While the WRAIR-FEST was being organized, the Army also had a standardized Team QA, Medical Intelligence Detachment. This was only three personnel "for selective collection, initial examination, evaluation, and classification of technical and medico-military information and dissemination of intelligence derived therefrom."[13] Supposedly, there would be five per army in the field, 15 personnel just to provide medical intelligence, but only one went to Vietnam. The 521st Medical Detachment (QA) deployed by 1966, interrogating prisoners, examining captured supplies and equipment, and contributing to reports such as *Medical Causes of Non-Effectiveness among Viet Cong Troops*.[14]

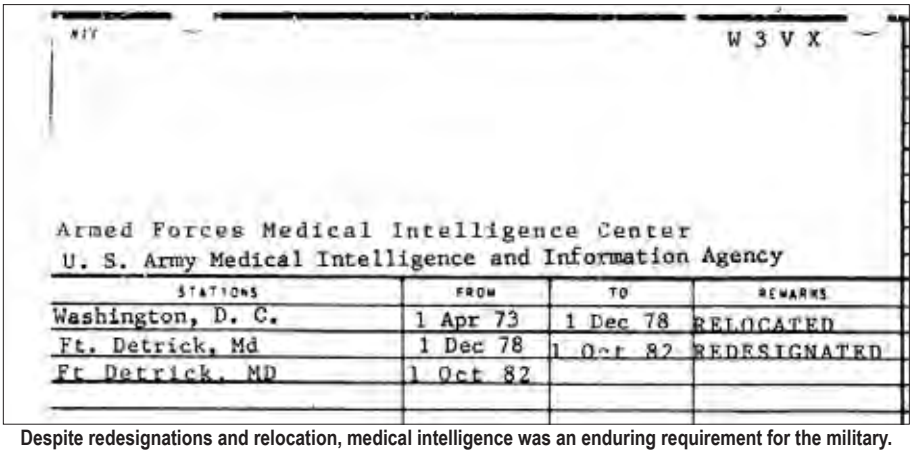
After Vietnam, medical intelligence again returned to Washington. DIA dropped medical intelligence, apparently to cut headcount, but the Army resumed the mission as the U.S. Army Medical Intelligence and Information Agency (USAMIIA). USAMIIA became solely responsible for Department of Defense medical intelligence, incorporating the general medical intelligence mission as well as the ongoing medical science and technology and medical materiel exploitation programs. DIA had begun keeping databases of medical facilities, which did not require medical expertise although evaluating capabilities did.[15] Another kind of field team was organized (again, at least on paper), the Team LP, Medical Technical Intelligence Team, as an intelligence unit rather than a medical one.[16]

Photo courtesy of the U.S. Army Medical Department Museum

Technical intelligence board of captured medical supplies, Vietnam.

Moving to the Intelligence Community

In 1982, USAMIIA became a joint organization, the Armed Forces Medical Intelligence Center (AFMIC), with the Navy committing resources. (Previously, the Navy had relied mainly on its Naval Medical Research Units.)[17] It was not part of DIA but had a DIA representative on its interdepartmental advisory panel and certainly worked collegially. Products included traditional reviews of diseases and medical capabilities in geographic areas, the medical part of intelligence preparation of the battlefield.[18] More topical material was pushed out in a "weekly wire" of concise assessments. AFMIC developed considerable expertise on biological weapons and warfare, something that had been considered as far back as World War II but had not been a major topic.



NIY W 3 V X

Armed Forces Medical Intelligence Center
U. S. Army Medical Intelligence and Information Agency

STATIONS	FROM	TO	REMARKS
Washington, D. C.	1 Apr 73	1 Dec 78	RELOCATED
Ft. Detrick, Md	1 Dec 78	1 Oct 82	REDESIGNATED
Ft Detrick, MD	1 Oct 82		

Despite redesignations and relocation, medical intelligence was an enduring requirement for the military.

Two minor areas became major areas during Operations Desert Shield and Desert Storm. The information on medical facilities was useful for targeting, so that U.S. and coalition forces did not hit hospitals (and such) and give Saddam Hussein a propaganda victory. The nascent Iraqi bioweapons program also generated lots of attention for AFMIC because it had the right information at the right time.

In 1992, AFMIC was transferred to DIA but continued its traditional work, providing information on the health risks in an area, for instance Somalia, as United States and United Nations forces tried to re-establish stability in that country.[19] Products and dissemination changed, and unclassified information was made available on CD, while "Medical Environmental Disease Intelligence and Countermeasures" became a web-distributed product, currently available as an app through the Medical Communications for Combat Casualty Care program.[20] AFMIC supported the military, congressional, and White House staffs, but most support was to operational forces.[21] As deployments have increasingly been to immature theaters, knowledge of diseases and medical facilities has become more important.

AFMIC, since 2008 the National Center for Medical Intelligence, is the only organization in the world with this comprehensive medical intelligence mission. They continue to provide integrated, all-source intelligence for the Department of Defense and other government and international organizations on foreign health threats and other medical issues to protect U.S. interests worldwide.

Endnotes

1. Dr. Edward T. Wolf's papers are at the John P. McGovern Historical Collections and Research Center, Houston Academy of Medicine–Texas Medical Center Library, Houston TX.

2. For World War II in general, see Gaylord W. Anderson, "Medical Intelligence," in *Preventive Medicine in World War II, Vol. IX, Special Fields*, eds. Robert S. Anderson

and Ebbe C. Hoff (Washington, DC: U.S. Government Publishing Office [GPO], 1969), 251–340.

3. For a personal account, see Carlo Henze, "Recollections of a Medical Intelligence Officer in World War II," *Bulletin of the New York Academy of Medicine* 49, no. 11 (November 1973): 960–973.

4. Mary Ellen Condon-Rall and Albert E. Cowdrey, *United States Army in World War II: The Technical Services: The Medical Department: Medical Service in the War Against Japan* (Washington, DC: U.S. Army Center of Military History, 1998), 234, 244. This is one book in a series of 79 volumes divided into multiple sub-series.

5. James Stevens Simmons, Tom F. Whayne, Gaylord W. Anderson, Harold MacLachlan Horack, and Ruth Alida Thomas, *Global Epidemiology: A Geography of Disease and Sanitation* (Philadelphia: J. B. Lippincott & Co., 1944, 1951, 1954).

6. Jonathan D. Clemente, "The Fate of an Orphan: The Hawley Board and the Debates over the Postwar Organization of Medical Intelligence," *Intelligence and National Security* 20, no. 2 (2005): 264–287, DOI: 10.1080/02684520500133935.

7. "Chronology of Army Medical Intelligence, 1941–1973," DigitalCommons@University of Nebraska–Lincoln, 1973, https://digitalcommons.unl.edu/dodmilintel/105/.

8. "Special Text, ST 8-30-1, Medical Intelligence, 1951," DigitalCommons@University of Nebraska–Lincoln, 1951, https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1058&context=dodmilintel.

9. This is from BG Sams' biographical file, Army Medical Department Center of History and Heritage, Fort Sam Houston TX. BG Sams wrote about his activities with sufficient panache to receive a Distinguished Service Cross.

10. "Brief History of AFMIC (Total Manpower)," DigitalCommons@University of Nebraska–Lincoln, 1992, https://digitalcommons.unl.edu/dodmilintel/106.

11. Louis T. Dorogi, "Notes on the Establishment of the United States Army Special Warfare Center (Airborne) Surgeon's Office," *Journal of Special Operations Medicine* 10, no. 4 (Fall 2010): 58–63.

12. Louis T. Dorogi, "The United States Army Special Forces–Walter Reed Army Institute of Research Field Epidemiology Survey Team (Airborne)," *Journal of Special Operations Medicine* 9, no. 2 (Spring 2009): 54–71.

13. Department of the Army, Field Manual 101-10-2, *Staff Officers' Field Manual, Organizational, Technical, and Logistical Data, Extracts of Tables of Organization and Equipment* (Washington, DC: U.S. GPO, 19 January 1965 [obsolete]).

14. Combined Intelligence Center Vietnam, Special Report 67-001, *Medical Causes of Non-Effectiveness among VC Troops* (7 July 1966).

15. Denis C. Kaufman, *Medical Intelligence: A Theater Engagement Tool* (Carlisle, PA: U.S. Army War College, 2001).

16. Department of the Army, Table of Organization and Equipment 30-600H, *Military Intelligence Organization* (Washington, DC: U.S. GPO, 15 July 1977).

17. This section draws heavily on Kaufman, *Medical Intelligence*.

18. Armed Forces Medical Intelligence Center, *Medical Capabilities Study: The Caribbean Area* (Washington, DC: Defense Intelligence Agency [DIA], 1990).

19. Armed Forces Medical Intelligence Center, *Operation Restore Hope: Health Risks and Countermeasures in Somalia* (Washington, DC: DIA, 1992).

20. "About the MC4 App," Army Medical Communications for Combat Casualty Care Resources, U.S. Army, https://www.mc4.army.mil/Mc4System/Apps.aspx.

21. Gerard Schumeyer, "Medical Intelligence…Making a Difference," *American Intelligence Journal* 17, no. 1/2 (1996): 11–15.

Dr. Sanders Marble has worked in various capacities for the Army Medical Department history program since 2003, including being the Command Historian at Walter Reed Army Medical Center. He is currently the Senior Historian, Army Medical Department Center of History and Heritage, U.S. Army Medical Center of Excellence, Fort Sam Houston, TX. Dr. Marble holds a bachelor of arts from the College of William & Mary and a master of arts and a doctorate from King's College, University of London. He has written a variety of books, articles, and chapters on medical history.

Keeping Intelligence Professionals Engaged

by Lieutenant Colonel Michael Norton

Introduction

LTG Scott D. Berrier, the Army's Deputy Chief of Staff for Intelligence, G-2, challenged U.S. Army intelligence organizations to find unique ways to keep intelligence professionals engaged in their craft. With deployment opportunities decreasing after more than 18 years of combat operations, it is up to leadership at all levels to accept this opportunity and share institutional knowledge and experience with the younger force. Failing to leverage lessons learned will have detrimental effects on our Army.

Collective experience has taught us that human intelligence (HUMINT) collection is one of those skillsets that can deteriorate if not exercised continuously. The U.S. Army Africa (USARAF)/Southern European Task Force (SETAF) G-2X[1] accepted LTG Berrier's challenge and developed a program to effectively employ HUMINT collectors from U.S. Forces Command (FORSCOM) units using U.S. Africa Command (USAFRICOM) delegated Defense HUMINT Executor authorities. This employment allows HUMINT collectors the opportunity to execute their craft supporting real-world operations, eliminating the need to be forward deployed. Overall, this will increase readiness while allowing collectors to remain operationally engaged.

This article identifies the process used to effectively employ continental United States (CONUS) based HUMINT collectors to answer Army Service component command (ASCC), combatant command, and national-level intelligence requirements in order to help set the theater in the USAFRICOM area of responsibility (AOR).

Mission and Lines of Effort

USARAF/SETAF provides mission command, protects the force, sets the theater, conducts security force assistance, and supports joint and international partners in order to achieve USAFRICOM and U.S. Army Campaign Plan objectives. The organization executes that mission by focusing on six lines of effort.[2]

1. Strengthen partner networks.
2. Strengthen partner capacity.
3. Enable operations.
4. Maintain readiness.
5. Protect U.S. persons and facilities.
6. Set the theater.

As the USARAF Commanding General's senior intelligence officer, the Assistant Chief of Staff, G-2, focuses on ensuring intelligence drives operations for the commander. This vision includes setting the intelligence theater. Nested in the overall plan, the USARAF G-2X has focused on increasing collection and collection opportunities by opening doors across the African continent. Currently, there are 2,078 U.S. personnel across Africa supporting numerous theater security cooperation events.

As the ASCC responsible for Africa, USARAF plays a critical role in setting the theater on the African continent by actively building partner capacity and executing theater security cooperation events. These events focus on ensuring our African partners can contribute to regional security throughout the continent. Working by, with, and through our various partners, USARAF is prepared to respond throughout the African continent to execute contingency operations.[3] Intelligence support to those engagements and our partners focuses on setting the theater. Setting the theater "describes the broad range of actions conducted to establish the conditions in an operational area for the execution of strategic plans."[4] We accomplish this task by employing intelligence professionals in garrison and in a forward-deployed capacity under the authorities of Title 10 (Armed Forces) and Title 50 (War and National Defense) of the U.S. Code.

To ensure successful operations, USARAF maintains communication with country teams across the 53 countries inside the USAFRICOM AOR in order to answer commander's requirements. In addressing this vast AOR, USARAF identified gaps in collection and used those gaps to open collection opportunities. The intelligence theater in Africa is immature; in order to establish conditions to help set the theater, USARAF recognized unique ways to address the problem set. Detailed below are those opportunities that have led to the employment of CONUS-based collectors.

Foundation

In 2014, FORSCOM established a memorandum of agreement with each ASCC. This agreement allowed the ASCC to request and fund FORSCOM HUMINT collectors in order to execute operational missions in their respective combatant command AOR.[5] With the reduction in overseas contingency operations and newly assigned regionally aligned forces, FORSCOM HUMINT collectors were identified as being in a unique position to support operations at home station and forward deployed. This allows HUMINT collectors an opportunity to stay engaged and use their perishable skillset. USARAF signed the memorandum of agreement in 2015, and the agreement continues to serve as the foundational document for the successful employment of CONUS-based collectors.

Identifying and Addressing Gaps

USARAF's mission allows for year-round engagements throughout the USAFRICOM AOR. An assessment of the theater revealed intelligence gaps, including that U.S. Army personnel were supporting missions across the AOR without receiving comprehensive intelligence support. One such unit is the ordnance company (explosive ordnance disposal) based in Fort Hood, Texas. This unit provides counter-improvised explosive device training to select African partners. The unit deploys from CONUS directly to the USAFRICOM AOR, conducts the assigned mission, and redeploys to home station. USARAF would then deploy HUMINT collectors from Vicenza, Italy, to Fort Hood, Texas, to execute collection under the Foreign Military Intelligence Collection Activities (FORMICA) program.

Understanding the strain on resources, USARAF worked closely with FORSCOM and assisted in drafting an operations order that would allow for elements of III Corps, located on Fort Hood, to conduct the FORMICA mission on behalf of USARAF. HUMINT collectors, as internally tasked by III Corps, provide FORMICA pre-briefings to the unit before deployment. Once the unit returns from its mission, the same collectors then debrief the unit and begin the report writing process. Reports from this collection are routed through the USARAF G-2X for pre-publication review and publication to the intelligence community. This plan conserved resources by preventing expensive travel from outside CONUS while employing FORSCOM collectors in their own backyard. Most importantly, it directly answered LTG Berrier's challenge to keep the intelligence force engaged.

U.S. Military Observer Group

The U.S. Military Observer Group serves as the staff agent for Secretary of the Army's Executive Agent functions providing oversight, training, equipment, logistics, and administration support to U.S. military observers, individuals, and special teams serving in United Nations missions. The U.S. Military Observer Group provides support to Secretary of Defense approved positions within six United Nations missions, which the Office of the Secretary of Defense has directed as the number one allocation requirement. Currently, there are six locations across the USAFRICOM AOR:

U.S. Navy Photo by MC2 (SW/AW) Evan Parker

A Zambian soldier talks through troop positioning with a United States Army Africa regionally aligned forces training advisor during an ambush response training scenario. The training is in preparation for the Zambian troop's upcoming deployment supporting the United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic.

- ✦ United Nations Support Mission in Libya located in Tunis, Tunisia.
- ✦ United Nations Multidimensional Integrated Stabilization Mission in Mali located in Bamako, Mali.
- ✦ United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic located in Bangui, Central African Republic.
- ✦ United Nations Mission in the Republic of South Sudan located in Juba, South Sudan.
- ✦ United Nations Organization Stabilization Mission in the Democratic Republic of the Congo located in Goma, Democratic Republic of the Congo.
- ✦ United Nations Mission for the Referendum in Western Sahara located in Laayoune, Western Sahara.

These unique missions, spread across a continent that does not support intracontinental travel, presented a significant challenge for USARAF. How do we leverage these U.S. Army entities to help set the theater and answer commander's requirements? In working with the Military Intelligence Readiness Command, USARAF began employing the 337th Military Intelligence Battalion (MI BN) that is geographically aligned to the USAFRICOM AOR. 337th MI BN collectors would travel to the Military District of Washington and provide counterintelligence and HUMINT pre-briefings and then subsequent debriefings twice a year. Many of the intelligence information reports from this collection opportunity have been briefed at the most senior levels of the Department of Defense.

Lack of Serialized Reporting

USARAF, in direct coordination with U.S. Special Operations Command (USSOCOM), identified a significant gap in serialized reporting and developed a plan to address the deficiency. Executing worldwide authorities, USSOCOM is at the tip of the spear helping to shape the environment and deter violent extremist organizations throughout Africa. USARAF collectors are working with select organizations within USSOCOM, via a memorandum of agreement, to convert these interrogation reports to serialized intelligence information reports for publication and intelligence community consumption.

Units Involved

USARAF G-2X personnel traveled extensively to engage commanders and staffs at multiple levels, including FORSCOM; III Corps; 3rd Brigade Combat Team, 101st Airborne Division; 504th Expeditionary-Military Intelligence Brigade (E–MIB); and 337th MI BN (Reserve) in order to "sell" the concept of keeping intelligence professionals engaged. While commanders were eager to participate, they had to find the right balance between this opportunity and steady state operational requirements. USARAF worked exhaustively to demonstrate the value generated from these unique opportunities and highlight the national-level impact of these operations. USARAF was assigned a regionally aligned unit from Fort Campbell, Kentucky. Currently, the 3rd Brigade Combat Team, 101st Airborne Division, is filling this role. This unit provided HUMINT collection from a forward-based location on the African continent, at their home station in CONUS, and they sent a liaison officer to serve in the USARAF G-2X. The primary focus for the liaison officer is managing their unit's collection efforts. However, the USARAF G-2X creates professional development opportunities, including travel to the combatant command and to the African continent, to provide senior-level mentorship to their deployed collectors. This relationship helps build well-rounded intelligence professionals for our Army. USARAF worked, via a memorandum of agreement, to engage many other FORSCOM units, including III Corps, 1st Armored Division, and 504th E–MIB. USARAF has also been successful employing the 337th MI BN (Reserve).

Challenges Faced

While the hard work and dedication of professional individuals result in the achievement of success, throughout the process challenges arise that slow progress. In hindsight, these challenges were minor; however, as with anything new, they made our unit pause to find feasible solutions. Detailed planning, open communication, and continuous refinement will allow the unit to address any challenge without affecting mission support.

Operationalizing Regionally Aligned Forces. The first challenge was specific to regionally aligned BCT employment and was a result of a lack of specified tasking from FORSCOM through the division, brigade, and specific battalions. The BCT would step in and provide internal guidance that was incongruent with the collection efforts the USARAF G-2X was trying to accomplish. Orders would flow from USARAF to the BCT, routed through FORSCOM, and each level would interpret them differently. This led to a delay in addressing the collection mission.

Initially, regionally aligned BCTs are not dedicated to the ASCC until they receive orders. They have competing requirements that must be addressed. Educating leaders at all levels was crucial to overcoming this challenge. It was clear that while the regionally aligned BCT was under the operational control of the ASCC, what was unclear and not defined was the technical authority to employ HUMINT forces. The USARAF G-2X worked with FORSCOM and the subordinate corps and division to ensure guidance was clear so as not to affect the mission.

In order to fix this in the future, we recommend the following steps. Once the command identifies the regionally aligned unit, the ASCC assumes operational control and is granted direct liaison; then the regionally aligned unit, in coordination with the ASCC, should conduct an internal military decision-making process and receive guidance directly from the ASCC. This approach will prevent misinterpretation of the higher-level commander's intent.

Serialized Reporting. The second challenge involved serialized reporting. The USARAF G-2X wanted to increase serialized reporting throughout the intelligence community by employing any collectors willing to execute the mission. Because the memorandum of agreement between the ASCC

and FORSCOM is not a tasking document, USARAF relied on FORSCOM to task their subordinate units to execute the mission. The authorities for collection were clear upon publication of orders assigning the mission. There were some additional opportunities, discussed above in the "Lack of Serialized Reporting" paragraph, which made the USARAF G-2X have to "sell" the bigger picture to each participating unit. Socializing these opportunities, down to the battalion level, provided an increase to participation and production.

Recommendations

From an ASCC perspective, reaching out to FORSCOM and leveraging the memorandum of agreement is a great start to get more intelligence professionals engaged. If your unit is below the ASCC level, we recommend reaching up and finding a way to participate in the continuing development of your unit's capabilities. Using live environment training opportunities via Foundry will help the unit gain reps and sets that directly lead to overall enhanced abilities for our Army. The author will work to establish a synchronization meeting across the ASCCs to facilitate the sharing of ideas, best practices, and lessons learned as they pertain to this subject. This synchronization will allow a more in-depth discussion on the topic at the classified level.

Increasing situational understanding and setting conditions for mission success are the primary goals of intelligence collection. This focus ultimately leads to a better-informed commander and increases overall unit effectiveness. While each theater has its own unique challenges, many of these challenges can be overcome by exploring opportunities to increase collection. Capturing and sharing lessons learned will create a solid foundation by which our Army, and its Soldiers, can build on in the future. Employing intelligence professionals both inside and outside your organic unit will serve to enhance the force, maintain mission readiness, and keep intelligence professionals engaged. LTG Berrier, USARAF accepted your challenge and will continue to lead the way for our intelligence professionals.

Endnotes

1. The G-2X is the U.S. Army counterintelligence and human intelligence staff element.

2. U.S. Army Portal, U.S. Army Africa Intelink, accessed 4 November 2019, http://www.usaraf.army.mil/.

3. Department of the Army, Field Manual 3-94, *Theater Army, Corps, and Division Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 21 April 2014), 2-1.

4. Department of the Army, Army Doctrine Publication 4-0, *Sustainment* (Washington, DC: U.S. GPO, 31 July 2019), 2-4.

5. Department of the Army, *Memorandum of Agreement between U.S. Army Forces Command and U.S. Army Africa for Mutual Support for the Conduct of Human Intelligence Operations*, 15 February 2015.

LTC Michael Norton is the Chief, G-2X for U.S. Army Africa/Southern European Task Force stationed in Vicenza, Italy. His previous assignments in this field include Deputy G-2X, U.S. Army Central, and Chief, CJ-2X for Operation Inherent Resolve. He most recently served as an interagency fellow assigned to the Central Intelligence Agency.

Federated Technical Control and Analysis Elements: Setting the Theater for Cryptologic Warfighters

by Captain Thomas Mahoney

Strategic Context—Origins of a Federated System

The 2018 National Defense Strategy describes "an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations."[1] Aggressive traditional powers, rogue regimes, proto-states, and violent extremist organizations threaten the post-World War II international order.[2] To address this increased complexity and uncertainty, the U.S. Army, as part of a joint force, postures itself to transition rapidly from a state of competition to armed conflict and then back to competition under enhanced and improved circumstances.[3] During periods of competition, the Army prepares the operational environment for potential transition to armed conflict by setting the theater.[4]

At the core of the intelligence warfighting function, the U.S. Army Intelligence and Security Command (INSCOM) and its subordinate military intelligence brigades-theater (MIB–Ts) set the globe and set the theater, respectively. This responsibility occurs in advance through a combination of preparatory intelligence activities and the establishment of authorities and permissions normally reserved for periods of conflict.[5] Posturing Army or joint forces to rapidly transition from competition to conflict necessitates that the intelligence warfighting function execute these analytic and administrative functions for each of the individual intelligence disciplines.

Within the signals intelligence (SIGINT) discipline, technical control and analysis elements (TCAEs) perform these critical functions. Currently, INSCOM maintains the Army technical control and analysis element (ATCAE) at the National Security Agency headquarters. In March 2019, the ATCAE hosted a forum to discuss how best to enable Army cryptologic forces to address the emerging challenges identified in the Army's multi-domain operating concept. As a direct result of the ATCAE forum, INSCOM is undertaking a major initiative to create a federated system of TCAEs, arrayed across echelons. The federated TCAEs will deliver the needed technical support to Army cryptologic forces around the globe, ensuring they possess the organizational agility and flexibility to answer any requirement, in any domain.

History and Authorities

The ATCAE traces its origins back to the 1970s and 1980s, when the Deputy Chief of Staff for Intelligence directed its formation to "provide SIGINT operational support to tactical SIGINT units" in a response to merging the Army Security Agency into INSCOM. Over the decades, the roles and functions of the ATCAE adjusted to meet emerging requirements and needs. As shown in Figure 1, in 2012 the ATCAE disbanded and reorganized into the Global Operations Center–SIGINT. This reorganization was part of a broader INSCOM initiative to establish an overarching capability that was similar to an analysis and control element in support of deploying units. The system comprised Global Operations Centers for each intelligence discipline, answering to a prime Global Operations Center located at the National Ground Intelligence Center. As conditions changed and the Army and national focus shifted to a future fight executed across all domains, the need for TCAE roles and functionality to return became clear. To meet this requirement, INSCOM disbanded the Global Operations Center–SIGINT in 2017 and reconstituted the ATCAE in its place.[6]

Figure 1. TCAE Reorganizations from 1986 to Present

TCAEs derive their roles and authorities from the INSCOM Commanding General, who functions as the principal Army Service cryptologic component.[7] The Director, National Security Agency/Chief, Central Security Service, as the

responsible officer for all cryptologic activities, delegates the authority to conduct cryptologic operations to each of the Service cryptologic components. As the Army Service cryptologic component, the INSCOM Commanding General exercises his authority to set individual theaters for cryptologic operations by setting the globe for all Army units performing a SIGINT mission.[8] As the strategic environment evolves and the national focus shifts from counterterrorism and counterinsurgency to global competition and conflict, contested across all domains, INSCOM's federated TCAE initiative postures Army cryptologic forces to provide effective intelligence support to any operation or contingency.

Figure 2. Timeline for Federated TCAEs

Implementation of a Federated TCAE System

Department of the Army G-2's SIGINT strategy served as the catalyst for INSCOM's federated TCAE initiative.[9] Consideration of emerging requirements, resurgence of pacing threats, and a shift toward multi-domain operations drove the decision to distribute TCAE functionality across echelons by way of a federated system of TCAEs. INSCOM's federated system establishes TCAEs at the Army, theater, and operational level.[10] The ATCAE distributes technical control (administrative) and technical production (analytic) functions and responsibilities to the TCAEs at subordinate echelons, ensuring that Army cryptologic forces are properly enabled, regardless of location or mission.

Following guidance from the INSCOM Commanding General, MIB–Ts aligned to each theater reorganized their organic cryptologic personnel and resources to establish theater TCAEs (TTCAEs). Dedicated to enabling cryptologic operations within their theater, these TTCAEs set the foundations necessary to exercise TCAE functionality. In March 2019, the ATCAE hosted a forum at the National Security Agency-Washington to discuss the implementation of INSCOM's federated TCAE system initiative. The Commanding General reiterated the importance of the federated TCAE and issued instructions for MIB–Ts to establish TTCAEs and integrate them into the federated system. As shown in Figure 2, each TTCAE participates in a certification exercise to assess its initial operational capability and they should reach full operational capability by July 2020.

Certain regions or operations will also establish operational TCAEs (OTCAEs). These OTCAEs are responsible for and enable cryptologic forces aligned to or involved in their operation. The first OTCAE has been established as part of the 501st MIB–T. The OTCAE will synchronize efforts with the Army Pacific TCAE, passing authorities and responsibilities for Army cryptologic forces as they transition from theater into the specific operation. As shown in Figure 3 (on the next page), the Army National Guard and Army Reserves are also establishing TCAEs to enable cryptologic operations within their respective components. The Army National Guard-TCAE and the Army Reserve-TCAE will work closely and be collocated with the ATCAE to synchronize and enable Army cryptologic operations holistically.[11]

TCAE Core Functions

TCAEs at every echelon enable compliant and effective execution of Army cryptologic operations.[12] To provide the maximum level of support to a commander's priorities, SIGINT requires integration of collection, storage, and analysis across echelons, from tactical to national, as part of the U.S. SIGINT system. To accomplish this, TCAEs task organize into three lines of effort:

- Exercise technical control.
- Generate technical production.
- Enable operational readiness.[13]

These lines of effort ensure Army cryptologic forces have access to the U.S. SIGINT system, knowledge of the signals environment and threat, and the tradecraft necessary to execute their mission.[14]

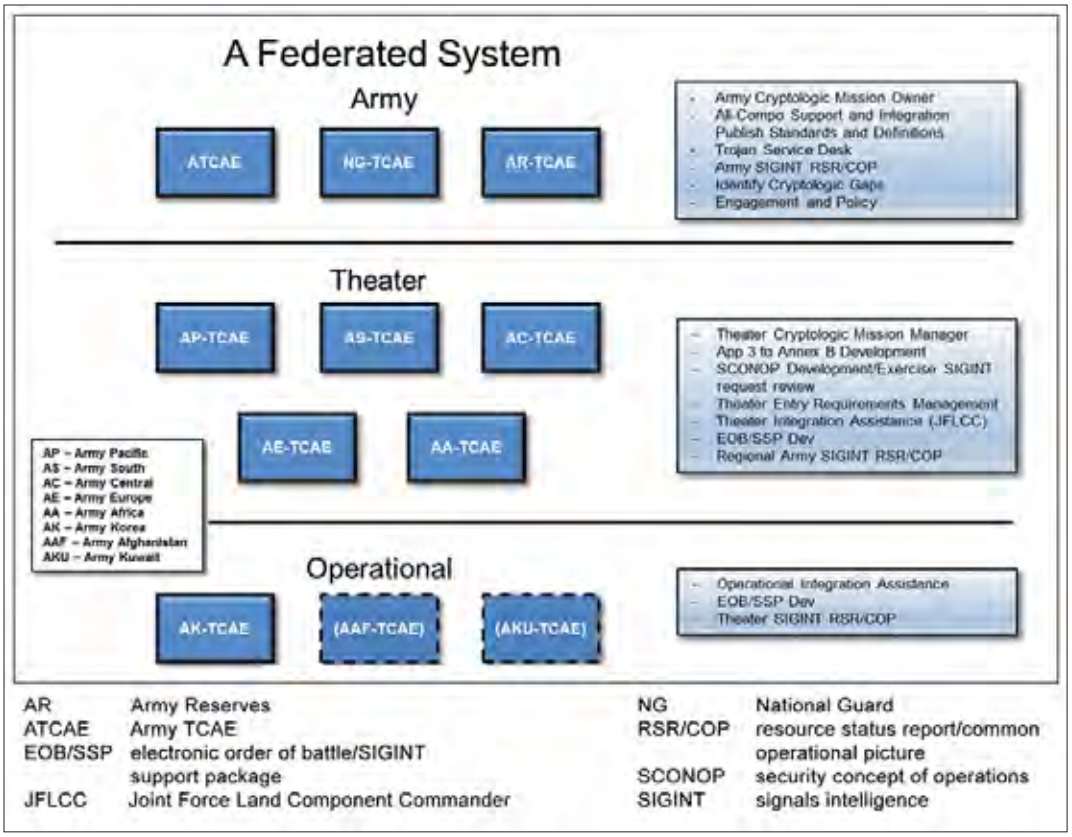


Figure 3. TCAEs as Part of a Federated System

Technical Control

In order to access the U.S. SIGINT system, cryptologic forces must comply with laws, regulations, and executive orders that drive National Security Agency policy. The ATCAE serves as the cryptologic mission owner for access to national databases. In this role, the ATCAE exercises technical control of all Army units operating under the SIGINT operational tasking authority.[15] The multi-domain operating concept identifies the need for Army units to conduct detailed tactical and operational intelligence preparation of the battlefield, including cryptologic operations, during periods of competition.[16] The Army units, as part of a joint, interagency, and multinational team, must be enabled with the necessary authorities to operate in the electromagnetic spectrum and cyberspace.[17] The ATCAE's technical control section bears the responsibility to ensure that Army units are postured to execute their respective SIGINT missions compliantly.[18] They secure the Army's necessary SIGINT authorities and entitlements to support Army cryptologic forces through all phases of an operation (Figure 4).

TTCAEs and OTCAEs serve as anchor points for all Army cryptologic operations within their theater or operation. Army cryptologic forces coordinate access to the U.S. SIGINT system and mission authorizations with their respective TTCAE/OTCAE. Units submit all required documents and certifications to secure the SIGINT authorities necessary to satisfy their commander's priority intelligence requirements. TTCAEs assist with the documents and certifications and then exercise technical control of the cryptologic missions. The technical control encompasses both the mission management (administrative requirements) and data flow management (technical connectivity requirements). TTCAEs also work closely with the Army Service component commands to articulate cryptologic requirements clearly within theater entry requirements. This ensures that Army forces arrive in theater ready and able to execute their cryptologic mission.

The ATCAE's technical control section supports the federated system of TCAEs with two 24-hour watch desks that monitor network access and adjust cryptologic missions in support of command requirements. They also manage a SIGINT common operational picture, network access support, and resource status reports.[19] The TTCAEs and OTCAEs feed their own common operational pictures and resource status reports to the ATCAE for inclusion in the global Army common operational picture and resource status reports. This information provides situational awareness and understanding of capabilities and capacity, critical to leaders and decision makers at every echelon.

Figure 4. Technical Control Functions

Technical Production

While technical control enables Army cryptologic forces with the technical access and authorities necessary for their mission, technical production focuses on technical

intelligence and tradecraft development.[20] Technical production requirements derive from Army Service component command priorities, as well as operational and contingency plans. These requirements focus technical production on how best to enable cryptologic forces. At the theater level, technical production centers around—

- SIGINT support packages describing the signals environment in a specified region.
- Electronic order of battle focused on the threat's communications and emanations within the electromagnetic spectrum.
- Working aids that enable Army cryptologic forces to more effectively execute their mission.

Additionally, if an Army unit identifies tradecraft gaps or the need for tailored SIGINT training or tradecraft, the TTCAE can reach out to the ATCAE's technical production section. The ATCAE technical production section is able to leverage organizations and entities from across the U.S. SIGINT system and intelligence community to develop needed tradecraft solutions. They then export it to the force through mobile training teams, digital training venues, and whatever means best support the forward cryptologic elements.[21]

Operational Readiness

Technical control and technical production feed operational readiness. Together, they enable TCAEs to ensure that Army cryptologic forces around the globe possess the authorities, accesses, and knowledge necessary to execute their respective SIGINT missions. The TTCAEs ensure that theaters are set for rotational units, regionally aligned forces, time-phased force deployment data units, and any other cryptologic forces. Close collaboration between the theater and Army TCAEs ensures that Army cryptologic forces are operationally ready, both from a technical control perspective and from a situational understanding and tradecraft perspective. The federated system creates a mutually supportive relationship—vertically from strategic to theater to operational, and horizontally across cryptologic forces aligned against a mission or operation. The federated TCAE system establishes the foundations for the SIGINT discipline of the intelligence warfighting function to fight and win, regardless of threat, across domains, in an environment where all domains are contested.

Additional Resources

The ATCAE offers additional resources, including a series of ATCAE publications available on milSuite. Access https://login.milsuite.mil/ and enter "ATCAE" in the Search field (common access card login required).

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://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

2. Ibid.

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

4. Ibid., xi.

5. Ibid., 17.

6. Department of the Army, Army Technical Control and Analysis Element (ATCAE) Publication (Pub) 1-0, *ATCAE Charter* (Fort George G. Meade, MD: May 2018), 2 (common access card [CAC] login required).

7. Department of the Army, Army Techniques Publication 2-22.6, *Signals Intelligence Volume II: Reference Guide* (Washington, DC: U.S. Government Publishing Office, 20 Jun 2017), 2-6 (CAC login required).

8. Ibid.

9. Department of the Army, *The United States Army Signals Intelligence (SIGINT) Strategy*, 25 June 2018.

10. Department of the Army, ATCAE Pam 1-0, *The TCAE* (Fort George G. Meade, MD: November 2018), 4 (CAC login required).

11. Ibid.

12. Ibid., 4.

13. Department of the Army, ATCAE Pub 1-0, *ATCAE Charter,* 16.

14. Department of the Army, ATCAE Pam 1-0, *The TCAE,* 3.

15. Department of the Army, ATCAE Pub 1-0, *ATCAE Charter,* 16.

16. Department of the Army, TRADOC Pam 525-3-1, *The U.S. in Multi-Domain Operations,* 27.

17. Ibid., 28.

18. Department of the Army, ATCAE Pub 1-0, *ATCAE Charter,* 21.

19. Ibid., 21–22.

20. Ibid., 29.

21. Ibid., 30.

CPT Thomas Mahoney serves as the officer in charge of technical production within the Army technical control and analysis element, 704th Military Intelligence Brigade. Past assignments of note include command of Headquarters and Service Company, Eighth Army; command of C Company, 304th Military Intelligence Battalion; and two deployments to Iraq.

Echelons Corps and Below Technical Control and Analysis Cell Concept

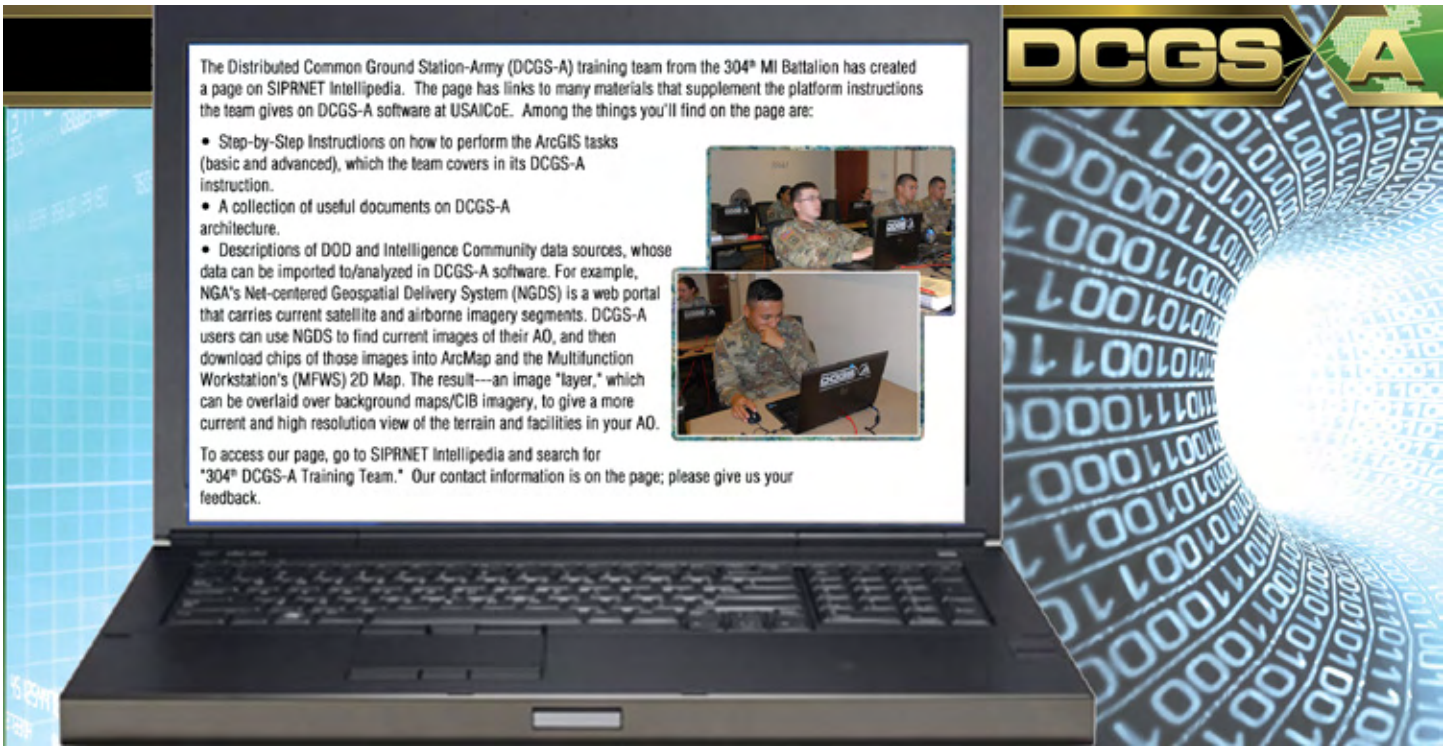
Signals intelligence (SIGINT) elements at the corps, division, brigade combat team, and expeditionary-military intelligence brigade (E–MIB) could form technical control and analysis cells (TCACs). These TCACs would perform administrative functions that ensure subordinate units' adherence to cryptologic access requirements, as well as staff functions that ensure SIGINT integration into operations.

The TCAC will provide technical control, in-depth analysis, integration, and synchronization of SIGINT operations in a distributed environment to de-conflict ongoing national-to-tactical SIGINT operations and to maximize support to the commander through access to the SIGINT enterprise. These actions involve coordination with other intelligence organizations and agencies, both in theater and through intelligence reach, to ensure their SIGINT operations do not conflict with other organizations'/agencies' planned SIGINT operations. The TCAC also creates target packages for SIGINT collection missions and recommends targets for action to the commander. The TCAC conducts detailed analysis to provide actionable intelligence for the commander.

Subordinate to the TCAC are the SIGINT collection teams. These teams provide SIGINT collection, exploitation, and limited analysis to generate actionable intelligence. They detect, track, and locate targets and provide SIGINT support to electronic warfare and cyberspace operations in support of missions within assigned areas of the corps and division area of operations.

At both the corps and the division, the TCAC will be located within intelligence and electronic warfare battalion (corps)/(division) multi-domain military intelligence (MI) detachments of the E–MIB. These detachments conduct multi-discipline intelligence analysis, targeting, and battle damage assessment; SIGINT collection support to electronic warfare and cyberspace operations; and expeditionary processing, exploitation, and dissemination.

At the brigade combat team, the TCAC will be an element of the MI company's intelligence collection platoon.



Military Intelligence Civilian Excepted Career Program as a Career Field

by Mr. Ricardo Romero

Introduction

The Military Intelligence Civilian Excepted Career Program (MICECP) is an Army Civilian intelligence program that provides expert support to intelligence organizations worldwide. The U.S. Army Intelligence and Security Command executes MICECP through the Commander, U.S. Army Field Support Center. AR 690-950-4, *Military Intelligence Civilian Excepted Career Program*, governs the execution and implementation of the program. The regulation further prescribes the policy and procedures for the hiring, training, career development and management, appraisal, recruitment, and employment of MICECP employees engaged in foreign counterintelligence (CI), tactical, operational, and strategic human intelligence (HUMINT), and other specialized technical intelligence collection and operational support functions. AR 690-950-4 supplements other applicable regulations on Army Civilian personnel management.

Background

In 1956, the U.S. Civil Service authorized the excepted service program for Army intelligence. A year later, the U.S. Army Intelligence Center issued General Order 8, establishing the Army Survey Detachment as the management unit of the excepted service program. The detachment's Intelligence Civilian Career Program, the predecessor of MICECP, counted 172 CI and HUMINT specialists in the United States, Caribbean, and Pacific and European theaters. In 1986, the Army Survey Detachment was re-designated the Army Field Support Center.

The Excepted Service Program

MICECP personnel are Army Civilians serving in an excepted service program. MICECP employees differ from traditional Army Civilians, each of whom brings subject matter expertise to their position. The Army recruits and develops MICECP personnel for a career in intelligence rather than a specific position. For example, a MICECP member at the journeyman level, GG-13 paygrade, in the CI career track/investigations career path can serve effectively at multiple types of investigative positions, including—

- Investigator at a field office in the continental United States and in the European, Pacific, North Atlantic Treaty Organization, Korean, and/or Southwest Asian theaters.
- Army representative on a joint terrorism task force at a Federal Bureau of Investigation platform.
- Army force protection attaché in a force protection detachment on a State Department platform.
- CI management duties at each echelon from the field office level to the Department of the Army level.

Recruitment and Career Planning

MICECP recruits, employs, and develops motivated, highly qualified, and exceptionally skilled civilian intelligence professionals to fill sensitive and critical CI and HUMINT positions that directly support worldwide missions executed by U.S. Army commanders, U.S. intelligence community staff offices, and joint commands. MICECP provides a specialized and centrally managed career program for civilian intelligence professionals who can operate and excel in all environments. By developing personnel of the highest standards, MICECP meets the operational and strategic requirements at all echelons in both traditional and emerging intelligence disciplines.

The MICECP of today has evolved from its nascent years. Initially focused on only CI and HUMINT career tracks, the program now has three distinct career tracks: CI, HUMINT, and technical support to a specific intelligence discipline. Within CI, there are five career paths: CI Investigations, Strategic CI Operations, CI Support to Cyber Operations, Technical Surveillance Countermeasures, and Polygraph.

Ever versatile and flexible, MICECP continues to evolve as the operating environment changes and new threats emerge. This flexibility is evidenced with the ongoing fielding of the fourth MICECP career track involving specialized assistance to intelligence operations, which is expected to be fully fielded in 2021. With this new career track, MICECP can effectively address and provide solutions for evolving Army operational challenges worldwide.

Each of the career tracks offers professional growth with supervisory positions, staff and management positions, and promotion opportunities at the GG-14 and GG-15 paygrades.

Mobility and Global Opportunities

MICECP assignments are worldwide, at every Army echelon, and some are located at various agency platforms outside the Army. MICECP personnel support 29 organizations, and the overseas assignments are in 37 countries with locations in 21 time zones. MICECP members also perform operational coverage throughout the United States, with permanent duty stations in half of the 50 states. Furthermore, MICECP employees tend to be a professional, interconnected group, allowing MICECP personnel to interact with each other in problem-solving efforts to find solutions to intelligence challenges presented to commands and organizations supported by MICECP members. The MICECP workforce readily accepts organizational challenges and works together to identify multiple courses of action to achieve organizational goals.

Each MICECP member agrees to and signs a mobility agreement, which facilitates rotational tours in the 3-to-5-year timeframe. The mobility agreement allows the Army to surge MICECP personnel worldwide in support of emergency and specialized operations. The mobility agreement, coupled with provisions from AR 690-950-4, also facilitates professional growth among the MICECP population. MICECP personnel rotations occur every 3 to 5 years for three main reasons. In the first year, MICECP members learn the new skills associated with the position; by the second year, these members should be competent in the position; and in years 3 to 5, these members should be able to master the skills associated with their respective position and begin training for follow-on assignments. Additionally, regular rotations limit the possibility of stagnation in one type of assignment. To help with planning, MICECP Career Management uses an "Individual Career Assessment Plan," or career map, for two follow-on assignments for each MICECP member, with suggested training to increase competitiveness for these assignments.

Specific Skillsets and Continuous Training

The Army hires MICECP members for their specific "toolbox" of skills. At each assignment, MICECP members learn and master new skills while applying those skillsets already possessed. Each MICECP member's capability continues to grow and enrich with every new assignment. The MICECP Career Management Branch rarely assigns a MICECP member to a position the member performed previously because the employee will have little opportunity to develop and improve their skillset. Supported organizations highly covet these skillsets because MICECP personnel tend to offer multiple courses of action to address the operational and leadership challenges encountered by those organizations.

MICECP personnel receive centrally managed training in a continuous effort to enhance each member's leadership and technical skills. While MICECP members possess subject matter expertise in each position they fill, employees are continuously preparing for their next assignment. The program highly encourages leadership training for each MICECP member, as the Army expects employees to be coaches, mentors, and trainers to all personnel they work with and encounter. Some MICECP personnel also prepare for future supervisory positions at higher grades (GG-14 and GG-15) where leadership capabilities are paramount. Furthermore, some MICECP positions are language-coded to enhance satisfying command requirements. Thus, MICECP provides a broad range of language training opportunities to its linguist workforce. Many MICECP employees have proficiency in several languages, which often enhances successful mission outcomes in multiple theaters of operations.

Conclusion

Over the past few years, MICECP has made great strides with its workforce in improving transparency regarding assignment planning and personnel actions. The program has found that transparency, along with fairness and consistency, is an excellent tool for recruiting and retaining talent within MICECP. As requirements and challenges evolve in the Army, MICECP will evolve correspondingly, ever ready to prepare for and adeptly address future challenges.

Mr. Ricardo Romero enlisted in the Army in 1984 and transitioned to the Military Intelligence Civilian Excepted Career Program (MICECP) as an Army Civilian in 1998. He currently serves as the MICECP Career Program Manager. He is a dual-tracked career MICECP member in counterintelligence and human intelligence and is an Arabic and Italian linguist. He served in the 66th and 513th Military Intelligence Brigades-Theater and the 902nd Military Intelligence Group. He also served with the Army Field Support Center in various positions, including joint terrorism task forces with the Federal Bureau of Investigation, force protection detachments, and field offices in Atlanta, Detroit, Italy, and Germany in investigative, collections, research and technology protection, and management roles. Mr. Romero attended Michigan State University, with continued studies in various languages at the Defense Language Institute, University of Detroit-Mercy, and University of Maryland-University Center. He also earned advanced management and leadership certificates from Harvard Law School and the U.S. Graduate School.

The Utility of Civil-Military Relations for Intelligence Professionals

by Major George Fust

People define themselves in terms of ancestry, religion, language, history, values, customs, and institutions. They identify with cultural groups: tribes, ethnic groups, religious communities, nations, and, at the broadest level, civilizations. People use politics not just to advance their interests but also to define their identity.

— Samuel P. Huntington

The Clash of Civilizations and the Remaking of World Order

Introduction

You are the unit intelligence officer and your boss has tasked you with generating a country study for country "X." Your boss wants relevant information to help the decision-making process. He doesn't want the typical tourist snapshot you generated last time. He wants depth and rigor. He needs to know how the unit's actions will influence the host nation government. What long-term effects will occur? Who are the key influencers in the government? How does the government and society function? What central levers exist to accomplish the objective? Too often, the focus is on the tactical and operational levels, and these domains take precedence over the strategic. An understanding of civil-military relations can help provide the answers to the questions your boss didn't know he needed.

Putting Civil-Military Relations in Perspective

The concept of civil-military relations is best understood as the space between the "P" and the "M" in the well-used acronym PMESII–PT.[1] An understanding of a country's political structure and personalities is a required first step. It is also necessary to understand the same for the nation's military. The bare minimum intelligence analysis will highlight these facts. It may even provide a historical timeline or predictions about the future. What is often lacking, however, is an understanding of how these categories interact. They are not separate entities, but rather a complex web of interconnected relationships. Capturing this dynamic will likely be far more valuable at the strategic level than knowing how many tanks a country has or that the country is a federal presidential republic. The study of civil-military relations can provide utility for intelligence professionals.

Where to begin? Civil-military relations is inherently an interdisciplinary body of knowledge replete with theory and an ever-evolving set of tools that can be applied to describe phenomena as they occur. While the theoretical aspect largely resides in academia, the application is in practice every day. The interaction between those responsible for governing and those responsible for defense is a paradox. Why should those with real power (weapons, tanks, planes, etc.) follow the directives of those without? What factors contribute to the stability of this arrangement? How can external forces or influences change this dynamic? The answer is different for every country.

Lessons from Our History and the Huntington Model

The United States was founded on the principle of military subordination to the democratically elected representatives of the people.[2] George Washington explained the

importance of this model during his Newburgh Address in 1783. He further demonstrated his belief in it by publicly resigning his commission before becoming the first President of the Republic. Throughout the next two centuries, the U.S. military would evolve into the professional force that it is today.

The Newburgh Address

On March 15, 1783, General George Washington made a surprise appearance at an assembly of Army officers at Newburgh, New York, to calm the growing frustration and distrust they had been openly expressing toward Congress in the previous few weeks. Angry with Congress for failing to honor its promise to pay them and for its failure to settle accounts for repayment of food and clothing, officers began circulating an anonymous letter condemning Congress and calling for a revolt. When word of the letter and its call for an unsanctioned meeting of officers reached him, Washington issued a general order forbidding any unsanctioned meetings and called for a general assembly of officers for March 15. At the meeting, Washington began his speech to the officers by saying, "Gentlemen: By an anonymous summons, an attempt has been made to convene you together; how inconsistent with the rules of propriety! How unmilitary! And how subversive of all order and discipline…" Washington continued by pledging, "to exert whatever ability I am possessed of, in your favor." He added, "Let me entreat you, gentlemen, on your part, not to take any measures, which viewed in the calm light of reason, will lessen the dignity, and sully the glory you have hitherto maintained; let me request you to rely on the plighted faith of your country, and place a full confidence in the purity of the intentions of Congress."[3]

It is unfathomable to imagine the 82nd Airborne Division (or any other) marching on the Capitol to seize control. Instead, theorists of the U.S. civil-military model, commonly referred to as the Huntington model (conceived by Samuel P. Huntington, American political scientist, adviser, and academic) are concerned with degradations of the relationship on the margins. Discussions focus on topics such as, Should retired officers endorse presidential candidates or political parties? Is there a growing civil-military divide? Again, these are threats to optimal civil-military relations, but they are not existential threats to the Nation. The Huntington model of *objective* control[4] and others[5] that have evolved from it are unique to the United States. Here is what Samuel Huntington wrote:

> ***Subjective*** civilian control achieves its end by civilianizing the military, making them the mirror of the state. ***Objective*** civilian control achieves its end by militarizing the military, making them the tool of the state. Subjective civilian control exists in a variety of forms, objective civilian control in only one. The antithesis of objective civilian control is military participation in politics: civilian control decreases as the military become progressively involved in institutional, class, and constitutional politics. Subjective civilian control, on the other hand, presupposes this involvement. The essence of objective civilian control is the recognition of autonomous military professionalism; the essence of subjective civilian control is the denial of an independent military sphere. Historically, the demand for objective control has come from the military profession, the demand for subjective control from the multifarious civilian groups anxious to maximize their power in military affairs.[6]

Every Country is Unique

Using the U.S. model to build a country study will likely result in flawed results. Every country has a unique history and culture from which its civil-military relations evolved. Comparative analysis to the U.S. model will be helpful for developing the questions to ask, but not from an evaluative perspective. The robust literature available in the United States is a necessary starting point for any intelligence professional trying to understand civil-military relations. For example, comparative civil-military literature can help create an exhaustive list of questions, which might include the following:

- Do personal relationships exist between civilian leaders and military leaders?[7]
- Does the military view themselves as the final arbiter of the political process?[8]
- Does a distinction exist between military roles and missions?[9]
- Is the military working to the fullest extent of its duty?[10]
- Is the military competent to do what civilians ask it to do?[11]
- Are the civilians the ones making key substantive policy decisions?[12]
- Do civilians decide which decisions civilians make and which the military make?[13]
- Is the military avoiding any behavior that undermines civilian supremacy in the long run?[14]
- Is civilian authority internalized in the military as a set of strongly held beliefs and values?[15]
- Do civilians exhibit due regard for the military (respect military honor, expertise, autonomy, and political neutrality)?[16]
- Is there low frequency of interference by civilians on military autonomy and exclusiveness?[17]
- Is the relationship between the military and civilian institutions functional (i.e., not strained)?[18]
- Is the military primarily used as an instrument of national defense (not used for nation building)?[19]
- Is there close affinity between the military and bureaucrats?[20]

- ✦ Are there constitutional constraints on the political impact of the military?[21]
- ✦ Do the normal constitutional channels function?[22]
- ✦ Is public attachment to civilian institutions strong?[23]

The answers to these questions can fill that space between the "P" and "M" of PMESII–PT. They help describe the function and structure of a government with greater accuracy than the standard method. They help illuminate the relevant interactions between a country's military and its leaders. Understanding this interaction is critical to developing courses of action that will have strategic effects.

How does one accurately answer the above questions? Most militaries around the world do not have professional journals that regularly publish articles highlighting civil-military relations. The United States is unique in this regard. Most countries' militaries have a culture against discussing their relationship with the civilian government. Journalists, academics, and think tanks can provide useful information; however, these sources are often biased or misinformed. The resourceful intelligence professional will be able to find a way to reliably answer the questions derived from comparative civil-military relations literature.

Conclusion

Leveraging civil-military relations theory will better facilitate a strategic understanding of examined countries. At a minimum, it will provide a more robust country analysis. It will also likely lead to a more informed and deliberate decision-making process. The intricacies of the relationship between a country's military and civilian leadership reveal how the country is *actually* governed. They reveal power dynamics, explain why certain events occur, help forecast conditions when the inputs change, reveal preferences, and help identify where to apply limited resources. Your boss didn't know he needed to know these things, but he will be more effective when you reveal them to him. It's your job as an intelligence professional to leverage the utility of civil-military relations.

Epigraph

Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster Inc., 1997), 21.

Endnotes

1. PMESII–PT—political, military, economic, social, information, infrastructure, physical environment, and time.

2. Russell Weigley, "The American Civilian-Military Cultural Gap: A Historical Perspective, Colonial Times to the Present," in *Soldiers and Civilians: The Civil-Military Gap and American National Security*, eds. Peter D. Feaver and Richard H. Kohn (Cambridge, MA: MIT Press, 2001); and Charles A. Stevenson, *Warriors and Politicians: US Civil-Military Relations Under Stress* (New York: Routledge, 2006).

3. "Washington puts an end to the Newburgh Conspiracy," HISTORY.com website, A&E Television Networks, LLC, updated July 27, 2019, https://www.history.com/this-day-in-history/washington-puts-an-end-to-the-newburgh-conspiracy.

4. Samuel P. Huntington, *The Soldier and the State* (Cambridge, MA: Harvard University Press, 1957).

5. Peter D. Feaver, *Armed Servants: Agency, Oversight, and Civil-Military Relations* (Cambridge, MA: Harvard University Press, 2009).

6. Huntington, *The Soldier*, 83–84; emphasis added.

7. Dale R. Herspring, *Civil-Military Relations and Shared Responsibility: A Four-Nation Study* (Baltimore, MD: The Johns Hopkins University Press, 2013), 290.

8. Kees Koonings and Dirk Kruijt, eds., *Political Armies: The Military and Nation Building in the Age of Democracy* (London: Zed Books, 2002), 315.

9. Thomas C. Bruneau and Scott D. Tollefson, eds., *Who Guards the Guardians and How: Democratic Civil-Military Relations* (Austin, TX: University of Texas Press, 2006), 123.

10. Feaver, *Armed Servants*, 61.

11. Ibid.

12. Ibid.

13. Ibid.

14. Ibid.

15. Eric A. Nordlinger, *Soldiers in Politics: Military Coups and Governments* (Upper Saddle River, NJ: Prentice Hall, 1977), 13.

16. Ibid.

17. Ibid., 49.

18. Martin Edmonds, *Armed Services and Society* (Leicester, UK: Leicester University Press, 1988), 88.

19. Kotera Muthanna Bhimaya, *Civil-Military Relations: A Comparative Study of India and Pakistan* (Santa Monica, CA: RAND Corporation, 1997), 28.

20. Ibid., 35.

21. Claude Emerson Welch, *Civilian Control of the Military: Theory and Cases from Developing Countries* (Albany, NY: SUNY Press, 1976), 5.

22. Samuel E. Finer, *The Man on Horseback: The Role of the Military in Politics* (London: Pall Mall Press, 1962), 168.

23. Ibid., 21.

MAJ George Fust is a military intelligence officer who teaches American politics and civil-military relations in the Social Science Department at the U.S. Military Academy, West Point, NY. He holds a bachelor of arts from McKendree University and a master of arts in political science from Duke University. He previously served in the 173rd Infantry Brigade Combat Team (Airborne), 207th Military Intelligence Brigade, and 1st Infantry Division.

Photo illustration by Emma Morris

A Soldier uses a dry-erase board to brainstorm information that will later be used in the planning process.

Deciphering the Code:

Using Army Design Methodology to Inform Intelligence Analysis

by Major Erin A. Stevens

A Lesson from World War II

In the autumn of 1944, Adolf Hitler cloaked Operation Wacht am Rhein (Watch on the Rhine) in secrecy. He forbade discussion of the offensive, including via telephone, telegraph, and wireless. Even the operation's codename was designed for deception, chosen to give the impression the plan was for a defense at the Rhine.[1] When the attack launched in December, the element of surprise dominated, despite indicators that existed before the attack and that may have suggested its inevitability.[2] Ultra intercepts, air reconnaissance, prisoner interrogations, and information provided by civilians all suggested not only that there would be an attack, but that it would occur through the Ardennes Forest.

In November 1944, however, U.S. Army intelligence officers observing the 6th Panzer Army's transfer to the west bank of the Rhine River concluded that the 6th Panzer planned to counterattack at the Roer River.[3] Analysts believed that a German attack would take place north of the Ardennes, near Cologne, even as IX and XIX Tactical Air Commands identified rail movement, activity at marshaling yards, and piles of equipment in the Eifel region.[4] A week before the German attack, Third U.S. Army G-2 COL Oscar W. Koch determined that forces identified in Eifel would be used as a diversion or as a spoiling attack.[5]

The German offensive, later known as the Battle of the Bulge, is one of many examples of intelligence professionals

Photo courtesy of the Army Center of Military History

U.S. Army engineers emerge from the woods and move out of defensive positions after fighting in the vicinity of Bastogne, Belgium, during the Battle of the Bulge.

making inadequate assessments despite available evidence in support of a contrary point of view. But the purpose of this article is not to place blame or decry intelligence failures. Intelligence, like war, is a human endeavor, and analysts base their intelligence recommendations on more than the collection of indicators. Analysts use their creativity, judgment, skill, and experience alongside indicators and information collection to make determinations and provide warning intelligence. Operational planners use the Army design methodology (ADM) to capitalize on critical and creative thinking and to inform subsequent detailed planning. Likewise, the intelligence analyst can employ his or her creativity and judgment through a reverse- or enemy-perspective ADM.

The U.S. military faces problems that intersect, reinforce, and compound across diverse areas while relationships among actors and across systems interact in unanticipated and surprising ways.[6] Such ill-structured, complex problems demand that analysts facilitate systems thinking, avoid logical fallacies and cognitive biases, and have opportunities to reframe the problem when desired results prove elusive. The intelligence analyst can use ADM from an enemy perspective to give context to indicator analysis and fully employ their creativity and judgment to the examination of indicators. This technique may enhance the ability of the analyst to provide indicator analysis and predictive intelligence to the commander, thereby enhancing the likelihood of mission success.

The Role of Indicator Analysis

Analysts conduct indicator analysis as one of their fundamental tasks.[7] ATP 2-01.3, *Intelligence Preparation of the Battlefield,* defines an indicator as "an item of information which reflects the intention or capability of a threat to adopt or reject a course of action."[8] ATP 2-33.4, *Intelligence Analysis,* elaborates on the definition, describing an indicator as "positive or negative evidence of threat activity or any characteristic of the [area of operation] AO that points toward threat vulnerabilities, the adoption or rejection by the threat of a particular activity, or that may influence the commander's selection of a [course of action] COA."[9] Seasoned analysts understand that an indicator is not a piece of evidence like a fingerprint at a crime scene. They also understand that indicators are not always obvious and that they require aggregation.

Indicators are discrete items of key information that alone are not valuable but can provide insight and direction. Pieces of information do not take on meaning as indicators unless they are collected, interpreted, aggregated, and assembled. Take, for instance, the example indicators in ATP 2-01.3 (Figure 1 on the next page).

The absence or presence of maneuver or engineer assets does not necessarily provide evidence of the enemy's intended course of action. Indicators of military action, including troop movement, weapons relocation, or the presence or absence of formations, are typically visibly apparent to the intelligence community given adequate collection.[10] Potential indicators are numerous and can include the movement of units, movement of troops, recall

NAI	Grid Locations	Enemy COA	Indicators	HVT	NET/NLT
1	10A BC 12345 67891	COA1	1. SPF in hasty defensive positions in vicinity EA1 2. Blocking obstacles on southern portion of AA1	BMP-1KshM T-72B SPF SA-18	H+4/H+5
2	10A BC 23456 78910	COA2	1. SPF in hasty defensive positions in vicinity EA2 2. Blocking obstacles on southern portion of AA2	BMP-1KshM T-72B SPF SA-18	H+4/H+5
3	10A BC 21223 24252	COA3	1. Staging of the 65th Mechanized Battalion north of OBJ Bravo 2. The72d Mechanized Battalion positioned as fixing force in vicinity minefields on AA1 3. Presence of turning obstacles on northern portion of AA2	BMP-1KshM T-72B SPF SA-18	H+3/H+4
4	10T BC 23456 78910	COA4	1. Presence of the 72d and 65th Mechanized Battalions in forward defensive positions 2. The 2S191s remain in southern urban areas	BMP-1KshM T-72B SA-18 TDA-2K UMZ-K 2ST91	H-3/H+7

AA avenue of approach
COA course of action
EA engagement area
H-hour specific hour at which a particular operation commences
HVT high-value target
NAI named area of interest
NET not earlier than
NLT not later than
OBJ objective
SPF special purpose forces

Figure 1. Constructing an Event Matrix[11]

of reserve units or troops on leave, movement of supplies, opening of ports, rail yard activity, fuel movement, or missile placement. Indicators such as the specific emplacement locations and orientations of blocking or turning obstacles can provide even more specific information on the enemy's intent. These are all points of data that analysts may collect, label as indicators, and evaluate to make assessments on enemy actions.

Yet consider the idea of engineer presence. Engineer assets may be forward in both an enemy defense and an enemy offense. They may indicate a withdrawal or an attack, depending upon the type of asset present. When viewed this way, indicators are not evidence. Instead, the indicator provides insight into a situation and relies upon further judgment and interpretation to become valuable.

The JP 5-0, *Joint Planning*, definition of an indicator appears to subscribe to this sentiment. JP 5-0 employs the word "indicator" in its discussion of assessment and describes it as "a specific piece of information that infers the condition, state, or existence of something, and provides a reliable means to ascertain performance or effectiveness."[12] JP 5-0 determines that indicators should be relevant to a desired effect, objective, or end state; observable and collectable; responsive to changes in the operational environment; and resourced with sufficient collection assets.[13] JP 5-0 also offers some helpful guidance for selecting indicators:

- Choose distinct indicators.
- Include indicators from different causal chains.
- Avoid or minimize additional reporting requirements for subordinate units.
- Maximize clarity.[14]

From this perspective, indicators are discrete, have an associated timeline, and provide positive or negative information about an enemy's intent or capabilities. The interpretation of an indicator or group of indicators may turn into a warning and precipitate action on the part of the commander. That indicator analysis becomes predictive, and it precipitates warning intelligence that results in operational action, achieving the goal that intelligence drives operations.

Because anything the enemy does could be an indicator of his intended course of action or provide insight into his capabilities or vulnerabilities, it is imperative that the intelligence analyst understand enemy intent, vulnerabilities, and capabilities in combination with other activities he has undertaken. This complicates the effort of indicator analysis and requires increased emphasis on the analyst's creativity and judgment. A technique that the analyst may consider using in this situation is ADM, applying a reverse or enemy perspective.

The Army Design Methodology

ADM is an iterative sense-making process that aids in decision making by enhancing activities within the operations process, such as understanding, visualization, and description of the operational approach.[15] ADM enables commanders to drive the operations process through understanding, visualizing, describing, directing, leading, and assessing operations.[16] The methodology further applies critical and creative thinking to understand, visualize, and describe unusual problems and potential approaches to manage them.[17] It expands understanding of the operational environment, the operational problem, and the conceptual operational approach that facilitates a transition to detailed planning with a shared commander's vision and intent.

When using ADM from an enemy perspective as part of the intelligence preparation of the battlefield (IPB), the intelligence analyst is able to exercise his or her judgment and creativity while employing skills and techniques already encouraged in intelligence doctrine and practice. Enemy-perspective ADM enhances the enemy view of the environment and may expand upon the options for enemy courses of action, a difficult aspect of the IPB. Enemy-perspective ADM helps the analyst to frame the environment and understand the enemy's desired end state before developing detailed operational or tactical enemy courses of action. This puts the intelligence analyst fully in an enemy perspective which better enables the analysis of indicators and understanding of enemy behavior and intent.

ADM includes multiple activities conducted sequentially, simultaneously, and iteratively. The first activity in ADM is framing the operational environment, a familiar activity for the analyst.[18] Operational environments are complex and dynamic, and framing them involves organizing their interrelated variables and relevant actors.[19] During framing, analysts develop an understanding of the current state of the operational environment from an enemy perspective, while envisioning the enemy's desired future state using techniques such as brainstorming, mind-mapping, and questioning assumptions.[20]

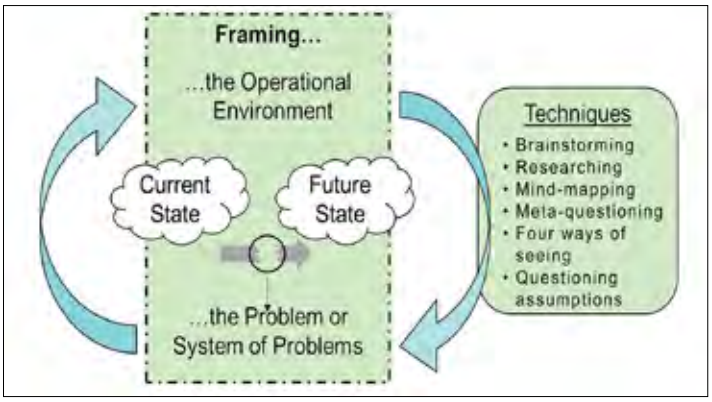


Figure 2. Problem Framing [27]

Framing the operational environment helps the analysis team frame the enemy's problem. When the team identifies the obstacles between the current state of the operational environment and the enemy's desired future state, the problem or system of problems emerges.[21] When the team identifies, maps, and describes interrelated issues, the team works to keep the focus of its efforts suitably narrow for the enemy's mission while remaining broad enough to capture factors that are either symptoms or causes of the obstacles impeding the enemy's desired future state.[22] The problem frame sets the stage for the enemy's operational approach. The problem framing activity (Figure 2) may prompt a return to the environmental frame, and vice versa. ADM encourages a rich understanding of both.

Framing solutions is the ADM activity that benefits from a proper understanding of the operational environment and the problem, and it allows a transition to the detailed development of enemy courses of action during IPB. One way to frame an enemy solution is the development of an operational approach (Figure 3). The operational approach describes broad actions required to transform current conditions into the enemy's desired end state.[23] The operational approach communicates the enemy commander's intent.[24] The operational approach is also the primary product of design and allows the translation of operational concepts into the enemy's specific mission and tasks.[25]

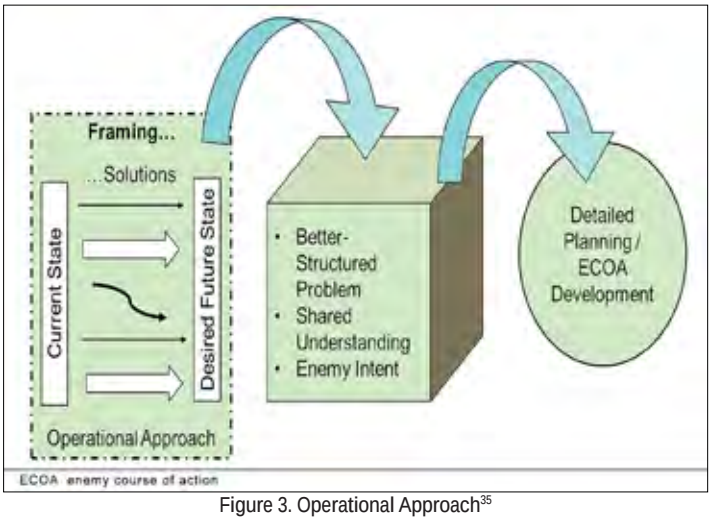


Figure 3. Operational Approach[35]

One of the benefits of ADM, which is also encouraged as an intelligence technique, is the facilitation of systems thinking. Systems thinking is a key concept of ADM.[26] Systems thinking is a process of understanding how aspects of a system work and influence each other as part of the greater whole. This helps the analysts examine the environment holistically from the enemy perspective and identify issues and tensions within the environment that may not be immediately apparent.[28] This technique helps de-compartmentalize the approach to the problem and avoids linear cause-and-effect thinking, which highlights the complexity of the enemy situation and thought process.[29] JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment,* recommends the use of a systems perspective because it helps identify potential sources of indications and warning.[30]

With systems thinking, analysts avoid the illusion that dividing complex problems into component parts makes them more manageable.[31] Breaking up problems divorces them from their context and prevents recognition of the consequences of shifts within the system.[32] Fully engaging in systems thinking prevents engagement in generalizations and abstractions that may create a faulty impression of the enemy's operational approach.[33]

ADM, like many intelligence skills and techniques, further encourages teams to avoid logical fallacies and overcome cognitive biases through the employment of critical and creative thinking.[34] When framing, participants in ADM guard against biases and fallacies through awareness of the thought processes and heuristics that contribute to faulty reasoning.[36] The intelligence analyst is familiar with these processes. A common cognitive bias is confirmation bias, which results from the brain's use of associative memory.[37] With confirmation bias, planners seek

evidence compatible with what they already think about a situation, which is often an intuitive view.[38] Analysts may ignore evidence contrary to the initial view and fail to recognize shifts in the problem or operational environment.

The Japanese became victims of their cognitive biases at Nomonhan in 1939, which aided in their defeat by the Soviet Army. After a series of escalatory engagements with a growing Soviet force, the Japanese Kwantung Army continued to operate off the assumption that the Soviet logistic force could not be larger or more capable than their own.[39] This assumption was built on confirmation bias, from which the Kwantung Headquarters staff sought evidence to confirm their impression of a Soviet Army broken by Joseph Stalin's 1937 purge of military leadership.[40]

The Japanese also fell victim to the mirror-imaging fallacy that can be overcome using the "four ways of seeing" technique used in ADM.[41] Mirror imaging means that analysts fill knowledge gaps by assuming the enemy acts the way the friendly army would act.[42] The Kwantung Army could not fathom the idea that the Soviet logistical effort included more than 4,200 trucks because they had only 800 in the entire region. Furthermore, operations by infantry beyond 125 to 175 miles from the railhead were equally unbelievable to the Kwantung Army, while the Soviets ranged beyond 200 miles.[43] Their anticipation of Soviet actions did not reflect the Soviets' intent or capability, which led to catastrophic defeat. The analyst with a holistic understanding of enemy intent and capabilities developed through the integration of enemy-perspective ADM into the IPB process can avoid many of these pitfalls.

> To succeed in the business of the future, we have to become the very people we're trying to reach.
>
> *—Brian Solis, digital analyst, speaker, and author*

Another important feature of ADM is the opportunity to reframe the problem when desired results prove elusive. Assessment is a crucial and continuous aspect of the operations and intelligence processes. Occasionally, assessment will reveal that the operational environment experienced a significant shift or that key assumptions are invalid. Under these circumstances, analysts may consider reframing their perspective of the enemy.[44]

Reframing provides an opportunity to gain new perspective on a problem or its proposed resolution. In World War I, the armies of Europe found they could not rationally cope with an attritional style of warfare.[45] The Soviet Army thus reframed its approach to combat to include a systems approach, a comprehensive idea of the center of gravity, and the *glubokii boi* or deep battle.[46] Soviet theorists visualized modern warfare to develop the operational level as a result of their reframing of the environment and the problem of overcoming attritional warfare.[47] Likewise, the analyst who recognizes that the interpretation of the enemy's problem or end state is inadequate has the opportunity to reframe the understanding of the enemy's intent and correct course.

ADM does not seek to replace detailed planning through operational processes such as the military decision-making process; instead, it enhances the staff's ability to conduct detailed planning. Likewise, an enemy-perspective ADM would not seek to replace the detailed enemy analysis within IPB; rather, it enhances understanding the enemy before entering into detailed course of action development.

Provide Context to Indicators with ADM

Intelligence is a function that allows a commander to drive operations. Most analysts and decision makers would agree that a difference exists between information and intelligence. Information is data, a collection of the things that we know. Intelligence is data used for a purpose, which has been analyzed, interpreted, and processed and can inform a commander's decision-making process. Intelligence focuses on the enemy's behavior and intent and aims to forecast potential future actions for the commander.

Indicators are a small part of intelligence but have the ability to shed light on the larger situation. When an analyst uses enemy-perspective ADM to enhance the detailed analysis conducted during IPB, the analyst may experience a shift in perspective that enables him or her to employ creativity and judgment with respect to indicators. A single indicator, or a dozen indicators, cannot necessarily reveal an enemy course of action. Yet a single piece of information might have context within an enriched understanding of the enemy's goals and operational approach.

Potential indicators are many, but at the tactical and operational levels, the focus tends to be on the tools of direct combat. Like the examples in ATP 2-01.3, *Intelligence Preparation of the Battlefield,* or ATP 2-33.4, *Intelligence Analysis,* the presence of prepared battle positions, the incidence of armored vehicles, and the assembly of combat formations feature heavily. Logistics preparations are a serious indicator of the preparation for hostilities.[48] Logistics preparations may disrupt the local transportation systems.[49] In some cases, trucks may even be requisitioned from the civilian economy as they were during the Soviet invasion of Czechoslovakia in 1968.[50] Enemy propaganda is also an indication of the enemy's intent because it indicates an enemy's concern about a particular subject.[51]

These discrete points, however, alone cannot provide adequate predictive intelligence. Indicators must be aggregated, analyzed, and assessed using the creativity, experience, skill, and judgment of the intelligence analyst. Enemy-perspective ADM can provide the context within which such indicators may be analyzed because it informs the enemy's operational approach and therefore the enemy courses of action. Furthermore, this technique may provide insight into the enemy's intent and strategy. When we understand the enemy's intent, more precise and realistic courses of action may develop during IPB. Pieces of seemingly unrelated information may correspond to an enemy action or reveal an enemy deception plan.

Consider briefly the surprise and deception involved in Operation Wacht am Rhein. Knowledge of an impending German offensive was gained when Hitler revealed to the Japanese ambassador his plan to attack in early November; the ambassador's report upon returning to Tokyo was quickly decrypted and disseminated.[52] The question then became, Where along the Western Front would the German Army attack?

During IPB, the analyst defines the operational environment, describes environmental effects on operations, evaluates the threat, and determines threat courses of action.[53] Having secured a foothold on the continent over the summer, Allied forces had a relatively mature understanding of the operational environment and its impacts on operations and threat capabilities. Intelligence analysis revealed part of Hitler's late-1944 plan, but not all. Information collected and assessed as indicators would have to reveal the specific course of action the Germans chose to execute.

The intent of the conduct of enemy-perspective ADM in this situation would be to give context to the discrete indicators. ADM and its associated techniques may have created a greater understanding of Hitler's desperation, of his view that incompetent and untrustworthy generals were the source of Germany's wartime failures, and of his intent to divide the alliance by isolating British and Canadian forces during the German drive to Antwerp.[54] Indicators may have been given context within a richer understanding of the enemy's environmental frame, problem frame, and operational approach. Yet history remains in the past.

For the current analyst, the complex world will only produce additional challenges. With the potential for a denied electromagnetic spectrum, and future technological aid still on the horizon, we must arm the intelligence analyst with every technique and skill available. ADM is an existing skill that allows the aggregation and analysis of indicators inside an IPB frame informed by a broader, deeper understanding of the enemy approach. It is a layer upon which to build an enemy framework that might give insight into enemy activity.

Consider the enemy obstacle presence indicator. Alone, it is a discernible item of information available for collection. For the analyst, it is a potential indicator, a point of insight into the enemy's behavior or desired course of action. The analyst who conducted ADM from the enemy perspective may have an advantage in the examination of this item of information. The analyst may have identified that the isolation of friendly forces from important resources informed the bulk of the enemy operational approach. This might have allowed the development of a rich course of action during IPB, highlighting the enemy would capitalize on the opportunity to conduct an offensive with the aim of isolation. This would give context to the forward presence of engineers and allow the analyst to flex his or her creativity and judgment in the assessment of the information. A greater depth of perspective on the enemy might even highlight the enemy engineers as part of a deception operation.

The analyst who understands the enemy well can be the best intelligence weapon on the battlefield. Techniques that enable the analyst to apply creativity, skill, and experience to the enemy problem set may enhance such a weapon. Like the operational planner who employs ADM to enhance the activities within the military decision-making process, the intelligence analyst can employ the same procedures from an enemy perspective to enhance the activities within IPB. Intelligence, like operations, remains both art and science. ADM is a way to use the art to improve upon the science and thereby achieve missions, defeat our enemies, and win.

Endnotes

1. Charles B. MacDonald, *A Time for Trumpets: The Untold Story of the Battle of the Bulge* (New York: Quill, William Morrow, 1985), 40.

2. Ibid., 52.

3. Ibid., 65.

4. Ibid., 66.

5. Ibid., 68.

6. Office of the Chairman of the Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World* (Washington, DC: The Joint Staff, 14 July 2016), ii.

7. Department of the Army, Army Techniques Publication (ATP) 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. Government Publishing Office [GPO], 18 August 2014), 4-5 (common access card [CAC] login required).

8. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield* (Washington, DC: U.S. GPO, 1 March 2019), Glossary-4.

9. Department of the Army, ATP 2-33.4, *Intelligence Analysis,* 4-5.

10. Cynthia Grabo and Jan Goldman, *Handbook of Warning Intelligence: Complete and Declassified Edition* (Lanham, MD: Rowman & Littlefield, 2015), 114.

11. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield,* 6-22.

12. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 5-0, *Joint Planning* (Washington, DC: The Joint Staff, 16 June 2017), VI-24.

13. Ibid., VI-25–VI-26.

14. Ibid., VI-26–VI-27.

15. Department of the Army, ATP 5-0.1, *Army Design Methodology* (Washington, DC: U.S. GPO, 1 July 2015), 1-3.

16. Department of the Army, Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 31 July 2019), 1-5.

17. Department of the Army, ATP 5-0.1, *Army Design Methodology*, 1-3.

18. Ibid., 3-1.

19. Ibid.

20. Ibid., 3-7.

21. Ibid., 4-2.

22. Ibid., 4-4.

23. Ibid., 5-1.

24. Ibid.

25. Office of the Chairman of the Joint Chiefs of Staff, JP 5-0, *Joint Planning*, IV-1.

26. Department of the Army, ATP 5-0.1, *Army Design Methodology,* 1-5.

27. The author created the figure using information in Figure 4-1, ATP 5-0.1, *Army Design Methodology,* 4-3.

28. Department of the Army, ATP 5-0.1, *Army Design Methodology,* 1-8.

29. Ibid.

30. Office of the Chairman of the Joint Chiefs of Staff, JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment* (Washington, DC: The Joint Staff, 21 May 2014), I-4. Available on the Joint Electronic Library Plus (CAC login required).

31. Peter M. Senge, *The Fifth Discipline: The Art & Practice of the Learning Organization* (New York: Currency Books, 2006), 3.

32. Ibid.

33. Dietrich Dörner, *The Logic of Failure: Why Things Go Wrong and What We Can Do To Make Them Right,* trans. Rita and Robert Kimber (New York: Metropolitan Books, 1996), 95.

34. Department of the Army, ATP 5-0.1, *Army Design Methodology,* iii.

35. The author created the figure using information in Figure 5-1, ATP 5-0.1, *Army Design Methodology,* 5-1.

36. Department of the Army, ATP 5-0.1, *Army Design Methodology,* 2-1, A-1.

37. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 81.

38. Ibid.

39. Stuart D. Goldman, *Nomonhan, 1939: The Red Army's Victory that Shaped World War II* (Annapolis, MD: Naval Institute Press, 2012), 132–33.

40. Ibid.

41. Department of the Army, ATP 5-0.1, *Army Design Methodology,* 6-1.

42. Ibid., 3-12.

43. Goldman, *Nomonhan, 1939,* 133.

44. Department of the Army, ATP 5-0.1, *Army Design Methodology,* 6-1–6-2.

45. Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (New York: Frank Cass Publishers, 1997), 174.

46. Ibid., 187, 219.

47. Georgii Samoilovich Isserson, *The Evolution of Operational Art,* trans. Bruce W. Menning (Fort Leavenworth, KS: SAMS Theoretical Special Edition, 2005), x.

48. Grabo and Goldman, *Handbook of Warning Intelligence,* 143.

49. Ibid., 147.

50. Ibid., 205.

51. Ibid., 192.

52. MacDonald, *A Time for Trumpets,* 24–25.

53. Department of the Army, ATP 2-01.3, *Intelligence Preparation of the Battlefield,* 1-3.

54. MacDonald, *A Time for Trumpets*, 38.

MAJ Erin Stevens is a military intelligence officer who served as a tactical battalion S-2, military intelligence company commander, and strategic-level intelligence briefer. She is currently an operational planner at U.S. Army Pacific Headquarters, Fort Shafter, HI.

Enabling Mission Success by Avoiding Over-Classification

by Major Daniel Jarvis

Introduction

Military intelligence professionals safeguard classified information daily. We limit access to the information using technical and physical methods and applying personnel and administrative control measures.[1] By their very nature, our military occupational specialties ingrain the task of securing information, reinforced through the framework of our duties. This instinct, developed in training and honed during operations, tends to cause many individuals to apply automatically the highest classification possible. This tendency can result in an unnecessary hindrance to the organizations we serve. Guarding information in order to deny access to the greatest extent possible is a detriment to mission accomplishment. Instead of using over-classifications to protect information, the intelligence professional has a duty to ensure operational success through applying the proper markings, sharing appropriately, and *granting* access to the right people.

A Natural Inclination to Protect

Service members across all warfighting functions take recurring, mandatory training emphasizing the protection of information against adversaries. It is no surprise that, when dealing with the greatest amount of classified information, the intelligence community believes it has the obligation to be the leader in the effort to safeguard it. The tendency of improperly trained individuals is to classify at the highest possible level within the system used.

Typical analysts' duties include research and data collection from a multitude of classified sources to create situational understanding for commands and make predictive analysis based on reporting and trends. These individuals are expected to have adequate knowledge of the subject matter, the appropriate classification guidelines, and the purpose of their tasks while compiling information for multiple products with derivative classifications.[2] For the sake of saving time and effort, the majority of analysts use the highest overall classification from the source data and label their own product similarly without fully knowing, or asking, which specific portions require the classification. They also tend to label electronic communication at the level of the system they are using instead of the level of information they are sending. Many individuals automatically label every SECRET Internet Protocol Router Network email as "SECRET//NOFORN" [not releasable to foreign nationals] without regard for the message itself. This ingrained default mindset is based on goodwill—doing our job to protect information that could cause damage to national security—but improper markings often tie our own organization's hands more than necessary by preventing the information from reaching the appropriate end user.

This lack of clarity or specificity when passing information is not only a bad habit but is also contrary to guidance from the Office of the Director of National Intelligence. The guidance recommends labeling information at the lowest possible level because over-classification "restricts information sharing [and] hinders the optimal use of intelligence information in support of national security and foreign policy goals."[3] The bottom line with creating products containing derivative classification is to use specificity and ask for clarification when necessary. This specificity includes the use of classification markings on individual lines or paragraphs within products or communications to identify precisely what part of the information requires the access and dissemination control. If a person is unsure of why an overall classification exists, he or she may apply the safe practice of using the highest label, but the best option is to verify with the originator.

Tragic Lessons from History

While the following lesson from history is not an example of over-classification of intelligence, it is an important

example of over-classification of information. Over-classification and the related inability to share information have led to issues ranging from unnecessary operational obstacles to some of the worst disasters in military history. In 1945, the USS *Indianapolis* participated in one of the most highly classified operations of World War II as it delivered components of the atomic bomb for use against Japan. Once the cargo arrived safely at Tinian, the USS *Indianapolis* stopped at Guam before continuing unescorted for Leyte when two torpedoes from a Japanese submarine struck it shortly after midnight on 30 July. It sank in less than 15 minutes. Hundreds of Sailors who did not initially go down with their ship died within the next three days after vainly trying to survive in the shark-infested waters, experiencing dehydration and hysteria. A passing pilot randomly spotted and rescued the survivors on the evening of 2 August.[4] The Navy, unaware the ship had sunk, had not begun an official search. Although the primary reasons for the tragic lack of a deliberate search and the unnecessarily delayed rescue were related to defects in scheduling, routing, tracking, and escort procedures, issues surrounding the classification of information also contributed to the disaster.[5]

Photo from the Bureau of Ships Collection in the U.S. National Archives

The USS *Indianapolis* **off the Mare Island Navy Yard, CA, 10 July 1945, after her final overhaul and repair of combat damage.**

The extremely sensitive nature of the USS *Indianapolis'* classified mission was so protected that the ship's purpose was known to only a limited number of top naval officials, and its mere presence in the area was known to only as few people (beyond the crew) as necessary for logistic and operational reasons. Hours after the sinking, when naval intelligence received reporting from enemy sources of the successful Japanese attack in the approximate scheduled location of the USS *Indianapolis,* analysts dismissed it as false reporting, uninformed the ship was actually there.[6] Due to the overly sensitive approach to protect the operation beyond the classified portion of the mission, the Navy lost hours of critical time to save lives. Highlighting what may happen when necessary end users are denied access to information, the blanket over-classification of every aspect related to the USS *Indianapolis'* mission complicated the situation and contributed to turning an unfortunate operational loss into a tragedy.

Further still, the inability to share intelligence has also proven disastrous at a strategic level. Now engrained in our national narrative, the infamous and seemingly unprovoked attack against the U.S. Pacific Fleet at Pearl Harbor catapulted the Nation into World War II. Although military and political leaders were aware of an existing threat and even received reports of a probable attack by the Japanese, the inability to predict the "when, where, or how" prevented the necessary preparations. Competitive interest, bureaucratic disorder, distrust, misunderstanding, and lack of communication between intelligence services prevented collaboration. National security suffered as a result. It is almost incomprehensible that this type of event could happen twice to the same nation in a 60-year span, but it did. In the time leading up to September 11, 2001, organizations within the U.S. intelligence community were not collaborating—a grave mistake to avoid in the future.

Sharing Properly

Learning how to share properly is a critical aspect to classifying information. Most likely, the originator will correctly classify a document given their subject matter expertise, but analysts must be aware of their ability to properly challenge the classification if necessary. According to regulations, if any authorized user has probable reason to believe improper or unnecessary classifications exist, they can communicate their concern to the security manager.[7] It is the intelligence professional's charge to use the standard prescribed processes and correct justifiable errors. This enables information to reach the appropriate level required for action, including when partnered with outside agencies or even foreign services.

A key tool available to the analyst is the Foreign Disclosure Office. Analysts need to know how to contact the office to

create appropriately sanitized and releasable information. Since we were an infantry battalion S-2 section preparing for a deployment consisting of retrograde operations and handover with Afghan forces, personnel from our section attended Foreign Disclosure Office training, specifically to enable the unit's internal ability to share releasable information with partnered forces. After the initial weeks in country, the commander directed leaders to share all knowledge and information with our partners, and the criticality of this skillset quickly became apparent. One company commander's initial misinterpretation of this guidance to share nearly led to an unauthorized disclosure of classified information. Trained personnel caught the error and corrected it before any security incident occurred. To enable operations moving forward, the ability of our intelligence section analysts to create two versions (one shareable and one not) for every disseminated intelligence estimate fostered success for both the organic companies and their partnered Afghan elements. Achieving successful operations with host-nation forces in the lead called for intelligence sharing; doing so correctly required the battalion intelligence section to create sanitized products and inform leaders on the proper procedures for handling them.

The Foreign Disclosure Officer and Foreign Disclosure Representative

The foreign disclosure officer (FDO) is a formally designated individual authorized and tasked to plan for, recommend, and effect the disclosure of classified military information (CMI) and controlled unclassified information (CUI) to an authorized representative of a foreign government or international organization. The FDO makes disclosure determinations based on the policies, directives, and laws that govern national disclosure policy and the release of classified information. The FDO provides this service to the command and staff and to assigned, attached, and supporting agencies, allies, and other multinational partners.

The FDO can be either a uniformed member of the staff or a Department of the Army (DA) Civilian. FDO responsibilities include, but are not limited to—

- Informing/advising the commander and staff on the impact and implications of current delegated disclosure authorities by country, category of information, and classification level on mission requirements.
- Advising the commander and staff on the recommended number and location of foreign disclosure representatives (FDRs) based on mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).
- Directing the information production requirements efforts within the organization for all categories of CMI/CUI to ensure maximum disclosure to unified action partners.
- Coordinating for the authority and permission to disclose information originated outside the organization.
- Developing and promulgating foreign disclosure guidance for deployments, exercises, training events, and official foreign visits/visitors (including exchange and liaison officers).
- Ensuring unit and organizational compliance with AR 380-10, *Foreign Disclosure and Contacts with Foreign Representatives.*

An FDR is an individual designated in writing who assists, advises, and makes recommendations to the FDO on disclosure matters. FDRs can be either DA members or Army-employed contractor personnel.

In addition to making releasable products for combined operations, the correct labeling of classified information further enables communication among cleared planners. This is more evident in the management of special access programs (SAPs). SAPs are specially compartmented capabilities used to support commanders' efforts that demand stringent access restrictions. Their control is managed down to the individual capability and is available to an extremely limited audience of planners and command authorities. Each authorized user is responsible for the proper and accurate marking of products and communications relating to these capabilities. With such stringent controls of highly sensitive information, one could assume the safest practice of protection is using the highest available classification as a "catchall" safeguard; again, even with increased sensitivity, this is the improper approach. Over-classifying in a compartmented environment unnecessarily further restricts an already narrow audience of planners. It is even possible to accidentally deny access to the intended authorized end users. Furthermore, access to SAP planning systems and facilities is often limited. It consequently becomes the SAP manager's responsibility to properly share information at the lowest possible classification to ensure understanding and planning happen at all appropriate levels. For example, even though the capability itself may require SAP levels of security, the effects may be transmittable over top secret networks or broader operations for cleared persons at the secret level. Security managers are responsible for enabling successful planning efforts, applying as much scrutiny as when they safeguard the information or capability.

Getting the Right People Access

Ensuring operational success from an intelligence perspective is more about getting the right people permission, not simply denying access. Planners must principally comprehend the why of their efforts. Understanding the commander's intent and desired end state is essential to developing intelligence support to operations. This allows

intelligence professionals to help commanders and staffs visualize the operational environment and make command decisions. A major challenge to this is the integration of key staff elements during the military decision-making process, collection operations, targeting, and assessments.[8] Often, intelligence planners' clearance and access exceed that of other staff members incorporated with these efforts. In addition to safeguarding information from spillage or disclosure, intelligence professionals must help determine if granting additional key planners access better enables operations.

Sometimes decision makers have access to information without enough individuals cleared to support the planning and staff work required. This occurs when granting access to a limited number of billets is based primarily on duty title, especially for sensitive compartmented information, alternate compensatory control measures, or special access requirements. If such a situation exists, the justification cannot be "that is the way it has always been"; the situation cannot remain unchallenged. Charged with getting the right people access, intelligence planners must determine if a need-to-know exists beyond predesignated billets to enable planning and operations.

Once the right people have the proper authorizations, they should be empowered to use their access to benefit the organization. Challenges associated with newly indoctrinated individuals include locating an available workspace within the appropriately cleared facility, establishing network connectivity with an account at the new classification levels, and understanding the purpose for gaining access. Security managers must take the extra step in letting people know *why* they are being read on to particular programs or caveats and how they can specifically contribute to planning. Maybe this includes explaining the procedures for nominating other persons for access who can provide additional benefits to planning efforts. Maybe they are serving in a unified organization and the person capable of providing the greatest benefit is a non-U.S. partner from an allied nation. The list of potential challenges is open ended, but if the reasons are justifiable, the solution to all of them is to ask through appropriate channels. Competent staff members do not stop at the first "no"; instead, they look for the answer. We must tell commanders how they can, not how they cannot.

Conclusion

This is by no means a suggestion to reduce the emphasis placed on the protection of classified information. It is a call to ensure intelligence professionals place just as much, if not more, attention to ensuring mission accomplishment. Maintaining current knowledge of classification guidelines and procedures, understanding the processes to share information appropriately, and seeking to gain access for the right people are essential responsibilities of the intelligence planner. Properly classifying information can be tedious, time consuming, and difficult. It may be quicker to opt for the easy choice and over-classify, but it is the obligation of intelligence professionals to take the "hard right" and enable our organization's success.

Endnotes

1. Department of Defense, Department of Defense Manual 5200.1, *DoD Information Security Program: Protection of Classified Information, Volume 3* (Washington, DC: U.S. Government Publishing Office [GPO], February 24, 2012), 14. Change 2 was issued on March 19, 2013.

2. Department of the Army, Army Regulation (AR) 380-5, *Department of the Army Information Security Program* (Washington, DC: U.S. GPO, 29 September 2000), 7.

3. Office of the Director of National Intelligence, *Principles of Classification Management for the Intelligence Community,* April 4, 2017, 2, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2017/item/1745-the-principles-of-classification-management-for-the-intelligence-community.

4. "The Sinking of USS *Indianapolis*: Navy Department Press Release, Narrative of the Circumstances of the Loss of USS Indianapolis, 23 February 1946," Naval History and Heritage Command website, accessed 24 October 2019, https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/s/sinking-ussindianapolis/narrative-of-the-circumstances.html.

5. Sam Cox, "Lest We Forget: USS Indianapolis and Her Sailors," *The Sextant* (blog), Naval History and Heritage Command, August 24, 2017, http://usnhistory.navylive.dodlive.mil/2017/08/24/lest-we-forget-uss-indianapolis-and-her-sailors/.

6. "The Sinking of USS *Indianapolis*."

7. Department of the Army, AR 380-5, *Information Security*, 13.

8. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 July 2019), 5-2.

Reference

Department of the Army. Army Regulation 380-10, *Foreign Disclosure and Contacts with Foreign Representatives*. Washington, DC: U.S. GPO, 14 July 2015.

MAJ Daniel Jarvis is the United States Forces Korea Integrated Joint Special Technical Operations Branch Chief and intelligence planner. He is a graduate of the Counterintelligence Officers Course and completed the Department of Defense Sensitive Compartmented Information Security Officers Course. His previous assignments include battalion S-2 and company commander, and he has deployed to Iraq and Afghanistan. He holds a master of arts degree in intelligence studies from American Military University.

Using the Military Intelligence Training Strategy to Conduct Battalion Collective Training

by Major Benjiman A. Smith

Introduction

The 303rd Expeditionary-Military Intelligence Battalion (E–MI BN) recently undertook a deliberate training progression to achieve a "T" rating (i.e., "trained") on military intelligence (MI) specific mission essential tasks (METs) to maintain proficiency as one of the Army's focused ready units. This article describes how the 303rd E–MI BN ("Longhorns") leveraged the recently published Military Intelligence Training Strategy (MITS) framework to plan, prepare, and conduct a battalion-level field training exercise that tested collective-level proficiency.

This article outlines a way to conduct training of the MITS tasks leading up to Tier 2 collective training for an expeditionary-MI battalion. It further addresses lessons learned by the 303rd E–MI BN during training progression through the four MITS levels: individual, crew, platoon/platform, and intelligence warfighting function. TC 2-19.400, *Military Intelligence Training Strategy*, provides a fundamental understanding of the MITS certification program.[1]

Background and Battalion Task Organization

Operation Longhorn Forge was a battalion-level field training exercise conducted in March 2019. It marked the first time the Longhorns conducted battalion collective training with all organic companies and systems since 2015. Since that time, the battalion had been geographically separated. B/303rd, the collection and exploitation company, was stationed at Fort Gordon, Georgia, in support of intelligence reach; and A/303rd, the counterintelligence (CI) and human intelligence (HUMINT) company, was deploying to and from Afghanistan in support of Operation Freedom's Sentinel. Both Alpha and Bravo companies had focused on supporting counterinsurgency operations in the U.S. Central Command area of responsibility and had limited experience with supporting large-scale ground combat operations to nest under the battalion's METs. The battalion reassembled at Fort Hood, Texas, in October 2018 and conducted reintegration, personnel turnover, and task organization change to return the formation to its modified table of organization and equipment configuration.

Photo courtesy of U.S. Army

Soldiers from the 303rd **Military Intelligence Battalion prepare for unit training utilizing a terrain model at Camp Bullis, TX, July 2019.**

The expeditionary-MI battalion consists of 285 Soldiers and is task-organized with three organic companies. The companies bring expanded analytical and collection capabilities compared to an MI company assigned to a brigade combat team.[2] The battalion is intended to provide MI support to either a division or a corps headquarters, performing both collection and processing/analysis in support of a combat arms commander. The headquarters detachment contains the intelligence and electronic warfare (IEW) systems integration section (equipped with the AN/TSQ-226(V)2 Trojan SPIRIT) and a wheeled-vehicle maintenance section, in addition to typical battalion-level staff sections. As shown in Figure 1, Alpha Company is organized with CI and HUMINT collection and management teams and contains a HUMINT operations cell to perform analysis and help direct future collection operations. Bravo Company is organized with both geospatial intelligence (GEOINT) and signals intelligence (SIGINT) processing, exploitation, and dissemination (PED) platoons, a Tactical-Intelligence Ground Station (TGS) PED platoon equipped with an AN/TSQ-179 TGS vehicle, and a multifunction platoon intended to conduct both SIGINT and HUMINT collection from the Prophet Mine Resistant Ambush Protected–All Terrain Vehicle. The battalion can be task-organized to support multiple echelons across a division or corps commander's area of responsibility. By December 2018, the battalion was manned appropriately and prepared to begin a deliberate training progression oriented on its four mission essential task list (METL) tasks.

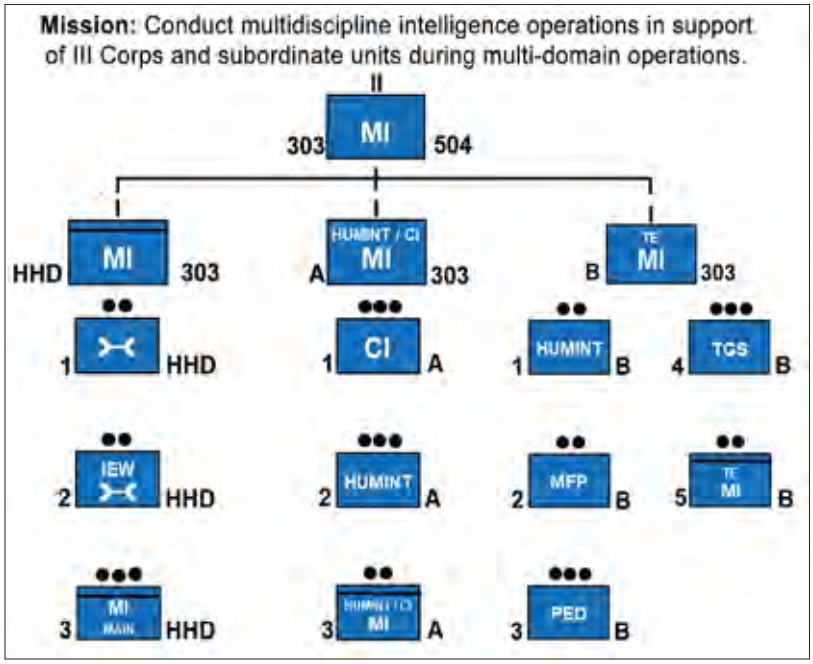


Figure 1. 303rd **E–MI BN Task Organization**

The 303rd E–MI BN METL tasks are divided into three areas to support both collection and analysis functions:

- MET One, *Direct Operational Intelligence Activities*, focuses on the battalion providing command and control over MI operations and integrating into the intelligence architecture necessary to support the combined arms team.
- MET Two, *Process Collected Operational Information*, tests the battalion's ability to turn information into intelligence and to manage the information and data required to support a commander's decision cycle. MET Two assumes the battalion will process SIGINT, HUMINT, and GEOINT information collected by the intelligence community, partners, allies, other services within the Department of Defense, and adjacent Army units.
- MET Three, *Collect Relevant Information*, tests the battalion's ability to collect HUMINT and SIGINT information in direct support of an operational commander's priorities and decision cycle.

As no published MITS exists to support the expeditionary-MI battalion, the 303rd E–MI BN commander and staff used MITS as a guide to develop a deliberate training strategy to train the 303rd E–MI BN along these METs.

MITS outlines a progression for certification of an MI company in a brigade combat team (BCT); the strategy has been practiced by multiple divisions and is generally led and organized by the division G-2. The strategy identifies nine different crews within the BCT MI company and tests the individuals and crews separately before integrating the intelligence warfighting function into a brigade-level operation. The strategy calls for a deliberate certification progression:

- Individual (Tier 4).[3]
- Crew (Tier 3).[4]
- Platform, intelligence warfighting function (Tier 2).[5]
- Intelligence warfighting function, integrated with BCT (Tier 1).[6]

Tier 4 certification focuses on individual military occupational specialty skills. Commanders can utilize institutional, operational, and self-development training courses to maintain their unit's military occupational specialty proficiency.[7] Tier 3 certification culminates with testing small units within the MI company to ensure they can perform a necessary group of tasks that support the intelligence process; these crews are certified in isolation from one another to ensure their performance does not affect or interfere with the other crews.[8] Tier 2 consists of an intelligence warfighting function certification exercise,

which tests MI systems and processes independent from combined arms formations. Units reach Tier 1 when they integrate the MI company and BCT S-2 section into a BCT collective training exercise. This methodical approach to training progression and tiered certification works well for a modular BCT that culminates with a collective training exercise at a combat training center. The 303rd E–MI BN used the MITS concept to develop a 5-month training strategy to progress from Tier 4 to Tier 1, as shown in Figure 2.

The 303rd E–MI Battalion Training Plan and Operational Approach

The Longhorns began their training progression in December 2018, with individual training and new equipment fielding of the Distributed Common Ground System-Army (DCGS–A) software package 3.4. The battalion conducted Tier 4 training throughout the training period, as individual course availability demanded that Soldiers attend specialized military occupational specialty training when possible. Tier 4 training included ongoing GEOINT PED support to U.S. Central Command's area of responsibility and individual training courses, such as:

- Source Operations Course.
- Defense Advanced Tradecraft Course.
- CI Investigations.
- Advanced CI Collections Course.
- Full Spectrum Counterintelligence.
- Tactical Site Exploitation: Document Exploitation, Cellular Exploitation, Media Exploitation.
- SIGINT Mode-1.
- Basic SIGINT Analytics.

Tier 3 training took the form of company situational training exercises for the battalion's seven MI platoons and the IEW section. The Longhorns used the Fort Hood Foundry site (Intelligence Training Center of Excellence) and the Fort Hood Mission Command Training Center to isolate the MI crews and train junior officers, warrant officers, and noncommissioned officers to lead their organizations. HUMINT and CI crew training included live interrogations and source meetings, and incorporated the operational management team. TGS, SIGINT, and GEOINT PED training was mostly conducted at the Fort Hood Foundry site and used Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) simulation to generate the volume of reporting necessary to challenge analysts. The multifunction platoon conducted live training throughout Fort Hood using Stratomist to simulate a sophisticated communications environment to facilitate signals training. The battalion staff conducted a staff-specific training scenario at the Fort Hood Mission

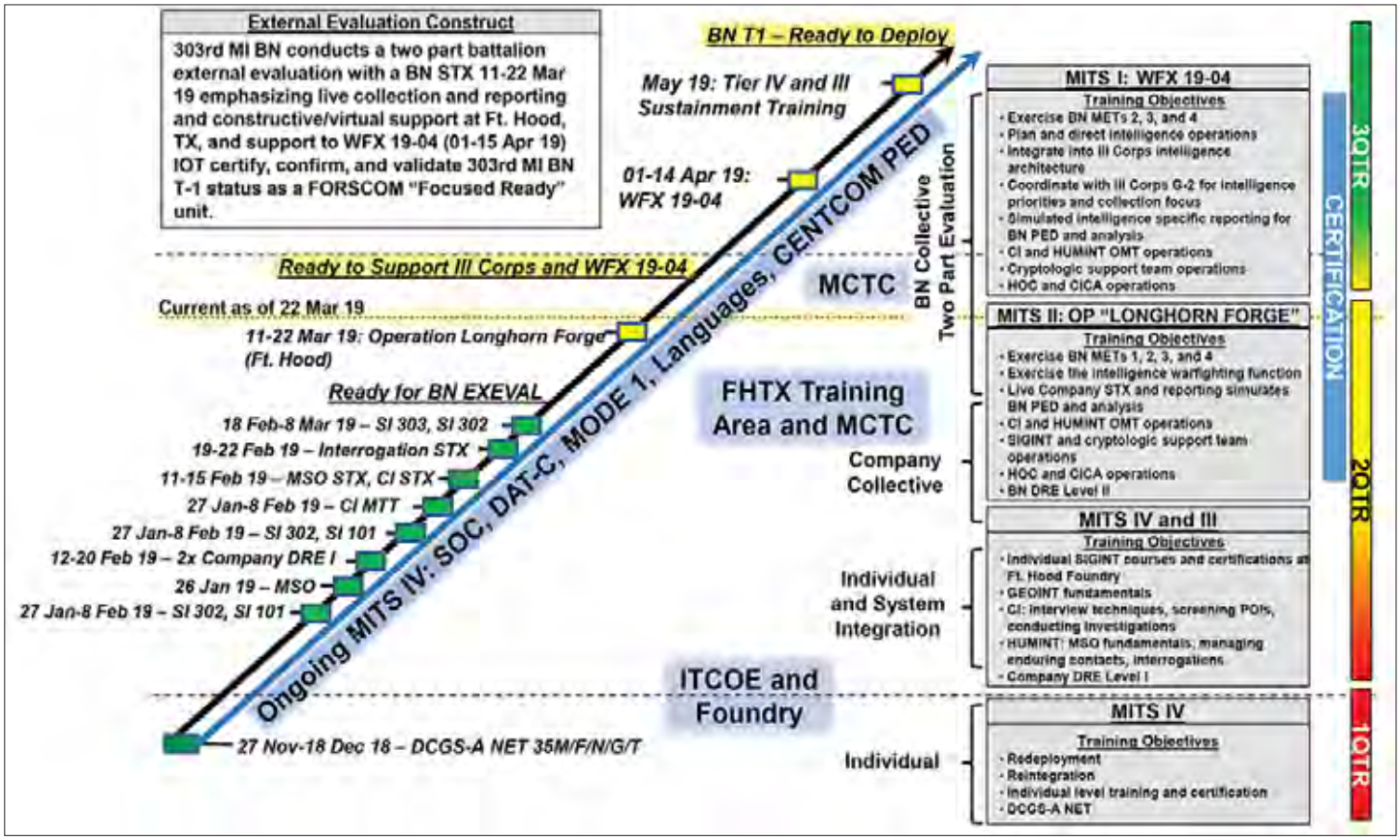


Figure 2. 303rd **E–MI BN MITS and Campaign Plan**

Command Training Center to prepare the staff to conduct command and control and integrate the battalion's crews into a collective training event. Throughout Tier 3 training, the battalion's IEW section performed multiple MI system communications exercises, which ensured that MI digital systems could communicate. By the middle of March 2018, the Longhorns were staged to progress to battalion collective training.

Expeditionary-MI Battalion Collective Training

The 303rd E–MI BN conducted a two-part certification exercise to progress from Tier 2 to Tier 1 in March–April 2019. The Tier 2 exercise, Operation Longhorn Forge, was a battalion collective training event conducted and resourced from Fort Hood, which included live, virtual, and constructive simulations to unite all intelligence disciplines under a common scenario, as shown in Figure 3. The Tier 1 exercise was the 303rd E–MI BN support to Warfighter Exercise 19-04, a III Corps digital event conducted across Fort Hood and bases throughout the central United States.

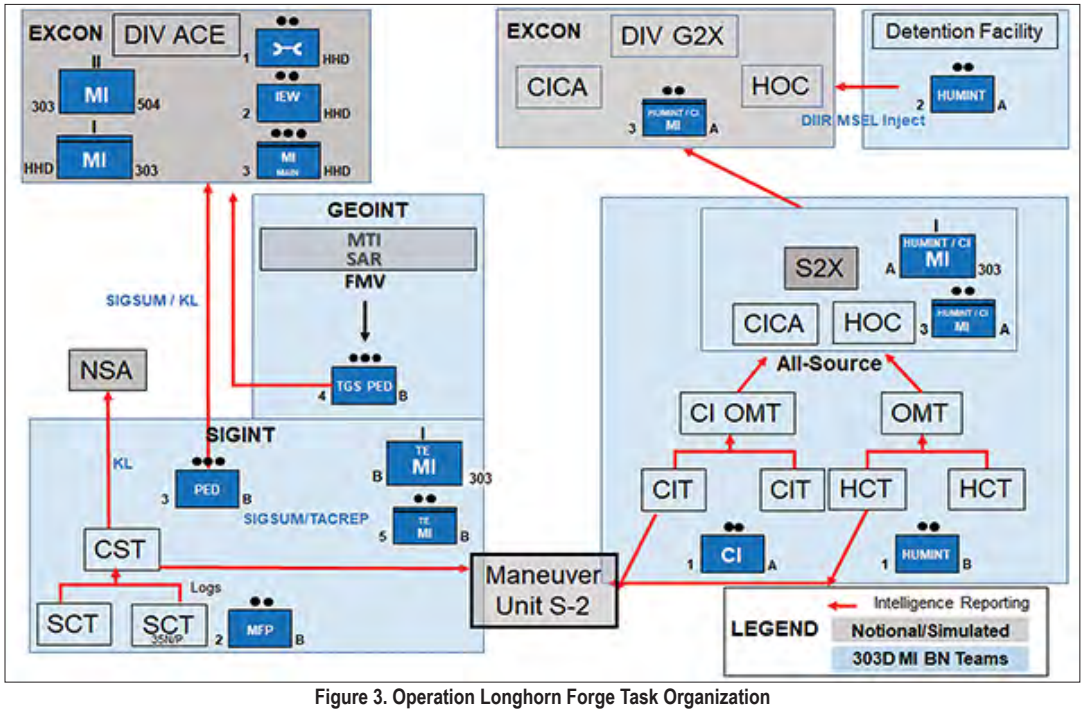


Figure 3. Operation Longhorn Forge Task Organization

Operation Longhorn Forge was designed to put all organic parts of the expeditionary-MI battalion into action during a single exercise, without partnering with a combined arms headquarters. The 8-day training event involved 162 Soldiers, including all seven MI platoons and the wheeled-vehicle maintenance and IEW sections (Figure 4 on the next page). The battalion task-organized its platoons at different locations throughout Fort Hood to simulate the ways in which an expeditionary-MI battalion would support a division commander during large-scale ground combat operations—

- from the tactical level (multifunction platoon collection against a ground threat),
- to the division close area (interrogations at the detainee holding area, TGS support to the division tactical command post), and
- to the division consolidation area (SIGINT and GEOINT PED in support of the division main-command post).

The 303rd E–MI BN chose to consolidate all HUMINT Soldiers under A/303rd to maximize role players and detention facility training resources. The Army's Caspian Sea decisive action training environment scenario formed the common background for the exercise.

Operation Longhorn Forge was designed to stress the battalion's organic communications architecture as much as possible. The battalion used Trojan SPIRIT, the battalion's organic intelligence communications platform, and a closed network database at the Fort Hood Foundry site to link data acquired from the Prophet collection platform with simulated reporting from the IEWTPT. This allowed the SIGINT and GEOINT PED sections to access reporting across the breadth of simulated collection platforms in both the upper and lower enclaves. Secure frequency modulation and the newly fielded Joint Battle Command Platform enabled the MI platoons to test tactical reporting systems and send spot reports to move information quickly and support the commander's decision cycle. An expeditionary-MI battalion is not resourced with organic communications systems to access the Army's Warfighter Information Network-Tactical, so the battalion staff used a Fort Hood Digital Tactical Operation Center Site to connect to the Non-classified Internet Protocol Router Network and simulate connecting into a division's G-2 and main-command post network architecture. Overall, the exercise was an effective way to test all systems and processes within the intelligence enterprise before integrating the intelligence warfighting function into a larger collective training event.

The battalion also prioritized stressing its organic logistics and support systems in order to practice expeditionary

deployment operations. The battalion used the unit's organic very small aperture terminal system to access the Global Command and Control System-Army and order maintenance parts. The wheeled-vehicle maintenance team provided organic recovery support throughout the operation. Although the expeditionary-MI battalion is not organized with food service or refueling assets, the S-4 section established daily logistics missions to provide Class I and III supply, replicating how the expeditionary-MI battalion would pull resources from the supported division's sustainment brigade.

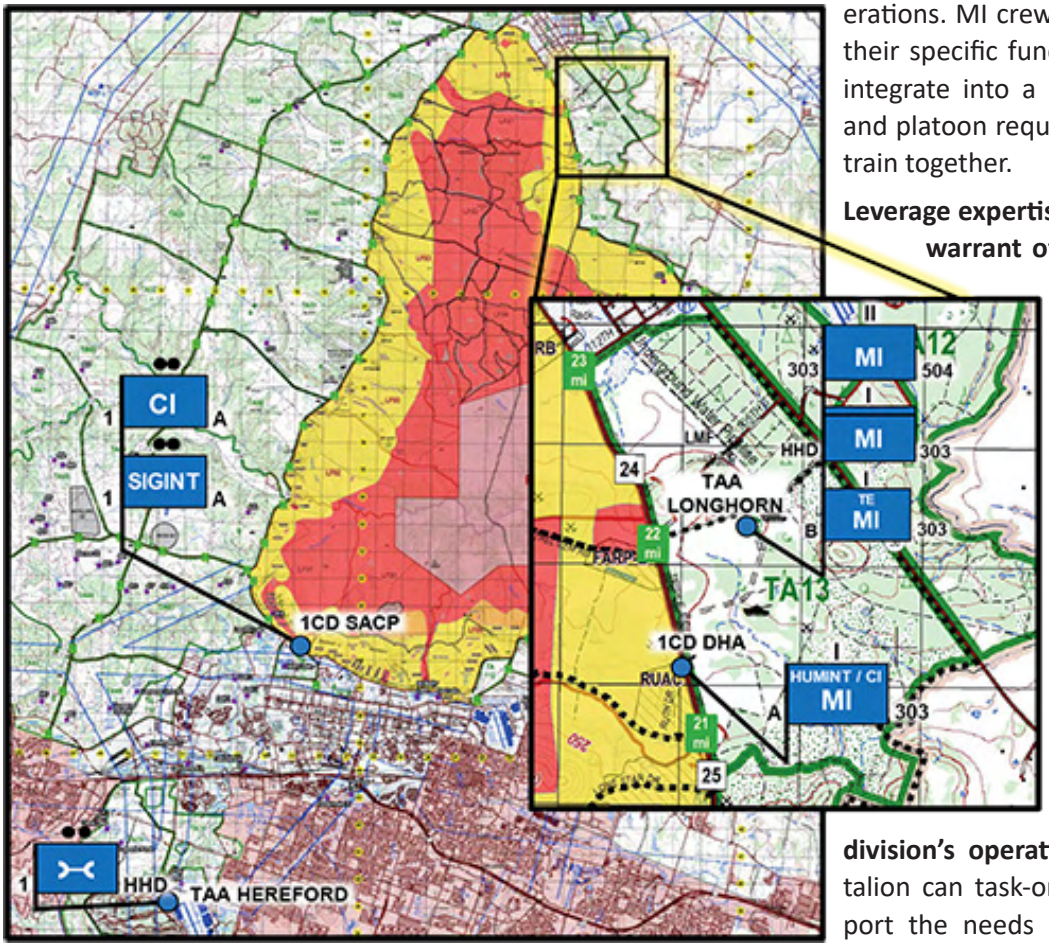


Figure 4. Operation Longhorn Forge—MITS Tier 2

Tier 1 training and the battalion's culminating training exercise was accomplished by integrating operations into the III Corps Warfighting Exercise 19-04. The III Corps team planned and resourced this event. The Longhorn Battalion provided SIGINT and GEOINT PED support to the III Corps staff and provided MI command and control for intelligence collection systems in constructive simulation. As a digital warfighting exercise, this event did not include a live-collection mission for the HUMINT, CI, or multifunction platoons. Exercising the intelligence warfighting function in isolation during the MITS Tier 2 event allowed the Longhorn Battalion to improve the organization's systems and processes, which helped the organization to integrate successfully into a larger training event.

Lessons Learned for Future Expeditionary-MI Battalion Collective Training

The 303rd E–MI BN's approach to training highlighted the following lessons learned for future MITS Tier 2 events:

A systematic training progression from crew and platoon to battalion collective is necessary to operate effectively as a team. The Army's MITS is easily adapted to the expeditionary-MI battalion training for large-scale ground combat operations. MI crews and platoons must understand their specific functions and understand how they integrate into a division's operations. Each crew and platoon requires a specific set of resources to train together.

Leverage expertise from the organization's senior warrant officers to plan and resource the best training events. An expeditionary-MI battalion is organized with multiple senior HUMINT, SIGINT, CI, and IEW warrant officers. Integrate these players into the battalion's overall training plan to design a scenario and communications architecture that will replicate expeditionary-MI battalion operations across a division's area of responsibility.

Study combined arms doctrine to understand how an expeditionary-MI battalion could and should best integrate into a division's operations. The expeditionary-MI battalion can task-organize in multiple ways to support the needs of a combat arms commander. Some Army doctrine is rather outdated (ATP 3-91, *Division Operations*, was last updated in 2014 and still refers to the legacy battlefield surveillance brigade),[9] but intelligence planners must have a thorough grasp of combined arms warfare to understand how an expeditionary-MI battalion will support a division commander's operations.

The IEW section must conduct multiple MI system communication exercises to establish a functioning intelligence architecture. The IEW section has the unenviable task of maintaining and integrating a host of MI systems into the intelligence architecture, including DCGS–A, GEOINT Workstation, TGS, Command Post of the Future, Intelligence Fusion Server, and both SIGINT and HUMINT program of

record B-version trucks. Conduct MI systems communications exercise in conjunction with Tier 3 crew and platoon training to establish working MI systems and economize IEW technical expertise.

Integrate live, virtual, and constructive resources to tailor requirements for all MI platoons. MI platoons require a variety of resources in order to benefit their training audience. Incorporate resources to simulate live collection and PED, including HUMINT/CI role-player support, GEOINT platforms such as the Joint Surveillance Target Attack Radar System, Stratomist, or other signals-replicating equipment. Incorporate intelligence simulations such as IEWTPT from the installation Foundry site to augment live collection and replicate the volume of reporting necessary to engage the PED platoons.

Resource observer-coach-trainers from higher headquarters and adjacent units to evaluate training progression. The 303rd E–MI BN resourced observer-coach-trainers from the 3rd Security Force Assistance Brigade, 1st Cavalry Division, and III Corps G-2 section to provide the appropriate subject matter experts to evaluate MI collection, processing, and analysis. Use the task evaluation criteria matrixes published through the Army Training Network as a guide for evaluating crews and platoons.

Whenever possible, integrate combat arms formations and a division G-2 section into the Tier 2 exercise. The multifunction platoon and HUMINT platoon will likely operate in conjunction with a combined arms force during large-scale ground combat operations. Integrate an infantry, cavalry, or armor formation as a training enabler to provide the MI platoons with a partner force to conduct intelligence operations. Integrate military police elements at the detainee holding area to stress detainee handling procedures. When available, request that a division G-2 section establish a cell collocated with the battalion command post to rehearse reporting intelligence and information to a supported headquarters.

Conclusion

Expeditionary-MI battalions can use the MITS framework as a guide for conducting battalion collective training. A proper Tier 2 certification exercise must stress all elements of the expeditionary-MI battalion and use live, virtual, and constructive training enablers to tailor training for each intelligence discipline. The 303rd E–MI BN successfully utilized the MITS framework to develop and implement a training strategy for the unit METL tasks supporting both its collection and analysis missions.

Endnotes

1. Department of the Army, Training Circular (TC) 2-19.400, *Military Intelligence Training Strategy* (Washington, DC: U.S. Government Publishing Office [GPO]), 1 August 2019) (common access card [CAC] login required).

2. Department of the Army, *2019 MI Battalion Expeditionary–Modified Table of Organization and Equipment (MTOE)*, Document Number 34425KFC01 (Washington, DC, 17 October 2018).

3. Department of the Army, TC 2-19.404, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 4* (Washington, DC: U.S. GPO, 23 January 2019) (CAC login required).

4. Department of the Army, TC 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3* (Washington, DC: U.S. GPO, 23 January 2019) (CAC login required).

5. Department of the Army, TC 2-19.402, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 2* (Washington, DC: U.S. GPO, 20 May 2019) (CAC login required).

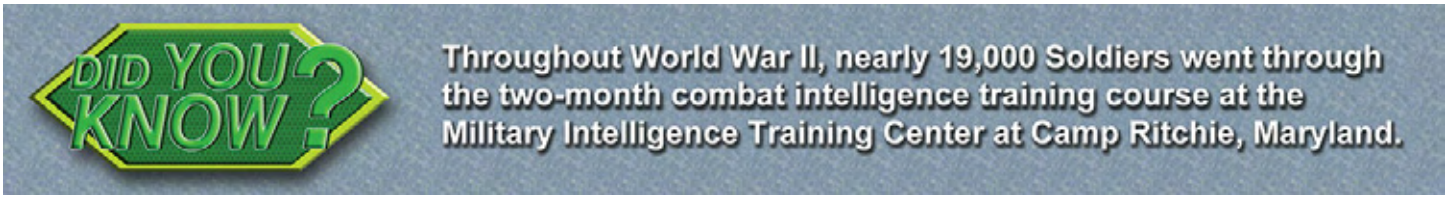
6. Department of the Army, TC 2-19.401, *Military Intelligence Training Strategy for the Brigade Combat Team 1* (Washington DC: U.S. GPO, 14 May 2019) (CAC login required).

7. Department of the Army, TC 2-19.404, *MITS for the BCT Tier 4*.

8. Michael Adamski and William Denn, "82nd Airborne Division Military Intelligence Training Strategy Lessons Learned," *Military Intelligence Professional Bulletin* 45, no. 1 (January–March 2019): 33–39.

9. Department of the Army, Army Techniques Publication 3-91, *Division Operations* (Washington, DC: U.S. GPO, 17 October 2004).

MAJ Ben Smith currently serves as the J-2X Foreign Entity Vetting Branch Chief at U.S. Transportation Command. His previous assignments include operations officer for the 303rd Expeditionary-Military Intelligence Battalion. He holds a master of science in strategic intelligence from the National Intelligence University and a bachelor of arts in history from the University of Dayton.



Building Intelligence Relationships

by Lieutenant Colonel Casey L. Ramirez and Major Megan M. Spieles

Introduction

As many of us already know, intelligence is a commander-centric warfighting function. In order to support the commander, the intelligence professional must establish and maintain an intelligence architecture. Most will agree that when people hear the word "architecture" in a military sense, they think it applies solely to systems and their ability to "talk" to one another. While digital connectivity is important, connectivity alone lacks the most crucial aspect of the intelligence architecture—the relationships among people. Many of the intelligence shortfalls we observed over the last few years as intelligence observer-coach-trainers at the Mission Command Training Program trace back to how people communicated. This occurred not only within organizations, but also with organizations' ability to communicate with higher, lower, and adjacent units in an effort to collectively support the commander's ability to make a decision.

Mission Analysis

In a well-defined mission, the military decision-making process is often where the intelligence officer and staff test the intelligence architecture. The most important step within the process is step two, mission analysis. Intelligence preparation of the battlefield (IPB) is the foundation of mission analysis. IPB is one of three staff functions, as defined in doctrine, and its conduct often defaults to the S-2/G-2. The end state of IPB is that the commander and staff have a thorough understanding of the operational environment and the threats that will affect the mission. As we observed in many units, when it came time to review the order and begin mission analysis, each staff section stove-piped their efforts.

With the exception of one unit we observed, the S-2/G-2 took portions of the base order, Annex B, and Annex L and developed IPB exclusively, often at the direction of the chief of staff or commander. Many intelligence sections did not include the entire staff's input, nor did they know how to do it. It is crucial to remember IPB is a staff process, not something done solely by the S-2. Staff input helps to—

- ✦ Shape focus areas for all warfighting functions.
- ✦ Provide a more in-depth understanding.
- ✦ Develop requests for information and priority intelligence requirements (PIRs).

U.S Army Photo by CPT Jason Sweeney

The 79th Infantry Brigade Combat Team medical officer briefs the command during a combined-arms rehearsal February 12, 2018, at Camp McGregor, NM.

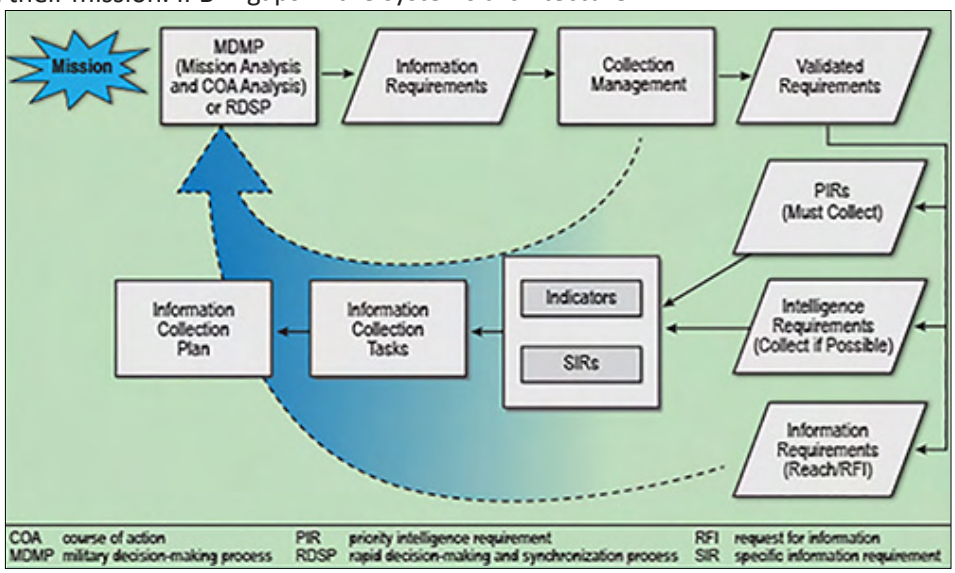
For example, the Fires section is able to understand how the enemy would employ fire systems based on capabilities and the terrain; Logistics can provide knowledge of transportation equipment and insight into what would affect movement; and Signal understands where a command headquarters should position for optimal communications and knows the enemy's capabilities.

Establishing the Architecture

How does the intelligence officer build the relationship architecture? He or she should start by educating the staff on capabilities and the proper conduct of IPB. The S-2 must know what is important to each staff section and what each staff section needs to know about the threat or environment so that they can effectively conduct their mission. IPB is the foundation of the military decision-making process and helps ensure the staff can develop feasible courses of action—this is how to create "symbiotic" intelligence. The staff feeds the S-2/G-2, and the S-2/G-2 in turn feeds the staff. Furthermore, IPB is not a fire-and-forget event. It is continually updated and refined based on a more developed understanding of the operational environment, not just as the threat changes but also as the friendly situation changes.

The aforementioned concepts can also apply to establishing the overall architecture. The intelligence section needs to build a close relationship with the S-6 to discuss systems and capabilities, and with the operations section to discuss the command post layout and ways to ensure all Army Battle Command Systems can talk to one another. Without this dialogue, the unit cannot properly build its digital architecture to ensure the commander has the most relevant and accurate common operational picture. Another planning factor often overlooked is the 35T (military intelligence systems maintainer/integrator) support required to sustain intelligence systems (especially if the unit did not conduct proper training to establish and maintain its systems architecture). This is apparent when S-2 sections are not able to establish or re-establish their architecture after a command post displacement, or execute a primary, alternate, contingency, and emergency plan when that architecture is lost.

Conversations with higher headquarters need to occur to determine who will establish the overarching architecture. Based on observations, the corps and/or division headquarters should be the leading effort to establish an architecture and capture the process in a standard operating procedure. It is necessary to conduct rehearsals using the standard operating procedure before the execution of any combat training center or warfighter exercise. A shared responsibility should also exist among the corps, division, and unit S-2s to ensure there is a plan for intelligence systems maintainers to support units that do not have the requisite military occupational specialties in their modified table of organization and equipment in order to sustain the equipment. We will not see support from field service representatives during large-scale ground combat operations as we have during warfighter exercises; therefore, units should rehearse as often as possible in today's environment to determine current gaps in the systems architecture.



Requirements Development[1]

Understanding Priority Intelligence Requirements

Another challenge we saw repeatedly is the understanding of PIRs. Staffs know what the acronym stands for and what PIRs are, but they don't understand the PIRs' role in the commander's critical information requirement. Staffs also struggle with the importance and purpose of PIRs. The purpose of a PIR is to drive the intelligence section to fill the gap in knowledge the commander has about the threat or environment so that he or she can make an informed decision. The staff must link a PIR in space and time to friendly decision points to give the commander a complete picture that will support decision making. PIRs become more relevant and manageable when built for each phase of the operation. The situation template and event template built during IPB can make this possible. A properly built situation template and event template should give the intelligence staff and operations staff an understanding of when and where they should see threat activity. This is crucial for the

intelligence and operations staffs to synchronize, especially since the S-3 tasks information collection assets through orders or fragmentary orders. How do the intelligence staff and operations staff manage this? With tools such as the decision support matrix and collection matrix. The value of the decision support matrix and collection matrix is immeasurable because they link PIRs (knowledge about the threat) and information collection to each decision the commander has to make.

Outside the Organization

As we discussed the architecture within the organization, we also need to mention the architecture outside the organization, which for most brigades is extremely important. Intelligence officers must establish relationships with other organizations across the intelligence community. They do this by synchronizing their efforts with units and echelons—higher, lower, and laterally. This also consolidates collection efforts. The linking of collection efforts creates "national-to-tactical intelligence" and can serve intelligence and operations sections well, especially those units in the support and consolidation area that do not have a lot of organic collection capability. This, of course, is challenging if we do not establish a well-defined architecture before execution.

Conclusion

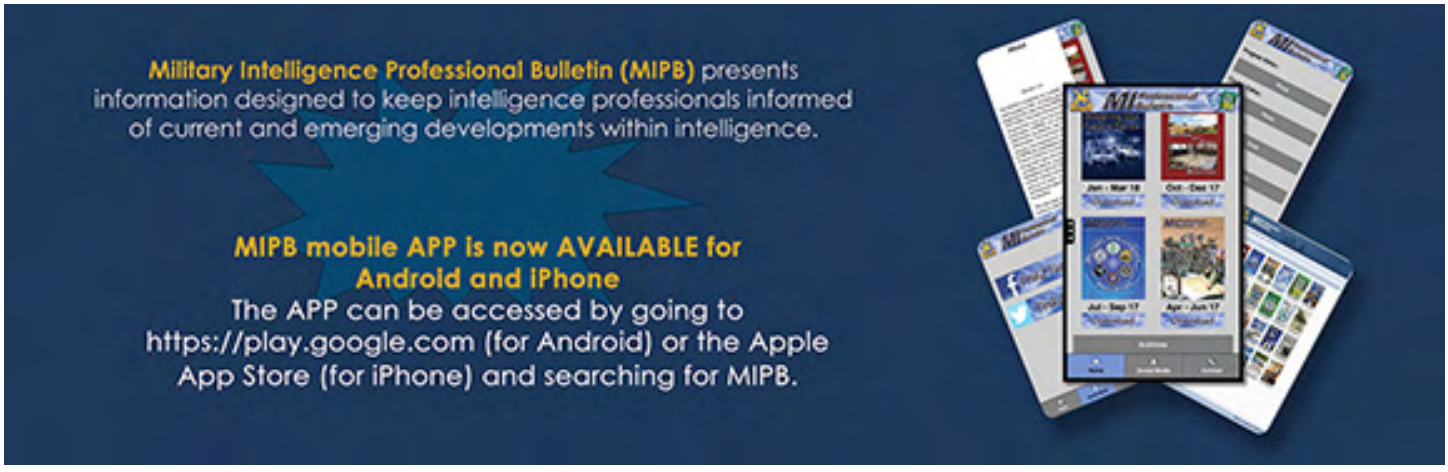
Intelligence architecture is crucial to supporting the commander's decision-making process. The coordination and continuous communication between staff sections, key individuals, and organizations are the core of the intelligence architecture. It is how collective and reinforcing intelligence relationships are created and maintained. It goes far beyond just digital systems and cannot be built behind a desk or solely through emails. Start by visiting staff sections across the formation. Participate in their processes before execution in order to identify shortfalls, not only to assist their commander but to assist yours as well. Build your architecture and build relationships early, with a genuine effort, to help one another and fight the fight together. You will find it rewarding to your commander, staff, and warfighting function—and to yourself as a standard-bearer in our profession of arms.

Endnote

1. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, 31 July 2019), 3-4.

LTC Casey Ramirez is currently the Deputy Chief of Military Intelligence Programs, Intelligence Security Cooperation and Engagement Division, J-2, U.S. Africa Command. He has more than 18 years of intelligence and maneuver experience. His previous assignments include serving as an intelligence observer-coach-trainer in Operations Group S, Mission Command Training Program (MCTP), Brigade S-2, 82nd Airborne Division Sustainment Brigade, and Corps G-2 Planner, XVIII Airborne Corps, as well as a variety of command and staff assignments in the United States, Europe, and the Middle East. LTC Ramirez earned a bachelor of arts in history from Florida State University and a master of arts in business and organizational security management from Webster University.

MAJ Megan Spieles is currently the 555th Engineer Brigade S-2. She was an intelligence observer-coach-trainer in Operations Group S, MCTP. She has more than 12 years of chemical and intelligence experience. Her previous assignments include serving as the 7th Infantry Division G-2 Analysis and Control Element Chief, company commander in the 201st Battlefield Surveillance Brigade (Expeditionary-Military Intelligence Brigade), and Battalion S-2, 801st Brigade Support Battalion of 4th Brigade Combat Team, 101st Infantry Division, as well as a variety of command and staff assignments, with two deployments to Afghanistan. MAJ Spieles holds a bachelor of science in elementary education from Bloomsburg University of Pennsylvania.



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

by Ms. Beth Leeder

Introduction

Welcome to the inaugural ***Training Readiness: From Our Fort to Yours!*** The purpose of this column is to open a dialogue between the institutional training domain (U.S. Army Intelligence Center of Excellence [USAICoE]) and the operational training domain (you) to enhance learning and create "seamless transitions as Soldiers move into and out of operational units and institutional opportunities."[1] Said another way, this column will share resources you can use with your Soldiers to enhance their learning and ultimately their readiness. In this initial column, I will introduce myself, discuss the difference between a brief and a learning opportunity, and provide one tip you can use to enhance learning in your units.

It seems to me that being a successful military intelligence (MI) professional is a combination of what you know (the science of the profession), how you use what you know (the art), and how much experience you have using what you know. The same is true with learning. I have spent my entire career (34 years) studying, researching, and working in the business of learning, first as a public school teacher and for the past 13 years as a Department of the Army Civilian at USAICoE. I currently lead staff and faculty development, curriculum design, and educational technology development for USAICoE. Learning is literally in the name of the division I lead—Teaching, Learning, and Technology Division, which is part of the Directorate of Training. Every day we work with the officers and noncommissioned officers of the MI Corps stationed at Fort Huachuca, Arizona, to figure out the most effective way to train and educate your Soldiers while they are at the schoolhouse. This column will blend the science and art of learning we use every day into observations, suggestions, and resources that will help you train the MI Soldiers you lead.

Four Key Points to Help Get a Student's Attention

So let's get down to business. Imagine it is early on a Tuesday morning after a long weekend. You arrive at work and find out you have to give a mandatory 350-1 training brief in the unit classroom at 1300. You know the kind…lots of PowerPoint slides that everyone has seen before. The training is important to your unit and its Soldiers, but for learning to occur, Soldiers have to pay attention and this is not an easy thing to achieve in a traditional brief. In fact, "training brief" is a bit of an oxymoron because training briefs are not usually set up to facilitate training or learning. In his book *Brain Rules,* Dr. John Medina gives four key points for getting and maintaining the attention necessary for learning to occur.[2] You can use these four points to transform the brief into a true learning opportunity:

- Emotions Get the Brain's Attention.
- Meaning before Details.
- The Brain Cannot Multitask.
- The Brain Needs a Break.

1. **Emotions Get the Brain's Attention.** Finding a way to connect the topic of the brief to an emotion is a good way to start. The most common technique involves using a personal story—yours or, with permission, the story of someone in the organization. But think beyond the story. A video clip, a newspaper article, a podcast sound bite, or even a picture can arouse emotion in your audience. Surprisingly it doesn't matter what the emotion is—empathy and fear could work equally well—as long as they tie to the content.

Announcing you have doubled the time allotted for the brief (undoubtedly making people angry) would not result in better learning, just angry people.

2. **Meaning before Details.** Deliver the meaning of the brief before the details so that Soldiers get the *gist* or crux of what you are talking about. Learning depends on connecting new information to information already present in the brain. Providing the gist first gives Soldiers a way to connect and organize the new information. The brain is really bad at remembering details, yet we tend to focus on providing lots of details when we brief. Soldiers will remember the gist far longer than the details, so if the details are essential, make sure your Soldiers know where to find them after the brief is over. For example, most 350-1 requirements are based on an Army regulation. Provide a link on the unit website, or if you can, add the link to any handouts you use.

3. **The Brain Cannot Multitask.** Regardless of what your teenager has told you, anything that draws the learner's attention away from the brief, like a cell phone, ambient noise, or even the temperature of the room, will decrease the Soldiers' attention. It is important for you to establish an environment as free of distractions as possible. This includes your slides. Ever seen a slide so full of pictures, colors, and really small font that it made your eyes cross? When you are creating slides for the purpose of learning, the less text the better. Can you replace some of the text with a picture or graphic to show the gist? Remember, Soldiers aren't likely to remember all that detail/text, but they may remember the gist of a picture. Don't make your Soldiers multitask by having them read font that is too small while they try to listen to what you have to say. If you absolutely must use the eye-crossing slide, hand out copies for each Soldier.

4. **The Brain Needs a Break.** This is a big one. The brain needs a break after 10 to 15 minutes of listening, and it is going to take one whether you stop talking or not. The break doesn't have to be long but it should be meaningful. For example, having everyone "stand and stretch" will provide a mental break, but since it is not tied to the topic at hand, it is not an effective break. The most effective way to turn a break into a learning opportunity is to include a carefully planned interaction every 10 to 15 minutes or so. Asking a question or providing a situation related to the topic for Soldiers to discuss, write about, or respond to provides a break and helps students make more of those connections we talked about in number 2 above (Meaning before Details).

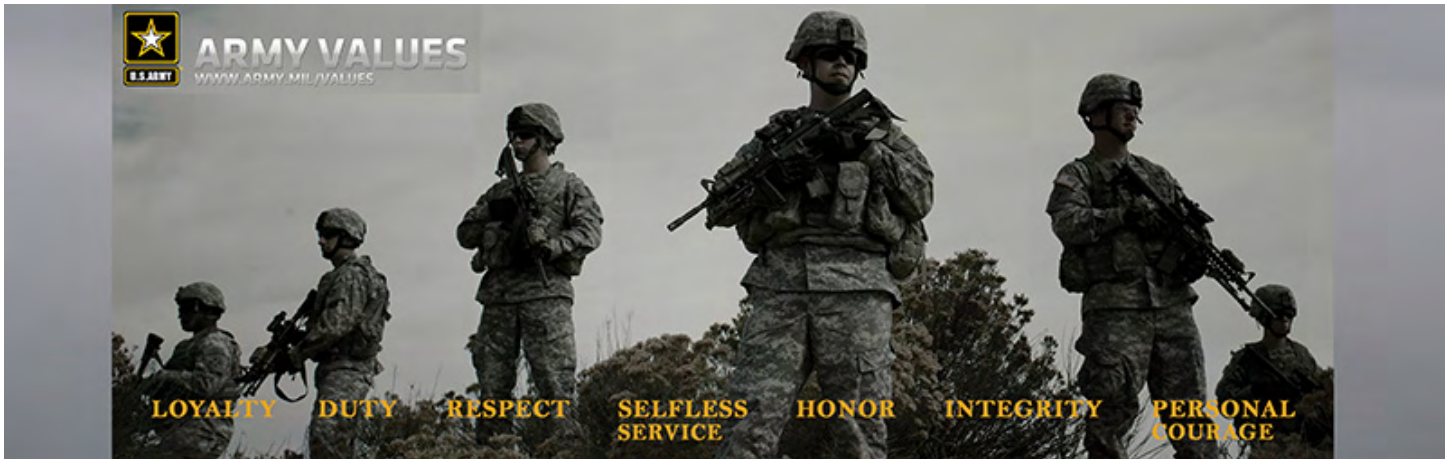
How to Get Help with Learning Techniques

You can apply these four key insights to any interaction you want to turn into a learning opportunity. At this point, you may be wondering how you can get help creating learning opportunities. First, look in your formations! You very likely have Soldiers who have been instructors or training developers. They learn techniques like the ones we've been discussing through the instructor courses taught at USAICoE. Another way to get help is to reach out with your questions through the shout box on the Intelligence Knowledge Network website (https://www.ikn.army.mil) or by contacting us directly. Our Fort is standing by to help in any way we can. Finally, you can look for this column in the next edition of *Military Intelligence Professional Bulletin* (MIPB). Future topics we are kicking around include making the most of distance learning, understanding learners' reactions to failure, and helping Soldiers with professional self-development. What would YOU like to see discussed in future columns? You can contact me through MIPB at usarmy.huachuca.icoe.mbx.mipb@mail.mil. Till then, Always Out Front!

Endnotes

1. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-8-2, *The U.S. Army Learning Concept for Training and Education 2020–2040* (Fort Eustis, VA: TRADOC, April 2017), 16.

2. John Medina, *Brain Rules 12 Principles for Surviving and Thriving at Work, Home, and School* (Seattle, WA: Pear Press, 2008), 71–94.



Change Is Constant—Yet Some Things Never Change

by Mr. Chet Brown, Chief, Lessons Learned Branch

Introduction

A master sergeant, an Army civilian, and a defense contractor walk into a gym one afternoon. Sounds like the opening line of a joke. Regrettably, it only describes what three individuals did upon returning to their intermediate staging base after a full day of tactical ground and air vehicle movement overseas. We had spent the penultimate leg of the day's movement in a C-130, our outbound flight, shoulder to shoulder in red webbed seats facing pallets of musty transit cases and muddy duffel bags. The brief ejection of aerial flares offered the only break from the monotony of the view and drone of the engines. A boring (transport) flight is a good flight. The accommodations and flight profile could have been worse.

The C-130 flight was relaxing compared to the last leg of our inbound flight on a CH-47 Chinook. Shortly after takeoff, we caught glimpses through the helicopter's hellhole of a sling load full of mortar rounds. Then we looked out the rear door and saw another Chinook leaving with a similar sling load. Flying over the mountainous terrain in the CH-47 was not as disconcerting as violating a lesson learned when we initially boarded the helicopter—a lesson previously shared by a combat veteran platoon sergeant during a Friday afternoon work call to "never get on a (Chinook) if you don't see hydraulic fluid on the floor." The indisputable logic of the platoon sergeant was if the bird was leaking, it meant at least some fluid was in the system. A dry floor meant no fluid. No fluid meant no hydraulics. No hydraulics meant no control. Gravity wins every time. Seeing us hesitate during the seating process, the crew chief made a remark that correlated a clean, dry floor with the improved quality and operation of modern hydraulic systems now installed on the CH-47 and other Vietnam-era aircraft. Clearly, this was not the first time he had to dispel a misperception from an outdated lesson.

Heading to the Gym—Mission, Interrupted

Back to the outbound C-130…the U.S. Air Force aircrew allowed the Army passengers to stand, stretch, and move just enough to stay out of the way of unloading the palletized cargo. Pallet cargo had priority over the human cargo. We anxiously waited to deplane and doff the helmet and tactical gear mandated for wear until we cleared the flight line. A brief workout at the gym before evening chow seemed to be a good way to relieve the discomfort of cramped muscles and stiff joints from being crammed into a variety of transport modes since o-dark-thirty. We had to be fresh as we continued on mission the next morning.

Our team's mission was simple. First, meet with the intelligence leaders at the echelons above corps (EAC) to understand the current campaign's overall intelligence production and intelligence interoperability requirements. Then go "downrange" to speak with Soldiers, noncommissioned officers, and officers who were using the latest intelligence processing system laptop computers at the division, brigade, and battalion levels in support of the campaign. We would be able to use the knowledge of EAC operations to understand the national-to-tactical intelligence implementation in theater. Conversations with Soldiers would reveal which of the system's features or capabilities should be changed, added, or removed. The requirement to obtain the full range of input available from all the system's users was too broad and important to levy solely on us—only three people.

We were part of a larger team comprised of computer engineers and software experts from the commercial vendor building the laptops for the Army. The accompanying experts were not the field service representatives or engineers with whom most of us are familiar and on whom we routinely depend. The commercial vendor's experts were the electrical, computer, and system software engineers

who designed and built the system, and who would lead the commercial vendor's employees in refining it. The larger team included personnel from the U.S. Army Training and Doctrine Command (TRADOC) Systems/Capability Manager, Program Executive Office, Program Manager, testing community, training domain, and experts in the national-to-tactical intelligence network. This was a diverse group of professionals dedicated to fielding the best capability to Army military intelligence (MI) Soldiers providing intelligence support to operations overseas.

On our way to the gym, we began to identify the offices of MI personnel at the supported corps and Army Service component command headquarters with whom we could discuss the information gathered and receive additional insights. The three of us had the gym to ourselves as we continued to discuss the work we would need to do once we returned to the continental United States. We agreed the team's most useful contribution would be to help the engineers apply all the pertinent recommendations. Then a televised news bulletin interrupted the session. Our workout, and the plans to meet with the corps and Army Service component command MI leaders, ended when the second plane hit the South Tower.

Then and Now

The September 11, 2001, attack provides an important temporal differentiation between legacy and current MI laptop system lessons learned interest. The team formed in 2001 sought to apply the lessons learned from, and recommendations of, U.S. Soldiers they had visited in Germany and at Camps Able Sentry and Bondsteel in (then) Macedonia[1] and Kosovo, respectively. This task endures, as does our tactical presence in the Balkans. Today, we still collect lessons and recommendations from Soldiers operating MI laptop systems downrange, albeit the area to which the term "downrange" now references has expanded greatly.

Another change between then and now is how MI Soldiers access and leverage the national-to-tactical intelligence enterprise. Our excursion to speak with the Soldiers and supporting personnel at Camp Bondsteel provided a tactical perspective. Meeting with U.S. personnel at the higher headquarters level in Europe provided an operational perspective. What remains important is identifying and sharing the best practices of linking EAC with the tactical force at echelons corps and below. Soldiers use different equipment now than they did then.

The Army listened to the requests of Soldiers and leaders engaged in operations to improve its flagship intelligence processing system. Analysts attempted to use the system contrary to its original purpose of providing rapid, accurate, actionable intelligence to defeat a conventional combined arms threat force. The Army responded to the unanticipated operating conditions by building a smaller, lighter, more mobile (laptop-based) intelligence analysis automation system. Over the next several years, the Army and its corporate partners continued to transform the laptop and its parent family of systems in response to the differing and various intelligence users' continuously evolving tasks, missions, and types of operations.

The Army's current flagship intelligence processing system continues to evolve as rapidly as possible to address current and emerging operational and mission variables. The quick and frequent changes in the operational environment present unexpected challenges in collecting and applying lessons learned to drive system improvements. Personnel returning to areas where they had recently served reported that conditions had changed so much as to be almost unrecognizable. Some offered that their experiential knowledge was obsolete if they were absent from the area of operations for only a month or two. This is just one example of the speed at which the operational environment can change. The adage that change is the only constant definitely applies to Army operations.

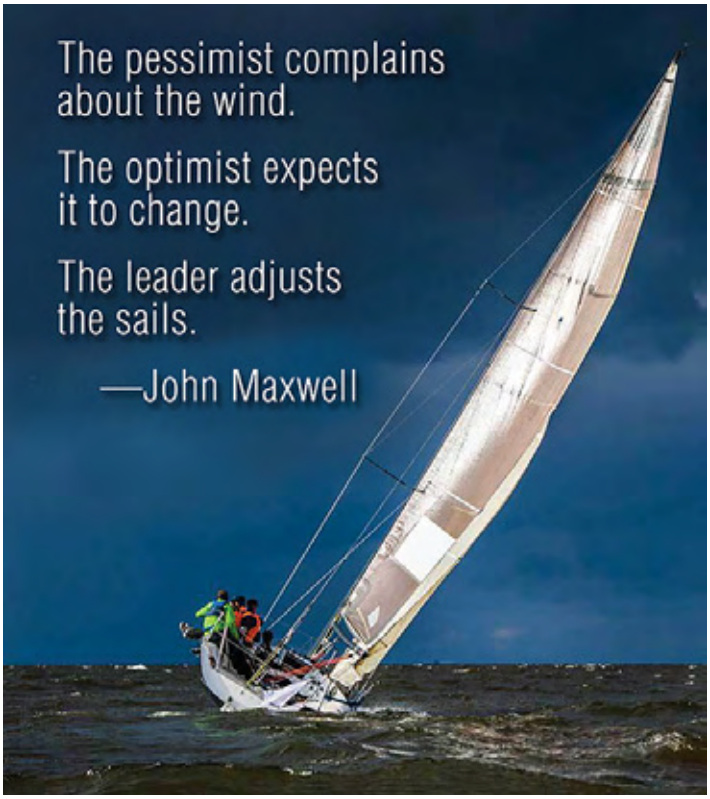
Conversely, some things in the Army never change. This is a different sentiment than the defeatist's lament that "the more things change, the more they stay the same." We know things change. We are all working to improve our profession by adapting to change to improve the situation and not remain the same. We want to adapt in anticipation of and before the inevitable environmental change occurs in order to remain ahead of our competitors. The Army recognizes the superiority of adapting in advance of, and not in response to, changing conditions. Army leaders have not wavered from the value placed on obtaining unfiltered Soldier feedback on Soldier, unit, and equipment performance. Support from EAC Army leaders and intelligence staffs 18 years ago provided the access to Soldiers using laptop computers at the tactical level. Today, with the same level of support from Army and MI leaders, we continue to collect and apply lessons, best practices, and recommendations from Soldiers using the latest intelligence processing laptop system—the Distributed Common Ground System-Army Capability Drop 1.

Commander's Guidance

When drafting this *Military Intelligence Professional Bulletin* (MIPB) submission, I received forwarded email messages originating from several U.S. Army general officers: TRADOC Commander, GEN Paul Funk; Headquarters, Department of the Army, Deputy Chief of Staff G-2 LTG Scott Berrier; and U.S. Army Intelligence Center of Excellence (USAICoE) Commanding General MG Laura Potter. Each email contained an element identifying the value of incorporating subject matter expertise into the Army's modernization efforts. GEN Funk's memo, *Funk Sends #3 – 28 August 19,* mentioned his recent attendance at "the TRADOC's Mad Scientist Conference, where the intelligence community comes together to discuss how future global trends will change our national security outlook and our Army." He emphasized, "TRADOC will be at the forefront of this change, driving constant improvements."[2] Clearly intentioned to be a comment on an aspect of effective leadership, GEN Funk's use of retired GEN Stanley McChrystal's quote "The solution that works perfectly one day can be miserably disappointing the next"[3] underscores the need to seek out what's not working or what we need to work tomorrow. The quote also demonstrates why we are still collecting lessons from Soldiers using laptop computers supporting operations. The laptop solution implemented back then is not the solution we need today. The system we are using today may not be what we need to win tomorrow.

The *Fiscal Year 2020 Combined Arms Center Command Guidance* also provides another example of what used to work may no longer be appropriate in that the "current force that is optimized for the [counterinsurgency and counterterrorism] COIN/CT fight and is not optimized to meet the requirements in the current National Defense Strategy."[4] Specifying the Army has a role in the National Defense Strategy confirms the Army is not alone in the need to apply experiential learning to meet emerging and current threats. In implementing the Combined Arms Center guidance in support of the National Defense Strategy, the USAICoE Commanding General described to us the crucial role of the Intelligence Center of Excellence. MG Potter directed us first to GEN Mark Milley's farewell speech as the Chief of Staff of the Army and then to the remarks of the incoming Chief of Staff of the Army GEN James McConville.[5] The guidance and words of the general officers underscore the inherent responsibility of all MI professionals (uniformed and Civilian) to contribute their unique perspectives and observations to support the readiness and development of our Nation's intelligence warfighting function capabilities.

This recent focus is a natural evolution of the USAICoE Commanding General's initial guidance to the Lessons Learned Team to keep abreast of the fielded force's intelligence and operations activities to discover, validate, and integrate relevant lessons and best practices into the MI force modernization and branch proponent efforts. MG Potter mandated we keep attuned to what the operating force is doing so that we may help ensure MI training and doctrine evolve to keep pace with, and in anticipation of, the field's requirements.



There Are Always Lessons to Be Learned

Performing the lessons learned tasks to fulfill the nested priorities of Army, TRADOC, Combined Arms Center, and USAICoE leaders may seem overwhelming. The good news for the Lessons Learned Team is that we are not alone. We are all in this together. If you are reading this, you are part of the "intelligence lessons learned" effort. If you are, or work with, an MI professional, you have something valuable to add to the discussion. Sometimes we are so close to the problem we may not be aware of the various and differing contributing factors or solutions. We may not be able to see the forest for the trees. We all benefit from information contained in an after action report, white paper, concept, MIPB article, or email telling of a useful technique or effective shortcut.

Intelligence is always engaged; thus, there are always lessons to be learned. The laws of physics prevent the USAICoE

Lessons Learned Collection Team from directly observing the breadth and scope of Army MI activities from the national to tactical. We are able to add value to the Nation, Army, and intelligence enterprise only through your support. You allow us to share what we learn from others with you. You allow us to observe training and operations and to meet with your Soldiers, noncommissioned officers, and officers. You provide after action reports; standard operating procedures; primary, alternate, contingency, and emergency plans; and examples of intelligence products. Your support allows us to provide all that we learn from you to those charged with driving improvements in the institutional, generating, and operating force.

We also depend upon an increasingly expanding lessons learned relationship with the U.S. Army Intelligence and Security Command (INSCOM), Center for Army Lessons Learned, and Army centers of excellence. Applying intelligence lessons learned to all the Army's warfighting functions is critical in anticipating the knowledge demands of training and preparing for large-scale ground combat operations. Impacts in one warfighting function ripple through every other warfighting function. Applying experiential learning (lessons and best practices) to help drive experimental learning (concepts, simulations, experiments, etc.) also helps reveal the challenges of multi-domain operations.

Exercise Defender 2020

We have additional sources of support with the temporary expansion of the intelligence lessons learned contractor capability. We have added two personnel at INSCOM headquarters and another two at USAICoE. The temporary (one-year) increase in the professional lessons learned capability provides some of the additional capacity needed to observe major learning events of the next year such as Exercise Defender 2020.[6] This exercise will span 10 countries throughout Europe (mainly Germany and Poland) from April to May 2020.[7] "Defender 2020 is a Department of the Army-directed, [U.S. Army Europe] USAREUR-led exercise designed to demonstrate the United States' ability to rapidly deploy a division to the European theater. This exercise, the largest in 25 years, will test echelons-above-brigade units in operational-level warfighting and its associated sustainment."[8] Defender 2020 is not Reforger 2.0.[9] Good news for you. It means I will not drag 1990s light infantry battalion S-2 Reforger lessons learned into a future MIPB column. Okay, maybe just one. Don't volunteer to be the washrack officer in charge for an armored unit as thanks for a couple days of hot chow.

I'll end by extending thanks in advance to those of you who are going to contribute your lessons, best practices, recommendations, and invitations in support of Exercise Defender 2020.

Endnotes

1. Macedonia is now the Republic of North Macedonia; this is not referring to Macedonia in Greece.

2. Department of the Army, *Funk Sends #3 – 28 August 19* (Fort Eustis, VA: Training and Doctrine Command, 28 August 2019).

3. Stanley McChrystal, Jeff Eggers, and Jason Mangone, *Leaders: Myth and Reality* (New York: Penguin Random House, 2018), 408, quoted in Department of the Army, *Funk Sends #3*.

4. Department of the Army, *Fiscal Year 2020 Combined Arms Center Command Guidance* (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 2 August 2019), 2.

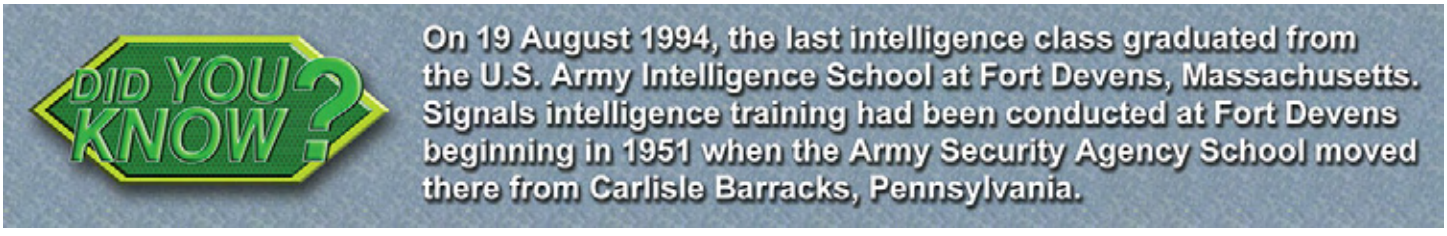
5. Timothy Quinn, email message to U.S. Army Intelligence Center of Excellence (USAICoE), August 12, 2019. Email sent on behalf of MG Potter, USAICoE Commanding General.

6. Edward A. Fraser and Robert V. Abernethy, "Strong Europe: A continental-scale combat sustainment laboratory," *U.S. Army Worldwide News*, April 1, 2019, https://www.army.mil/article/219091/strong_europe_a_continental_scale_combat_sustainment_laboratory.

7. John Vandiver, "Thousands of troops to take part in largest U.S.-led exercise in Europe since the Cold War, EUCOM says," *Stars and Stripes*, 7 October 2019, https://www.stripes.com/news/europe/thousands-of-troops-to-take-part-in-largest-u-s-led-exercise-in-europe-since-the-cold-war-eucom-says-1.602097.

8. Fraser and Abernethy, "Strong Europe."

9. Exercise Campaign Reforger (an abbreviation of "Return of Forces to Germany") was an annual exercise and campaign that the North Atlantic Treaty Organization (NATO) conducted during the Cold War. The exercise was intended to ensure that NATO had the ability to quickly deploy forces to West Germany in the event of a conflict with the Warsaw Pact. Wikipedia, s.v. "Exercise Reforger," last modified 20 September 2019, 02:15, https://en.wikipedia.org/wiki/Exercise_Reforger.



What's the Issue? United States–China Relations

by TRADOC Culture Center

Introduction

The United States is still the world's only true superpower, preeminent in its economic, military, ideological, and cultural reach. But two decades into the 21st century, all indicators are that the People's Republic of China is quickly headed toward superpower status itself. It is second only to the United States in regard to the size of a single nation's economy. It is also rapidly increasing its military spending and is growing more assertive in wielding its influence and economic power around the world. History teaches us repeatedly that when a nation on the rise challenges the existing dominant nation or nations, friction, rivalry, and sometimes conflict are inevitable. Combine this with significant cultural differences, and one has the situation that exists between the United States and China today.

The Chinese are very conscious and proud of what they see as 5000 years of uniquely unbroken ethnic history. Their perception of this history views China as the historical cultural center of Asia, when other countries used to pay tribute to China as the benevolent stewards of Asian civilization. This self-image plays a significant role in what China considers its rightful place in Asia, especially against the backdrop of the late 19th through the early 20th century, which many Chinese call the "Century of Humiliation." Much of Chinese policy today is in part aimed at China regaining its lost pride, its place in the world, and perhaps above all, the means to make itself strong again—in a way that other powers, especially Western ones, cannot diminish. At the same time, in what may seem contradictory to a Westerner, many Chinese also have an admiration for the United States, a country whose industriousness brought it from nonexistence to world preeminence in only two centuries, a chronological drop in the bucket by Chinese historical standards. Indeed, some might see modern China as a 21st century model for capitalism (albeit one overseen by China's authoritarian political rule), an economic system that the United States championed throughout the 19th and 20th centuries.

China is also the birthplace of Confucianism, a philosophy that the government often cites to justify principled government rule over a populace that collectively fulfills its duty by individuals subsuming themselves to what the government determines is best for the people. While the communists officially rejected Confucianism when they took control of China, this collectivist mentality is still a prominent factor in Chinese thought. Although China has many elements of capitalism in its economy, ultimately it is still a state-controlled economy within a communist system. It does not have what we would consider a free press, freedom of movement, or many of the other individual liberties that most Americans take for granted. This is in contrast to the relatively young and more historically forward-looking, less reflective United States, which achieved world preeminence in the 20th century and whose stated ideals of democracy, individual liberties, and international equality, enforced through international law and led by the United States, can come into conflict with China's worldview.

Another major factor to consider when examining United States–China relations is that despite the image of a unified, single-minded Chinese people intent on one common purpose, many potentially destabilizing forces exist within modern Chinese culture—economic, demographic, cultural,

and ideological, to name a few. China's greatest issues are internal. Additionally, Chinese policy often aims to solidify China's domestic atmosphere through developing common goals or causes, or by creating economic advancement and benefit that will win the satisfaction of the people. China, with its vast and unwieldy population, has experienced many foreign invasions over the millennia and incredibly tumultuous and lethal domestic periods since it became communist. This, combined with a 5000-year-old desire to seek and achieve harmony, results in a risk-averse mentality that seeks to eliminate situations that may lead to chaos.

The slogan says "Long live the triumph of Chairman Mao's revolutionary line of literature and art!" and the background shows the town of Yan'an, where Mao Zedong declared that all art and literature should serve politics first and art second. Characters from the revolutionary operas, 1974. Jiasheng Ding; Shanghai Theatre Academy (est.1945).

Roots of Contention

Century of Humiliation. Chinese officials did not meet with United States representatives during their first attempt to establish relations with China in 1784, but by the early 1810s, the opium trade between Western countries—led by Great Britain—and China had begun. To varying extents, many Western countries felt resentment at the way the Chinese government treated foreigners as inferiors who needed to acknowledge their subordination to the Chinese Empire. They also resented China for believing that Chinese culture was more superior and richer in history than all others were and that the Chinese emperor was emperor of the entire world.

In 1839, China sought to end the opium trade and confiscate stores of the addictive and damaging drug sold by Western countries, primarily Great Britain. The Western countries, once again led by Great Britain, refused to cooperate and went to war with China in what is now known as the First Opium War. England won decisively, forcing China to continue allowing the opium trade (in which the United States was engaged as well), to pay silver, and to open up even more cities to trade with the West. While the United States was not directly involved in the fighting and was generally looked upon with a bit more tolerance than some of the other European nations trading in China, Americans were still foreigners and in this way were associated with some of the anger about the Opium War in the public consciousness.

The Second Opium War involving England and France against China started in 1856 over the Western countries' perceptions that China was not living up to the treaties it had signed after the First Opium War. This also ended in a crushing Chinese defeat. The Chinese know the series of treaties China signed after the Opium Wars, such as the Treaty of Nanjing in 1842 and the Treaty of Tianjin in 1860, as the Unequal Treaties. In this series of treaties, China had to open up many trading ports, relax trade restrictions, grant legal extraterritoriality, and allow Western traders to build and live in expatriate communities and worship as they chose within Chinese territory. In return, the Western powers would not attack China. These losses in the Opium Wars began a period known in China as the "Century of Humiliation."

After the Opium Wars, the Chinese government, which had weakened and lost prestige, had to deal with several destabilizing incidents that came about as a result of the Western presence in China. These incidents included the Sino-Japanese War, the internal Taiping Rebellion, and the 100 Days Reform Movement. They also included the Boxer Rebellion, which the Chinese government initially opposed but later partially embraced. The Boxer Rebellion resulted in open conflict against Western powers (including the United States) and Japan, whose militaries ended the rebellion and then extracted massive monetary reparations and even more territory concessions from the Chinese government. This period was accompanied by massive famine and poverty in the majority of China, which was rural and

agricultural. All of this damaged and eventually led to the fall of Imperial China.

Then, in World War I, the Chinese sent more than 100,000 troops to Europe to fight on the side of the Allied powers. But at the war's end, Chinese territory that the Germans had controlled was not given back to China by the victorious Western powers but instead was given to China's enemies, the Japanese. Less than 20 years later, the Japanese invaded China and commenced a brutal occupation that directly or indirectly cost the lives of approximately 40 million Chinese.

Photo by rheins1

Shiyu, or Lion Islet, part of Kinmen County, one of Taiwan's offshore islands, seen in front of Xiamen, China, on September 7, 2014. Just off Kinmen's shores are the glass-walled high-rises from the booming mainland port of Xiamen in one of China's most prosperous provinces.

This "Century of Humiliation," from the First Opium War until the establishment of the communist People's Republic of China in 1949, is something both actively taught in schools and invoked in public pronouncements by the Chinese government. Seen from a Western perspective, many modern Chinese seem to look at this period more as a lesson and catalyst for resolute progress and development than a source of openly expressed anger with the West.

Treatment of Chinese Immigrants in the United States. In the United States, there was an influx of Chinese immigrants after the 1849 Gold Rush in California. Chinese immigrants also often ended up working on the construction of the railroads, in factories, and on farms. Some even managed to become business owners. Racial hatred, stereotypes about Chinese being drug pushers and all Chinese women being prostitutes, and fears about Chinese immigrants taking Americans' jobs resulted in great discrimination. Chinese were paid lower wages, had their rights legally restricted or eliminated altogether, were barred from gaining citizenship, and were the subject of a great deal of physical violence, including the murder, physical assault, and property theft of hundreds of Chinese. Many laws were passed specifically to limit the rights of Chinese residents in California. Numerous cities sought to remove all Chinese from their limits, and eventually the Chinese Exclusion Act banned almost any Chinese from immigrating to the United States. These laws were the first immigration-limiting laws in American history. Within China, this discrimination against Chinese created some ill feelings toward the United States.

People's Republic of China. By the mid-20th century, just before and after the Japanese occupation and World War II, China was engaged in a civil war between the Nationalists, who were allies of the democratic United States, and the Communists, who were allied with the Soviet Union. (The two sides had fought together against the Japanese.) In 1949, the Communists under Mao Zedong eventually won and allied themselves with America's Cold War foe, the Soviet Union. The Nationalists fled to what is known today as Taiwan. The United States did not recognize the communist government that controlled all of mainland China, known as the People's Republic of China, as the legitimate government of China. Instead, it recognized the Nationalists in Taiwan, the Republic of China, who claimed they were the true government of all China.

In the years before and during World War II, the Japanese occupation of parts of China was brutal and involved many atrocities. Though the United States decisively fought and defeated Japan in World War II, immediately afterward the United States helped rebuild Japan into the capitalist economic power that it is today and became allies with the island nation not much more than 500 miles away from the Chinese coast. The Japanese treatment of the Chinese during their occupation is very much in the collective consciousness of the Chinese.

During the Korean War (1950–1953), China (along with the Soviet Union) supported North Korea against the United States and South Korea. Later, when United States forces had fought up to the North Korean–Chinese border, the Chinese

fought the United States in open warfare. The Korean War eventually ended in a stalemate; to this day, China is an ally of North Korea, and the United States is an ally of South Korea. The Korean War has never been declared officially over, though that may change in the near future.

In the Taiwan Strait Crisis during the mid-1950s, the United States–backed Nationalists in Taiwan deployed to some nearby Chinese islands. The People's Republic of China considered this an act of aggression by the Nationalist government and responded by shelling the islands with artillery. The United States then indicated it would use military force to defend Taiwan itself. Eventually, the Chinese agreed to negotiate and the hostilities ended.

The Chinese asserted control of Tibet in 1950, and when there was a Tibetan uprising against Chinese rule 9 years later, the People's Republic of China's response killed thousands. The United Nations and the United States condemned these actions, which supported Tibetan resistance. China claims that Tibet has been part of China for centuries, and based on that interpretation of history, it is part of China. Today, the United States recognizes Tibet as part of China.

In 1964, China tested its first nuclear bomb, adding a clear level of threat to the United States in the "capitalist democracy versus communism" cold war.

The Chinese, along with the Soviets, supported the communists in North Vietnam and the Viet Cong insurgents in South Vietnam against the United States and South Vietnamese government during the Vietnam War.

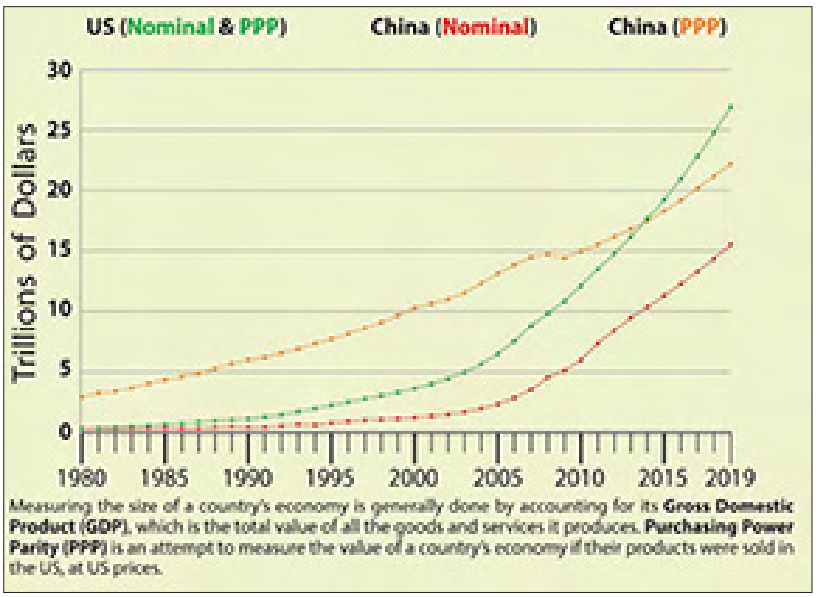
Later, when the Soviet Union and China split over various political and ideological differences, the United States reopened relations with the People's Republic of China for the first time as part of the United States strategy to defeat the Soviet Union, eventually recognizing the People's Republic of China as the legitimate government of mainland China.

Relations improved for some time until what is known in the West as the Tiananmen Square protests. The initial Tiananmen Square protest in the spring of 1989 resulted in student-led demonstrations against elements of the government, which occurred in many cities regarding a variety of issues, especially corruption, the effect of economic policies on urban dwellers, and the need to allow a greater expression of beliefs and grievances. The People's Republic of China government stopped the protests with violent measures and many people were killed or wounded. Several countries around the world, including many voices in the United States, were angered by this and called for sanctions. The United States suspended arms sales and high-level visits to China and implemented some economic sanctions, and relations grew more distant for a while. But in the long term, the United States has recognized China's economic importance on the world stage.

After the Tiananmen Square protests, China's economic policies became much more capitalist and much less communist, resulting in a rapidly growing and booming economy. In 2000, the United States normalized trade relations with the People's Republic of China. In 2001, China was allowed into the World Trade Organization and became a permanent Most Favored Nation of the United States, giving it highly favorable trade terms with the United States. China continued its rapid rise in economic wealth and power, becoming the United States' largest foreign creditor in 2008 and the world's second-largest economy in 2010.

The Issues

Economic Competition. The United States and China are the world's two largest single-nation economies, the United States having had the world's largest economy for the better part of the last 150 years. However, the current rate of growth puts China's economy on a path to surpass the United States, and by some measures, it has already. Historically, this makes competition and perhaps even conflict between the United States and China almost inevitable. Many of the region's countries risk alienation depending on whether they align themselves (for economic or security reasons) with China or the United States. China is aggressively seeking out raw materials and resources to power its economy and is therefore establishing relationships all



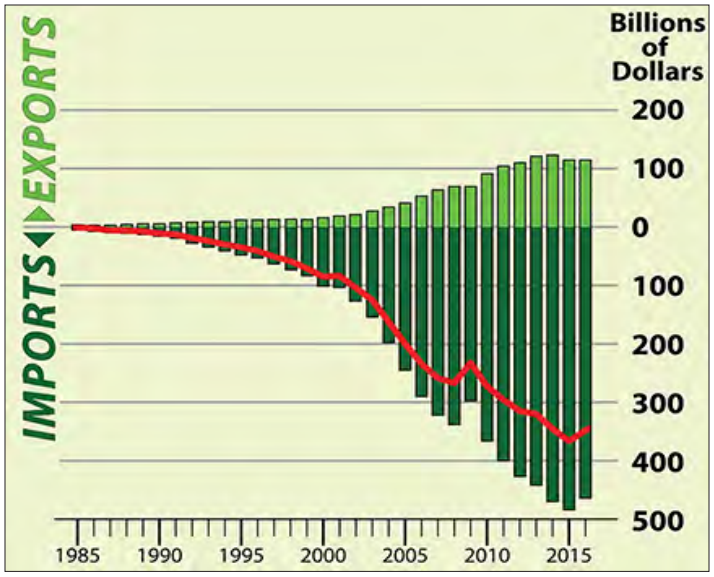
United States vs China GDP

around the globe. This often puts China in situations in which it is competing with the United States' interests economically and, inexorably, politically, socially, and even militarily.

Trade. The United States has a large trade deficit with China—with the United States buying close to $400 billion more of Chinese products than China buys from the United States. The United States believes this is fueled by restrictive Chinese trade practices that limit the amount of investment American entities can make in China and limit the number of goods and services the United States can export to China. This, in turn, not only limits potential American business profits but also can negatively affect American jobs. In the summer of 2018, the United States implemented tariffs and restrictions on multiple Chinese imports, including steel, aluminum, electronics, and clothing and began considering others to deal with what are considered unfair trade practices by the Chinese, as well as their technological and intellectual property theft. The Chinese believe they are still a developing economy with an average standard of living well below that of the United States and other developed countries and, as such, need to protect their economic growth and long-term prospects to provide a better quality of life to their citizens. They responded to U.S. trade restrictions with tariffs and restrictions of their own on U.S. products. China is also pushing for Chinese-Russian trade to be conducted exclusively in Chinese and Russian currency rather than the United States dollar, which has been the currency of international commerce for quite some time.

Intellectual Property/Cyber Theft. The United States finds Chinese practices of cyber theft and coercive procurement of business technology and information a very serious problem that is a crime, an act of aggression, and certainly detrimental to the United States' technological and informational edge. Many Chinese see the acquisition of technology and information as essential to China's prosperity and, by extension, their domestic welfare and security. China is also a communist society, albeit in a form unique to China. As such, Chinese may not see violating capitalist laws and standards to obtain for-profit, private intellectual property as negative, but rather as something that is more egalitarian, leading to more people being able to share in knowledge, which is a good thing. The Chinese also point out what they see is the United States' hypocrisy on the issue of hacking and nefarious cyber practices, especially given the revelations that came about as a result of Edward Snowden's espionage and theft.

Taiwan. The People's Republic of China considers Taiwan a province that is both historically and currently part of their country, as declared in their "One China" policy. This



United States Trade Deficit with China

is despite various Taiwanese political factions considering Taiwan as somewhere between a completely different nation and an independent, self-determining part of a single Chinese country. The People's Republic of China has stated that any actions involving a tangible attempt to support Taiwan's separation from the People's Republic of China will be considered an act of war.

The United States considers Taiwan's status as unsettled. While the United States does not support the idea of Taiwanese independence, it does not officially oppose it either. The United States officially "acknowledges" (notes the existence of) the People's Republic of China's "One China" policy but does not officially confirm the United States' support for it. In 1979, the United States established the Taiwan Relations Act, which allows the United States to sell defensive weapons to Taiwan and gives the United States the option to defend Taiwan militarily if necessary, according to what Congress determines. The People's Republic of China sees this as an intrusion into domestic politics and objects to the United States' arms sales to Taiwan. The United States' policy can be generally described as one designed to minimize open conflict between Taiwan and the People's Republic of China without angering the People's Republic of China too much.

North Korea. North Korea is an ally of China. Though China has had several occasions to be unhappy with North Korea, the two countries are still allies and comrades in their declared communist forms of government. North Korea also provides a land buffer between China and South Korea, a United States ally. China has already clearly shown during the Korea War that it does not want the United States or South Korea near the Chinese border. The United States, on the other hand, sees North Korea as a clear threat. It is

a nation that has invaded South Korea before and lethally attacked American and South Korean personnel in multiple incidents since then. It is currently a nuclear-armed nation that not only continues to develop nuclear weapons capable of hitting the United States and its allies but also openly and proudly proclaims it is doing so. China's support of North Korea, in general, and the perceived lack of strong measures by China to try to control its ally have been a source of great dissatisfaction for the United States. The long-term nature of the complicated relationship between China, North Korea, South Korea, and the United States is yet to be determined.

Human Rights. The United States and United Nations have cited China as a human rights violator in many areas: free speech, internet, press, religion, movement, association, political choice and practice, physical treatment of many of its citizens (including rural workers), treatment of many ethnic minorities, torture, wrongful executions of accused criminals and political prisoners, and a variety of other issues.

China objects to these accusations in several ways. First, it cites what it sees as the United States' hypocrisy on human rights, given our invasion of Iraq, rate of incarceration, racial and class issues, breakdown of families, extremism, and crime, to name a few. Second, China considers itself a developing country, where uplifting the quality of life for all its citizens requires measures that countries such as the United States also employed when it was still developing, in order to ensure a secure and prosperous future. These factors and the difference in cultures, many Chinese argue, put China in a different situation than the United States—one that cannot be assessed according to the same cultural expectations or standards. Third, China has a generally collective culture that seeks societal harmony above the needs of individuals. To the Chinese government, the welfare and security of the many and the means necessary to secure them are more important than the needs or wants of a relatively small number of people. This is a clear contrast to the United States' individualist culture, which the Chinese often perceive as chaotic, disorderly, and fractious.

Additionally, China has well over four times the number of people as the United States and has serious issues, including aging population demographics and difficulties related to its massive rural-to-urban migration over the past few decades. Analysts generally agree that China has to do everything in its power to keep the country united and on the same path, despite its public image of one vast, unified people, all marching to the same beat.

Maritime Disputes. China claims large areas of the South and East China Seas, along with several landmasses in those areas. These seas have billions of dollars in commerce passing through them every year and have massive oil and natural gas resources. China is also building islands and modifying reefs in the area to hold and supply military equipment, vessels, and personnel.

If one looks at the map, it quickly becomes apparent why these seas are physically important to China. To the east and south lie the United States' allies or countries traditionally aligned with the United States, effectively encircling China's Pacific coast. By gaining control of the South and East China Seas, China ensures commercial and military access to the Pacific and can counter any perceived United States military, political, or economic influence in the area.

China treats these areas as if they were Chinese territory, which means they push out other countries that are operating according to international law or those own countries' maritime or territorial claims. China often cites historical or claimed historical presence in these areas as justification for their assertions of control. China often views international law as laws made by, and for the benefit of, Western nations when they were unquestionably the dominant

Map of Areas Claimed

powers in the world, and not necessarily in line with Chinese culture and interests. In the Chinese consciousness, these laws also harken back to the Century of Humiliation when policies made in the name of free international trade were forced on China by Western powers.

The South China Sea is one of the most oft-traveled waterways in the world. Each day, thousands of vessels from many different countries travel and carry on international commerce vital to the region and the world as a whole. Most of the countries in the area believe they have the right to freely navigate it and claim waters close to their nations as their own. As a matter of principle, the United States supports internationally recognized law for determining the location of a country's maritime borders rather than international waters. The United States also supports these rules because they facilitate free trade and provide relatively equal rights to countries regardless of their size and power, including those countries that are U.S. trading partners and allies. The United States does not want China to control the South and East China Seas because this conflicts with international law and might create a Chinese stranglehold over Asian maritime commerce at the expense of other nations in the area. Many observers argue that these maritime disputes may eventually escalate into military conflict.

Endnote

1. rheins [CC BY 3.0 (https://creativecommons.org/licenses/by/3.0)].

Want to Learn More about China?

The role of history in Chinese policy:
https://www.theatlantic.com/china/archive/2013/10/how-humiliation-drove-modern-chinese-history/280878/.

https://www.nytimes.com/2017/07/13/opinion/chinas-quest-to-end-its-century-of-shame.html.

The treatment of Chinese in American history:
https://www.loc.gov/teachers/classroommaterials/presentationsandactivities/presentations/immigration/chinese4.html.

http://www.pbs.org/becomingamerican/ap_prog1.html.

The history of the People's Republic of China's relationship with the United States:
https://www.heritage.org/asia/report/the-complicated-history-us-relations-china.

https://www.cfr.org/timeline/us-relations-china.

http://uscpf.org/v3/wp-content/uploads/2014/08/backgrounder-on-United States-China-relations.

United States–China trade issues:
https://www.everycrsreport.com/reports/RL33536.html.

https://www.thebalance.com/u-s-china-trade-deficit-causes-effects-and-solutions-3306277.

https://www.brookings.edu/blog/the-avenue/2018/04/09/how-chinas-tariffs-could-affect-u-s-workers-and-industries/.

Theories on why the Chinese engage in certain practices and how to deal with these issues:
https://www.theepochtimes.com/why-china-will-not-abandon-theft-in-its-strategy-to-surpass-us-economy_2502976.html.

https://www.usatoday.com/story/opinion/2018/03/31/donald-trump-china-intellectual-property-theft-column/458320002/.

http://thehill.com/opinion/finance/379800-intellectual-property-will-make-or-break-us-china-relations.

http://thehill.com/opinion/cybersecurity/385379-to-stop-chinas-technology-theft-the-us-needs-a-people-warfare-strategy.

Taiwan as an issue between the United States and China:
https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/30/china-u-s-taiwan-relations-are-in-choppy-waters-heres-whats-going-on/?noredirect=on&utm_term=.6207a96053b8.

https://www.npr.org/2018/04/10/601215534/the-taiwan-travel-act-threatens-to-further-complicate-u-s-china-relations.

China's view of North Korea:
https://www.cfr.org/backgrounder/china-north-korea-relationship.

https://www.nytimes.com/2018/04/22/world/asia/china-north-korea-nuclear-talks.html.

http://www.scmp.com/news/china/diplomacy-defence/article/2143145/why-china-remains-cautious-over-prospects-breakthrough.

Human rights in China:
http://www.scmp.com/news/china/policies-politics/article/2142765/china-named-force-instability-us-human-rights-report.

https://thediplomat.com/2016/04/china-us-accuse-each-other-of-human-rights-violations/.

China's disputed maritime claims:
https://www.businessinsider.com.au/why-the-south-china-sea-is-so-crucial-2015-2.

http://theconversation.com/why-is-the-south-china-sea-so-important-to-the-us-71477.

https://www.brookings.edu/opinions/risk-of-u-s-china-confrontation-in-the-east-china-sea/.

Moments in MI History

Courage Under Fire: SFC Eugene Ashley, Jr., and the Battle at Lang Vei

by Lori S. Stewart, USAICoE Command Historian

On 6 February 1968, American personnel at a U.S. Special Forces camp named Lang Vei were tense. Located approximately 5 miles southwest of the Marine base at Khe Sanh, the camp was home to two 12-man Special Forces detachments, 14 South Vietnamese special forces soldiers, 280 Montagnard Civilian Irregular Defense Group strikers, and 161 H're tribesmen of the Mobile Strike Force. Because the camp was close to the Laos border, the camp itself and the surrounding area was also supporting 520 Laotians of the 33rd Laotian Volunteer Battalion and an additional 2,200 dependents who had survived a recent enemy attack on their camp. Throughout late 1967 and into 1968, North Vietnamese Army (NVA) and Viet Cong artillery fire had targeted Lang Vei often, and intelligence reports indicated enemy battalions were crossing the river along the Laos border. Earlier that morning, an enemy mortar barrage had awakened the camp and dinnertime was interrupted by an artillery attack. Personnel at defensive positions around the camp reported hearing engines idling and other strange noises. During the Tet holiday just a week earlier, the NVA and Viet Cong had attacked locations throughout South Vietnam. Now, an NVA division was headed for the Marine base at Khe Sanh, and the camp at Lang Vei was in its path. An attack on the U.S. camp was imminent.

Map courtesy of U.S. Army

Location of the Special Forces camp, close to the Laos border

Shortly after midnight on 7 February, an NVA combined infantry-tank assault drove through the perimeter fences into Lang Vei. This represented the first use of tanks by the North Vietnamese, and the unprepared forces at Lang Vei were immediately overwhelmed. The enemy destroyed the camp's ammunition and fuel dumps, leveled heavy weapons positions, overran bunkers, and blocked all avenues of approach to the camp.

Less than a mile away, SFC Eugene Ashley, Jr., the intelligence sergeant for Company C, 5th Special Forces Group (Airborne), 1st Special Forces, watched the horror unfold at the Lang Vei camp and volunteered to help relieve the camp.

Photo courtesy of U.S. Army

SFC Eugene Ashley, Jr.

As a 20-year old, Eugene Ashley, Jr., joined the Army in 1951 and served in the Korean War with the 187th Regimental Combat Team. Choosing to remain in the Army following the Korean War, he filled a variety of infantry assignments before completing Airborne School in 1956. He was promoted to sergeant in 1961 and served as a cavalry and armored battle group squadron leader and company sergeant with an airborne battalion. In 1965, as a staff sergeant, he deployed with the 82nd Airborne Division in Operation Powerpack, the United States intervention in the Dominican Republic. He was promoted to sergeant first class later that year; then he volunteered to join the Special Forces. In 1967, he deployed to Vietnam.

For the next 10 hours, SFC Ashley led a series of counterattacks against the enemy forces at Lang Vei, calling in airstrikes on the enemy fighters and his own position. During the fifth counterattack, Ashley was mortally wounded. His Medal of Honor citation best tells the story:

On 6 and 7 February 1968, Sergeant Ashley was the Senior Special Forces Advisor of a hastily organized assault force whose mission was to rescue entrapped United States Special Forces Advisors at Camp Lang Vei. During the initial attack on the Special Forces camp by North Vietnamese Army forces, Sergeant Ashley supported the camp with high explosive and illumination mortar rounds. When communications were lost with the main camp, he assumed the additional responsibility of directing airstrikes and artillery support. Sergeant Ashley organized and equipped a small assault force composed of local friendly personnel. During the ensuing battle, Sergeant Ashley led a total of five vigorous assaults against the enemy, continuously exposing himself to a voluminous hail of enemy grenades, machinegun and automatic weapons fire. Throughout these assaults, he was plagued by numerous booby-trapped satchel charges in all bunkers on his avenue of approach. During his fifth and final assault, he adjusted airstrikes nearly on top of his assault element, forcing the enemy to withdraw and resulting in friendly control of the summit of the hill. While exposing himself to intense enemy fire, he was seriously wounded by machinegun fire but continued his mission without regard for his personal safety. After the fifth assault he lost consciousness and was carried from the summit by his comrades only to suffer a fatal wound when an enemy artillery round landed in his area. Sergeant Ashley displayed extraordinary heroism in risking his life in an attempt to save the lives of his entrapped comrades and commanding officer. His total disregard for his own personal safety while exposed to enemy observation and automatic weapons fire was an inspiration to all men committed to the assault. The resolute valor with which he led five gallant charges placed critical diversionary pressure on the attacking enemy and his valiant efforts carved a channel in the overpowering enemy forces and weapons positions through which the survivors of Camp Lang Vei eventually escaped to freedom. Sergeant Ashley's conspicuous gallantry at the cost of his own life was in the highest traditions of the military service, and reflects great credit upon himself, his unit and the United States Army.[1]

In the aftermath of the battle, the Army found that 17 of the 24 Americans at the camp had been killed and six were missing. At least four of the missing had been captured. However, the North Vietnamese also suffered major losses and their planned assault on Khe Sanh had been stopped, which also prevented them from gaining control of the northern provinces along the Demilitarized Zone.

SFC Ashley's family received his Medal of Honor posthumously on 2 December 1969.

In 2001, the Eugene Ashley High School near Wilmington, North Carolina, was dedicated in his honor. He was also inducted as a Distinguished Member of the Special Forces Regiment in 2012, and the following year, the 3rd Battalion, 5th Special Forces Group (Airborne) operations complex at Fort Campbell, Kentucky, was named Ashley Hall in his honor.

Endnote

1. "Indomitable Valor: SFC Eugene Ashley, Jr.," U.S. Special Operations Command website, accessed 3 October 2019, https://www.soc.mil/ARSOF_History/medal_of_honor/recipient_ashley.html.

References

Briscoe, Charles H. "The Battle of Lang Vei." U.S. Special Operations Command website, August 2019. https://www.soc.mil/ARSOF_History/articles/19_aug_lang_vei_page_1.html.

Cash, John A. "Battle of Lang Vei." In *Seven Firefights in Vietnam*, edited by Loretto C. Stevens, 109-138. Washington, DC: Center of Military History, 1970. https://history.army.mil/books/Vietnam/7-ff/Ch6.htm.

"Distinguished Member of the Special Forces Regiment: Sergeant First Class Eugene Ashley Jr." U.S. Special Operations Command website. Accessed 3 October 2019. https://www.soc.mil/SWCS/RegimentalHonors/_pdf/sf_ashley.pdf.

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 a theme. We publish non-theme articles in most issues.
- Please do not include any personally identifiable information (PII) in your article or biography.
- Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

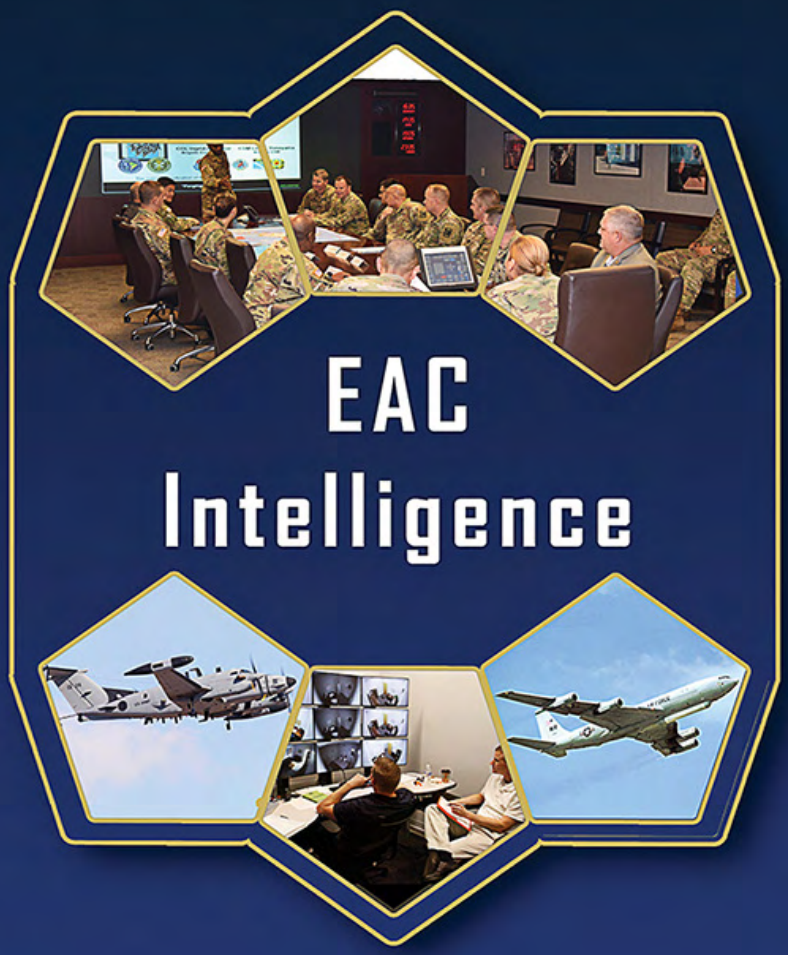
What we need from you:

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

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

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

MIPB (ATZS-DST-B)
Dir. of Doctrine and Intel Sys Trng
USAICoE
550 Cibeque St.
Fort Huachuca, AZ 85613-7017



EAC Intelligence

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

PIN:205923-000