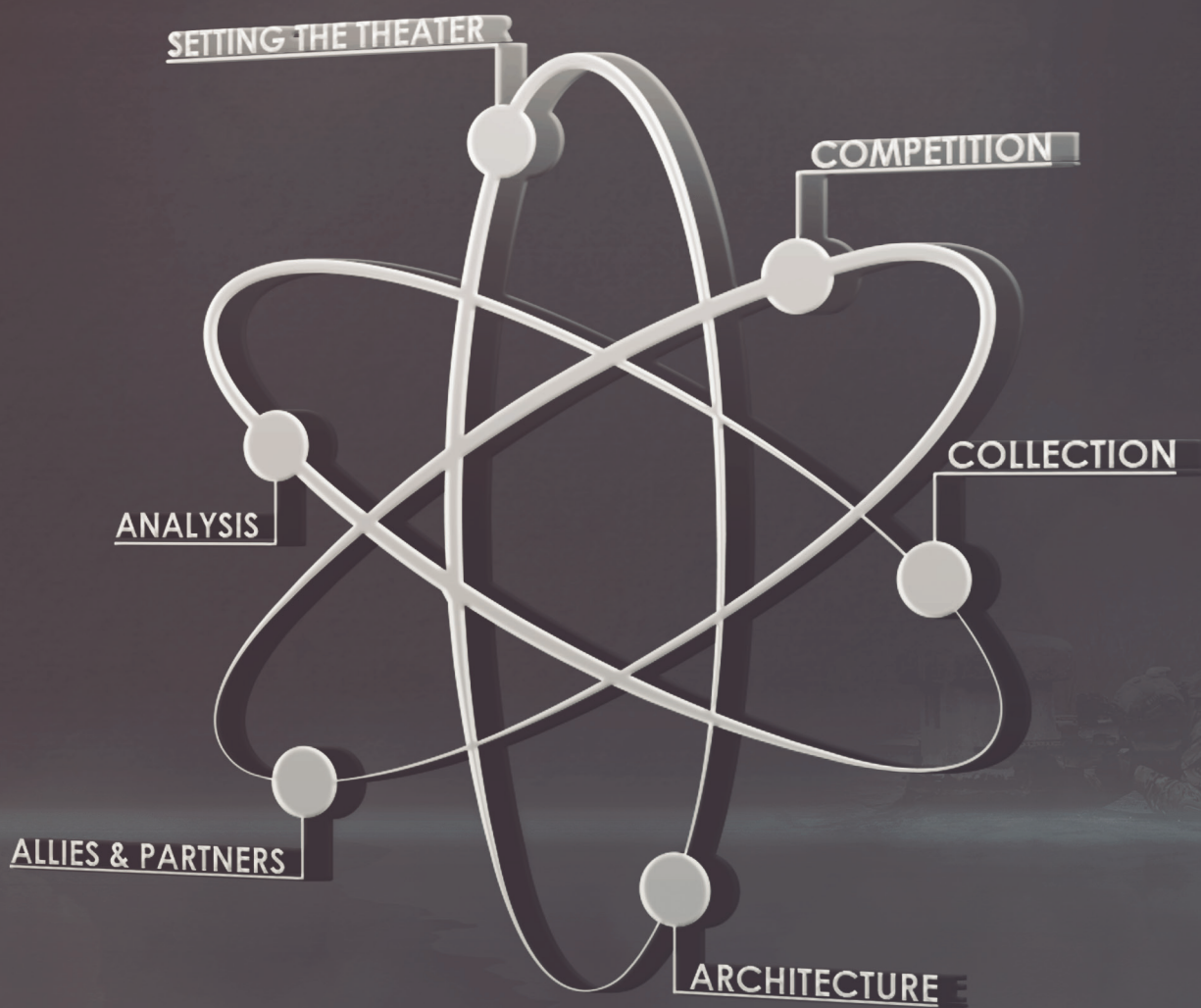


MI PROFESSIONAL BULLETIN

July–September 2021
PB 34-21-3



THEATER INTELLIGENCE
OPERATIONS

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 Cibique St., Fort Huachuca, AZ 85613-7017.

Commanding General

MG Anthony R. Hale

Command Sergeant Major, MI Corps

CSM Warren K. Robinson (ending 24 August 2021)

CSM Tammy M. Everette (beginning 24 August 2021)

Chief of Staff

COL Norman S. Lawrence

Commandant, Intelligence School

COL Christina A. Bembenek

Chief Warrant Officer, MI Corps

CW5 Aaron H. Anderson

Director, Doctrine and Intelligence Systems Training

LTC Crayton E. Simmons

STAFF:

Editor

Tracey A. Remus
usarmy.huachuca.icoe.mbx.mipb@army.mil

Associate Editor

Maria T. Eichmann

Design and Layout

Jonathan S. Dinger

Cover Design

Jonathan S. Dinger

Military Staff

CW4 Michael Janney

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.

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

Official:



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

2134302

From the Editor

This is the last quarterly issue of MIPB. To remain relevant, we are evolving and embracing new distribution channels and updated technology. In our last issue, we provided some initial information about our modernization plan. In this issue, we have an update to that plan on page 8. It provides details for the parts we know and identifies the parts we are still working out.

What doesn't change is our reliance on you! This is still your bulletin. For us to be successful, we depend on you. Some suggested topics for future article submissions include intelligence support to targeting, intelligence training, and Army intelligence modernization.

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



Tracey A. Remus
Editor

MI PROFESSIONAL BULLETIN

July–September 2021
PB 34-21-3
Volume 47 Number 3

THEATER INTELLIGENCE OPERATIONS

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 supersede information in any other Army publications.

Features

10 Theater Intelligence Operations in Competition

by COL Jay W. Haley, LTC Christopher J. Heatherly, Mr. Matthew D. Skilling, Ms. Laura K. Rettle, CPT Phillip J. Hoying, Mr. Ronald W. Bijeau, and Mr. Jon J. Sadowski

15 U.S. Army North Intelligence: America's Intelligence

by COL Laura Knapp and MAJ John Holland

20 Army Operations in the Arctic

by Mr. Michael Gearty

24 Understanding Emerging Space Domain Threats and Their Effects on Land-Based Operations

by CPT Andrew Compean and Mr. Daniel Selman

32 Bringing the Army Team to Africa

by COL Bill Bestermann and LTC James A. Crump

36 Challenges with Multinational Intelligence Cells

by CW4 Mark Benitez

41 Army Central Rolls Along with Intelligence Engagements

by COL John S. Chu and LTC Quentin D. McCart

46 Central America: A Strategic Battleground for Advancing Our Interests

by MAJ Mark Medlock

52 Russian Tactical Correlation of Forces and Means Computation Updated for Modern Equipment and Capabilities

by Lester W. Grau, Ph.D., and Mr. Clint Reach

63 Explosive Ordnance Disposal and Intelligence: Exploring Gaps between Mutually Supporting Communities

by LTC Philip D. Cordaro

69 700-Series Battalion Conducts External Evaluation to Improve Mission Essential Task Proficiency

by MAJ George Gurrola, CPT Mason Lockey, and CW3 Katy Tomlinson

DEPARTMENTS

2 Always Out Front

4 CSM Forum

6 Technical Perspective

74 Lessons Learned

78 Futures Forum

81 Military Intelligence Hall of Fame

85 Awards for Excellence in MI

89 Moments in MI History Part 3

93 Moments in MI History Part 4

Inside back cover: Contact and Article Submission Information



Always Out Front

by Major General Anthony R. Hale

Commanding General

U.S. Army Intelligence Center of Excellence



This is the last quarterly issue of the *Military Intelligence Professional Bulletin* (MIPB). The U.S. Army Intelligence Center of Excellence (USAICoE) has begun an initiative to modernize MIPB in a handful of ways. The first major change within this initiative is to discontinue quarterly hard-copy MIPB issuance and shift to a continuously updated online version of MIPB. We will also develop MIPB special editions two or three times a year. The first special edition focuses on publicly available information across our intelligence disciplines.

It is fitting that the theme of this last quarterly issue of MIPB is theater intelligence. This MIPB issue includes articles from many of the Army Service component commands (ASCCs), as well as articles covering other aspects of theater intelligence. The four functional ASCCs are important to the Army, but in this column, I will address intelligence in the five theater armies and one standing field army (the 8th U.S. Army).

The timing of this issue aligns with the July 2021 publication of FM 3-94, *Armies, Corps, and Division Operations*, and the imminent approval of ATP 2-19.1, *Echelons Above Corps Intelligence Organizations*. In my column, I briefly discuss theater intelligence during competition and crisis, while CW5 Anderson's column addresses theater intelligence in large-scale combat operations.

The Doctrinal Foundation

Before looking at current and future theater and field army intelligence challenges during competition and crisis, it is worth discussing the foundational doctrine within FM 3-94 and other doctrinal publications. The theater and field army mission is one of the most diverse and complex of any Army echelon. Theater armies support a geographic component commander (GCC) and provide the GCC with capabilities and support from all assigned and attached Army forces in the area of responsibility (AOR).



Additionally, theater armies are designated as ASCCs, responsible for recommending the allocation of Army forces to the GCC. It is important to note that field armies are not ASCCs.

Some of the most important aspects of field armies are that they—

- ◆ Set and maintain the theater in competition and conflict.
- ◆ Deter potential adversaries and secure advantages should deterrence fail. This aspect of army ac-

tions and operations facilitates flexible options for strategic commanders and decision makers.

- ◆ Exercise broad command and control of Army forces.
- ◆ Exercise joint roles of limited scope, scale, and duration.
- ◆ Provide cultural awareness and are continually involved with their security cooperation partners in the region.
- ◆ Provide unique enabling capabilities to the theater such as theater casualty evacuation, theater signal, theater sustainment, and theater intelligence.

During competition, field armies actively support the GCC through missions, tasks, and actions to shape the environment. Beyond shaping the environment, field armies prepare to rapidly transition to conflict should the GCC identify an increased threat or new operational requirements within the AOR. Specifically, armies plan for such diverse problem sets like destruction of enemy antiaccess and area denial capabilities; basing options; and reception, staging, onward movement, and integration of additional Army forces and equipment into an area of operations.

All of those army missions, tasks, and actions are informed and sometimes completely driven by intelligence. While the U.S. Army Intelligence and Security Command (INSCOM) is responsible for intelligence collection from a strategic perspective, the theater army G-2 staff and military intelligence brigade-theater (MIB-T), in conjunction with many other echelons above corps (EAC) organizations, focus their efforts within any one specific theater. There are six INSCOM MIB-Ts. Five MIB-Ts are tailored for and assigned to a GCC, which normally delegates operational control (OPCON) to the supporting theater army/ASCC. The 8th U.S. Army is also assigned OPCON of a MIB-T. Each MIB-T provides robust intelligence capabilities, including collection, processing, analysis, and dissemination support to the theater army/ASCCs, GCC, and intelligence community.

The Challenge

We are always operating within great power competition—especially in the U.S. Indo-Pacific Command AOR. Success during large-scale combat operations will be impossible if we as an Army wait for a crisis to establish theater intelligence collection management, collection activities, processing, analysis, and production. ATP 2-19.1, which the Army will publish soon, provides basic doctrine on EAC intelligence. However, doctrine can only go so far in accurately describing the inherent complexity of theater operations.

Theater intelligence requirements stretch across the globe—from the most remote corner of South America to the Arctic shipping lanes to the South China Sea and from space to cyberspace. The days when the United States enjoyed a capability overmatch against its threats no longer exists. Many peer threat capabilities now nearly-match, equal, or surpass our capabilities from a regional perspective. Even during competition, the operational environment across all domains is complex, congested, and contested, especially within the information dimension. The future threat is capable of bringing the fight to the United States on a significant scale.

Road Ahead


The road ahead will be informed by the fundamentals, which to a major extent match my one priority and three objectives here at USAICoE:

- ◆ **Keep people as our number 1 priority.** The Military Intelligence (MI) Corps will coach, teach, mentor,

and build caring leaders. We will also diligently recruit talent and reach into untapped pools of talent to build a new and different MI Corps of the future.

- ◆ **Build leaders with the right knowledge, skills, and behaviors.** One way to accomplish this objective is to develop and use relevant doctrine and other official Army content to build and maintain a professional MI Corps. We must also train as we intend to fight by training in a disrupted, intermittent, and limited communications-enabled scenario. I would offer that you can rarely ever conduct too many training “sets and reps” as an intelligence enterprise.
- ◆ **Drive change to train, man, and equip an excellent current and future MI force.** The MI Corps must tirelessly build intelligence capabilities through inclusive and collaborative means with joint headquarters, other Services, Army branches, and every MI staff and organization across the Army. New technologies and fields like artificial intelligence, machine learning, and data science will be important in future operations.
- ◆ **Dominate the information space from an MI perspective.** We will build trust in the MI Corps through deliberate communications with internal and external audiences. We wear the jersey of the best team in the world. We must tell our story, or someone else will.

Additionally, we will build trust and rapport with our allies and partners including them in everything we do, as much as possible. Our allies and partners have incredibly important regional knowledge and often bring unique capabilities to the fight.

I am confident that our force of intelligence professionals will continue to adapt. We will rise to overcome the myriad of intelligence challenges, even at the theater-level, to help the Army successfully compete with our peer threats. The United States may be at a disadvantage in some respects within great power competition, but we have a special weapon on our side—our talent. Ultimately, the American Soldier will continue to be our biggest advantage over any threat. Intelligence professionals remain at the forefront of this fight and will continue to make a difference.—Desert 6. 

Always Out Front!



CSM Forum

Command Sergeant Major of the MI Corps
U.S. Army Intelligence Center of Excellence



by Command Sergeant Major Tammy M. Everett

First and foremost, I want to express my gratitude and pride for all the hard work and dedication across our Military Intelligence (MI) Corps. I am extremely humbled to serve alongside you as the MI Corps Command Sergeant Major, and I am very excited for the future of our Corps. I am thankful for the great hand-over of responsibility with CSM Warren Robinson, and I will concede most of my space to him for his parting comments.

The theme for this quarter's *Military Intelligence Professional Bulletin* is theater intelligence. Each theater is unique in its own right, but the theme that combines them all is complexity. In order to fight and win our Nation's wars, we must train MI professionals to be technically and tactically proficient in their intelligence disciplines and warrior tasks.

At the U.S. Army Intelligence Center of Excellence, we are driving change and building leaders with people at



the forefront. We are redesigning institutional training to deliver highly trained, fit, and disciplined Soldiers to your formations. Publicly available information will be introduced to every intelligence discipline to assist in understanding the complexities of the operational environment. We are making tough decisions and refining critical tasks to ensure we are teaching the right things at the right time. The Soldiers trained at Fort Huachuca are capable of tackling the complexities of the current operational environment and will rely on you to continue to train them in

the operational force.

For those in the operational force, we need you at Fort Huachuca. We need you to give back to the institution to ensure we are delivering what the force needs. If you think you have what it takes to train the next generation of intelligence professionals, I invite you to join Team Huachuca!!



Always Out Front!

by Command Sergeant Major Warren K. Robinson

It is hard to believe that 3½ years have gone by since my selection to serve as the U.S. Army Intelligence Center of Excellence (USAICoE) Command Sergeant Major. This is my last column for the *Military Intelligence Professional Bulletin*, and before I leave, I have a few parting thoughts for the team.

Our Army is in capable hands. It seems that the leadership of every generation doubts the strength and abilities of the younger generation. Mine was no different. Our leaders thought we were undisciplined and soft, and they questioned our ability to maintain a



strong Army. Likewise, my generation recognizes that younger Soldiers are not the same as their predecessors. They think, learn, and communicate in a different way, and they have different requirements to be successful. I read somewhere that all Soldiers are entitled to outstanding leadership. To ensure the Army continues to stay strong, we must provide these young Soldiers with agile, adaptive leadership that understands the generational differences. I encourage you to be the leader who positively and proactively engages with young Soldiers and who provides them the purpose,


direction, and motivation they deserve to accomplish the mission and improve the organization.

An Army career is not lived in a straight line. None of us gets the experiences we require or desire in order to meet all the reasonable expectations the Army has of us. This is why it is important to invest in people. Start by defining what you want your Soldiers to do. If you have a Soldier, of any rank, who is not meeting your expectations, ask whether you have realistically developed that Soldier to meet the standard. Many times, Soldiers are capable of exceeding standards, but only if we take the time to invest in their development. If leaders believe it is easier to do everything themselves than to teach someone else, they will eventually fail because there comes a time in our careers when we have more requirements than we can fulfill. We need those young Soldiers to support us.

So what do you really want to accomplish? Too many times, people have the mindset of “this is how we’ve always done it.” Even worse is when someone who does not have the authority to say yes says no. No is an easy answer. It requires no work or thought. Change the mindset and start with what the answer needs to be, whether that is yes or no, and begin working backward to determine the hurdles. Then engage with the people who have the authority to provide that answer. If the policy does not afford the needed outcome, find the policymakers and ask for their help. Many times, policymakers are in their position because they are resourceful problem solvers.

I once read that good leaders always communicate with Soldiers and never leave them uninformed. By

communicating proactively, regularly, and as openly as possible, leaders develop Soldiers. In other words, leaders should dominate the information space because they cannot afford to assume their message will get to the lowest level. If leaders do not communicate regularly and deliberately, someone else will do it for them, possibly disseminating inaccurate information. As we know all too well, people do not have to be knowledgeable about a topic to freely share their comments. Worse is that many Soldiers might believe those comments from unreliable sources. Get information out to the appropriate level of leadership. Develop formal and informal feedback loops to determine who is effectively communicating with their Soldiers and, if necessary, their families. These interactions may even provide senior leaders an opportunity to train their mid-level and junior leaders. Use every means of communication available. Face-to-face is best but not always possible, so use social media and other means to reach a larger audience. Lastly, be transparent and address difficult topics up front. Once people know that leadership will openly address controversial topics (provide the *why*), they will develop trust and be drawn to those places where they can get reliable information. This also reduces the likelihood of someone perpetuating misinformation.

I know we are on the right path, and I am proud to have had the opportunity to contribute to the development of our Soldiers, especially during my time as the USAICoE Command Sergeant Major. Soldiers, civilians, and families made my 30 years in the Army one of the most amazing experiences of my life. Thanks to everyone for all your hard work and for continually pushing me to get better every day. It has truly been my honor to serve our Nation. 

Always Out Front!

Change of Responsibility

Having served as the Command Sergeant Major of the Military Intelligence Corps from 16 March 2018, CSM Warren K. Robinson relinquished his responsibilities as the Corps Command Sergeant Major to CSM Tammy M. Everette in a Change of Responsibility Ceremony on 24 August 2021.



Technical Perspective

by Chief Warrant Officer 5 Aaron H. Anderson
Chief Warrant Officer of the MI Corps
U.S. Army Intelligence Center of Excellence



Teammates,

Regardless of the battlefield, the future operational environment will be more complex and more lethal than any environment in which the U.S. Army has previously engaged. Theater intelligence organizations play a critical role in outlining the complexities of this future environment and understanding adversary capabilities across all domains. Our near-peer adversaries are actively working toward achieving technological advances enabling the integration of space, cyberspace, information, and electromagnetic warfare capabilities, with the intent of limiting or denying America's ability to globally project power. Empowering theater intelligence organizations with cutting-edge technology and modern architectures sets the conditions to facilitate overmatch and mitigate our adversary's anti-access and area denial capabilities.

In order to employ land power during a crisis, the Army must first "set the theater." "Setting the theater includes whole-of-government initiatives, including bilateral or multilateral diplomatic agreements that allow U.S. forces access to ports, terminals, airfields, and bases in the [area of responsibility] AOR to support future military contingency operations."¹ Critical to setting the theater is the military intelligence brigade-theater (MIB-T). The MIB-T represents the theater army's collection and information analysis capability. The MIB-T serves as the anchor point for any forces flowing into theater, providing reachback intelligence production, analysis, indications and warning, and processing, exploitation, and dissemination. MIB-Ts are postured to provide multi-discipline intelligence and possess a ready set of products, estimates, and order of battle to be provided to supported forces executing contingency operations or responding to a crisis. In the case of the 66th Military Intelligence (MI) Brigade in Europe and the 500th MI Brigade in the Pacific,



their forward positioning and persistent presence allow for continuous shaping and awareness in the competition phase as well as a ready presence should competition turn into crisis or conflict.

The U.S. Army will never fight a major war alone. Allies and partners will be critical to executing large-scale combat operations in a multi-domain environment. Forward-stationed MIB-Ts are in a unique position to establish and maintain intelligence and security partnerships in theater. Theater security cooperation and regional partnership events are founda-

tional cornerstones needed to shape the environment in the competition phase. Our adversaries are working every day, in multiple domains, to chip away at U.S. partnerships and alliances as part of their own shaping activities. We must be prepared to counter those initiatives and keep our partnerships strong, regardless of the theater.

Maintaining a coherent intelligence architecture from the theater level to the tactical edge is critical and necessary to support all other warfighting functions in large-scale combat operations. A recent warfighter exercise has illuminated the requirement to maintain system and process interoperability across the intelligence warfighting function and with our unified action partners. Establishing common data sharing standards and protocols at the theater level provides unity of effort and can assist in smooth data transfer at corps and below levels.

Incorporating new and emerging technology by theater intelligence formations will become increasingly important as the Army moves toward a force capable of executing true multi-domain operations. The use of artificial intelligence and machine learning at the theater level is not only important to future analytics but also in shortening the "kill-web," allowing commanders to prosecute targets more quickly. Additionally, new unmanned systems and sensors will inform future reconnaissance and surveillance

efforts, and emerging deep sensing capabilities will allow theater intelligence elements to see and shape the battlefield in a more robust way than ever before.

In the multi-domain environment, the ability to pass data across the intelligence enterprise at the “speed of need” is extremely important. The MIB-Ts must provide a constant flow of information to lower-echelon units while at the same time feeding joint, interagency, and multinational elements, ensuring situational awareness across the intelligence enterprise. As new formations such as the Multi-Domain Task Force and the Theater Fires Element come online, and are introduced into various theaters, the concept of the MIB-T as an anchor point is unlikely to change. What will continue to evolve are the habitual relationships between these organizations and the MIB-T as well as current policy and doctrine to enable multi-domain intelligence. With adversaries using all the

instruments of national power to influence the operational environment, the theater intelligence organizations must gain and maintain an ability to support operations in all domains and successfully counter adversary activities.

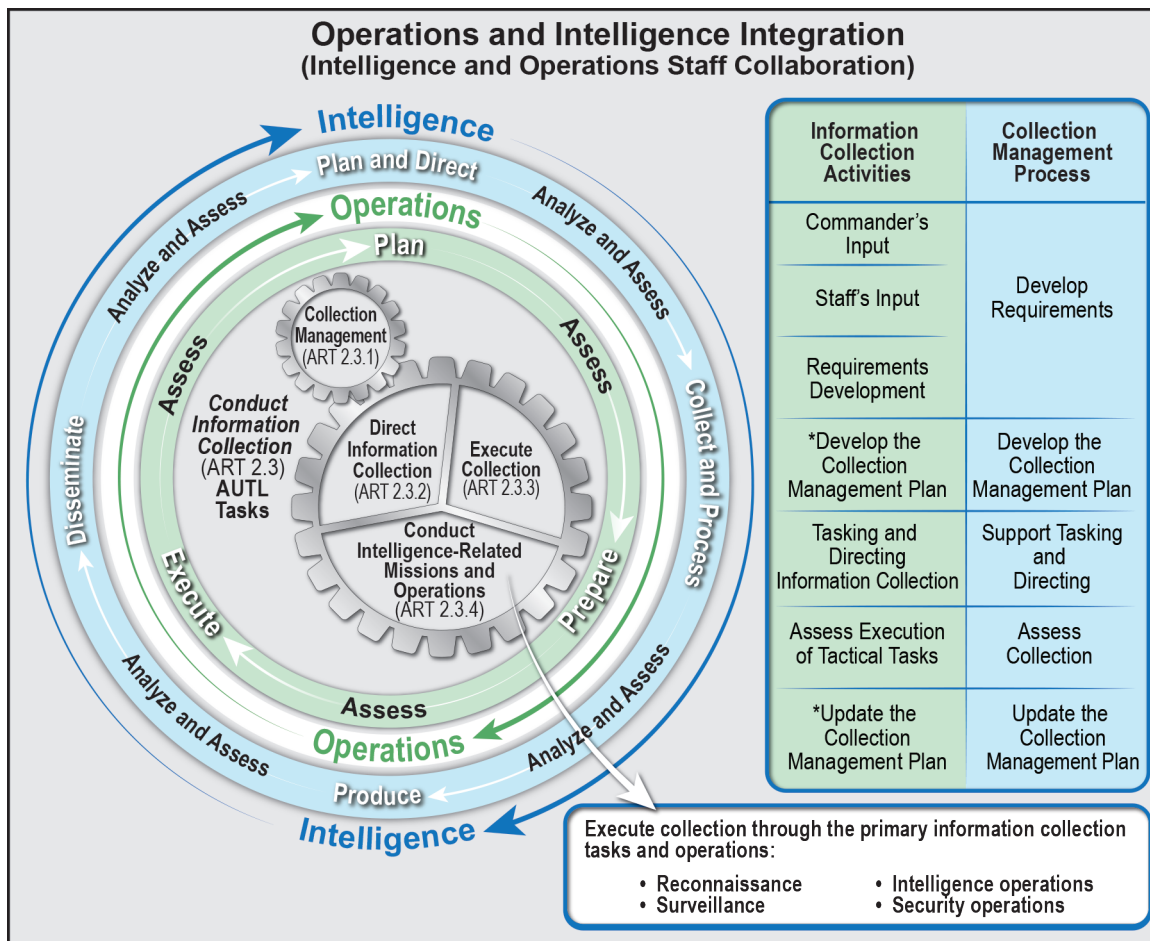
In closing, I would like to thank you and your families for your daily sacrifice, selfless service, and contributions to the Army in defense of our Nation. I would especially like to recognize those MI Soldiers who are currently serving in forward locations. Your contributions to the MI Corps and Army mission are greatly appreciated. 🌟

Endnote

1. Department of the Army, Field Manual 3-94, *Armies, Corps, and Division Operations* (Washington, DC: U.S. Government Publishing Office, 23 July 2021), 3-6.

Always Out Front! and Army Strong!

Know Your Doctrine...



This figure, from ATP 2-01, *Collection Management*, published 17 August 2021, illustrates the integration of operations and intelligence, and the relationship between information collection and collection management.



Modernizing MIPB

Underway

We are excited!

Significant changes are underway for *Military Intelligence Professional Bulletin* (MIPB). These improvements will leverage current technologies and align with the ways you consume information. The goal is to implement an improved online and social media experience for you, the reader. However, we have to implement these changes in increments. Here is the plan:

Online, our primary means of distribution:

The new MIPB website is up and working at <https://mipb.army.mil>. From now on, we will post MIPB articles to this website as we select and approve them for publication with far less lag time.

MIPB on Intelligence Knowledge Network (IKN) still going strong:

The old public-facing MIPB website on IKN is still available at <https://www.ikn.army.mil/apps/MIPBW>. It has the complete MIPB archive up through the April–June 2021 issue. No additional content will be posted to IKN, but the archive will not go away. All new content, beginning with this issue, will post to the new website on LandWarNet.

No more quarterly themed issues:

Units will no longer receive a quarterly issue of MIPB through the mail. Instead, all MIPB articles will be available on the new website. Authors can write about any intelligence topic they think is useful to our audience. The submission guidelines remain mostly the same and can be found on the inside back cover of this issue. We plan eventually to post them on the new MIPB website as well. A few areas of interest for FY22 include intelligence support to targeting, intelligence training, and Army intelligence modernization.

Special editions:

Not all of the details have been resolved, but our intent is to develop two to three special editions of MIPB each year. We will not develop and distribute these editions until all articles for the edition have been published online. Additionally, we have not finalized the hardcopy distribution details. These editions will differ from the previous quarterly issues in that—

- ◆ They will only consist of featured content.
- ◆ The articles will focus on a narrower theme.

Our first FY22 special edition, *Publicly Available Information across the Intelligence Disciplines*, is underway.

Social media:

In conjunction with the USAICoE Commander's Action Group, we are looking at the use of social media to advertise MIPB changes and the posting of new online articles. For now, go to U.S. Army Intelligence Center of Excellence on Facebook and Twitter for the latest scoop on MIPB.

Your input is invaluable to us:

We need your input! If you have comments or suggestions on how to improve MIPB, please let us know at—

MIPB mailbox:

usarmy.huachuca.icoe.mbx.mipb@army.mil

Note: The Army is transitioning email accounts to @army.mil, so please send your emails to our new email address.



Theater Intelligence Operations in Competition

BY

Colonel Jay W. Haley,
Ms. Laura K. Rettle,
Mr. Ronald W. Bijeau,

Lieutenant Colonel Christopher J. Heatherly,
Captain Phillip J. Hoying,
Mr. Jon J. Sadowski,

Mr. Matthew D. Skilling

For the joint force to play its role in advancing national interests, it must adopt a better framework for understanding, describing, and participating within a competitive operational environment.

—Joint Doctrine
Note 1-19, Competition
Continuum

Within this operational environment, the USAREUR–AF G-2 is charged with providing predictive intelligence that supports the commanding general’s Army Service component command and Combined Joint Force Land Component Command decision making to retain the strategic initiative and deter any potential adversaries. Successfully completing this mission requires the USAREUR–AF intelligence warfighting function to generate opportunities to compete against adversaries for access, influence, and information. It further requires the G-2 to master the ability to conduct intelligence operations in competition to enable maneuver and fires in the conflict phase, as well as set conditions for follow-on intelligence operations that would be too late to initiate during conflict (Figure 1).

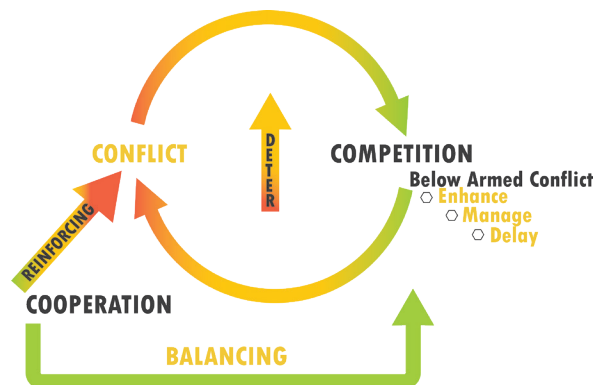


Figure 1. Competition, Conflict, Cooperation Model⁴

The intelligence process, from ADP 2-0, *Intelligence*, best describes how we successfully set conditions on a daily basis, as it “directly drives and supports the operations process.”⁵ Using the intelligence process model (Figure 2 on the next page), we will briefly describe how USAREUR–AF conducts theater intelligence operations in competition.

Analyze and Assess

Throughout the intelligence process and at every step of the model, we rigorously analyze and continuously assess our efforts in theater to ensure we use our resources as efficiently as possible. Additionally, during competition, we analyze and assess our processes with distinct checks:

Introduction

Sun Tzu was perhaps the first military theorist to espouse the idea of defeating an enemy without outright conflict. In his treatise, *The Art of War*, Sun Tzu wrote, “the ultimate achievement is to defeat the enemy without coming to battle.”¹ While that maxim remains true, the U.S. Army must be prepared to fight and win the Nation’s wars in all phases, from competition to crisis to conflict. The recent *Chief of Staff Paper #2* defines the Army’s role succinctly as, “the Army contributes to military competition by building and employing land force capability and capacity to support a broad range of policy choices.”² For the moment, the United States Army Europe and Africa (USAREUR–AF) remains in the competition phase with the Russian Federation. Russian competition activities are readily identifiable in a number of European and, increasingly more often, African nations. These activities are primarily “fought” in the non-kinetic information and cyberspace domains. Recent examples of competition activity in Western Europe, the Baltic States, and the Balkans point to both the scope and scale of Russian efforts to win without escalating to outright conflict. Indeed, one of Russia’s primary goals is to maximize its influence in its near abroad while minimizing the influence of the West, given the Russians’ skewed perception of the threat posed by the North Atlantic Treaty Organization (NATO) and the United States and the strength disparity in a conventional war.³

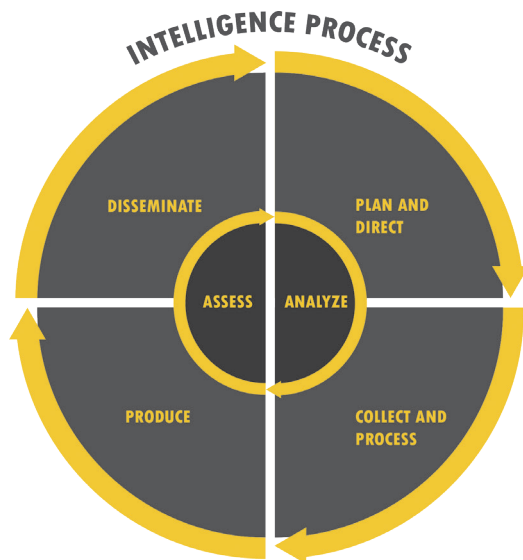


Figure 2. Intelligence Process⁶

- ◆ Yearly, we synchronize efforts to maintain and guide the long-term intelligence strategy in both the African and European theaters.
- ◆ Quarterly, we invite the senior leaders and planners of the intelligence warfighting function to discuss the execution of that long-term strategy and assess its progress or identify areas to focus additional efforts.

By bringing together all vested intelligence organizations with divergent viewpoints, we arrive at a coordinated assessment of our efforts, which allows us to execute the entire intelligence process.

Plan and Direct

A primary focus of the intelligence warfighting function during competition is identifying adversary activity, especially from the adversary's associated intelligence services, within the information and cyberspace domains. Recent world events clearly demonstrate the aggressive nature of Russian intelligence services in these critical spheres.⁷ This operational environment drives the first step in the doctrinal intelligence process. During the plan and direct step, the USAREUR–AF intelligence warfighting function identifies information requirements and the ways in which to best satisfy those requirements.⁸ We incorporate and focus our efforts into the G-3–led targeting and collection board; specifically, the G-2 provides full spectrum intelligence support and situational awareness to lethal and nonlethal targeting. We accomplish this through the incorporation of regular intelligence operations from all disciplines fused into a comprehensive intelligence picture. To bring a more robust intelligence assessment to the targeting process, the theater analysis and control element (ACE) implements the 66th Military Intelligence (MI) Brigade-Theater's targeting process in cooperation with the USAREUR–AF G-2 team, which comprises collection management, counterintelligence (CI), human intelligence

(HUMINT), signals intelligence (SIGINT), and open-source intelligence (OSINT). The intelligence warfighting function takes advantage of major exercises, such as DEFENDER-Europe 21, as prime opportunities to refine and rehearse the targeting process. In conjunction with the larger intelligence community, the intelligence warfighting function assesses the outcome of these operations for lessons learned and tactics, techniques, and procedures to improve with each iteration.

Security cooperation with allies and partners also creates desired outcomes and favorable conditions in competition readily transferable to crisis or armed conflict. Bluntly, our bilateral and multilateral intelligence security cooperation is extensive. In addition to technical and analytical coordination, we participate in several multinational exercises designed to build familiarity and interoperability. USAREUR–AF HUMINT entities are active participants in national exercises in multiple countries across Europe. We expanded our own Kosovo Force CI/HUMINT certification exercise into a multilateral training opportunity to include representatives from certain partner nations. Additionally, we are an active participant in NATO's exercise Steadfast Interest HUMINT.

Intelligence planning for exercise DEFENDER-Europe 20 started in September 2019. It aptly demonstrates the vital role cooperation plays in the competition phase of conflict. The planned scale of DEFENDER-Europe 20 allowed for considerable intelligence planning and integration with our NATO partners and allies in both exercise and real-world intelligence requirements. The Multinational Corps Northeast J-2 and the USAREUR–AF G-2 Plans cells sent reciprocal representatives to the respective headquarters. Their goal was to conduct intelligence preparation of the battlefield, mission analysis, course of action development, and annex creation of both the Combined Joint Force Land Component Command and the Multinational Corps Northeast operations orders for the DEFENDER-Europe 20 planning process. They were integrated into in-person and geographically dispersed planning and briefing.

Collect and Process

Collection and processing synchronization is imperative to provide critical information to drive competition operations and feed intelligence into the targeting process.⁹ Collection management takes on a new and interesting twist, as it requires execution on a continental scale in two separate and highly distinct theaters. Given current Russian and Chinese influence in Europe and growing influence in Africa, it becomes increasingly important to understand national, combatant command, ally, and partner collection capabilities and the ways in which to receive and apply that information to USAREUR–AF requirements.¹⁰ In the competition phase, we find bilateral and multilateral combined collection to



A U.S. Soldier fast ropes out of a CH-47 Chinook during African Lion 21, U.S. Africa Command's largest joint annual exercise.

be very productive throughout the intelligence process. The 66th MI Brigade's series of OSINT-combined collection operations, Northern Raven, is a perfect example of this relationship. To date, this operation produced more than 300 OSINT reports by co-locating U.S. OSINT collection tools and doctrinal training with the cultural understanding, military knowledge, and native language skills of the allies and partners. These types of operations provide a more holistic insight into adversary operations that our organic collection does not always achieve. Given our long-standing partnerships with NATO allies, these combined collection operations help to strengthen relationships that will pay dividends in the conflict phase. With the recent merger of USAREUR and U.S. Army Africa into USAREUR-AF, we see a unique opportunity to practice collection skills against this challenging dynamic. In 2021, USAREUR-AF conducted two major exercises, DEFENDER-Europe 21 and the Southern European Task Force-Africa's African Lion 21, nearly simultaneously. Taken together, DEFENDER-Europe 21 and African Lion 21 allow USAREUR-AF to test its ability to manage competition activity in two concurrent major exercises against related but separate problem sets.

As ADP 2-0 explains, processing is mutually dependent with collection.¹¹ It is an inherent fact that the information derived from bilateral and multilateral collection operations is delivered in a variety of formats and systems. Rapid processing of the various types of intelligence is key to developing a thorough and usable product for all nations concerned. Likewise, when participating in the competitive targeting process, the USAREUR-AF intelligence warfighting function cannot simply provide an incident map to the G-3 in the hope it will be useful. It requires the efforts of collection management, ACE, G-2X, targeteers, and single-source subject matter experts to combine intelligence information reports, tactical reports, Klieglight reports, imagery, full

motion video, or moving target indicator data into a usable product understood and applied by the entire targeting board. More importantly, this intelligence product becomes the "map" to direct competition operations.

Produce

Production is the application of analysis to collected information and existing intelligence.¹² In most cases, the 66th MI Brigade ACE performs this function. In the USAREUR-AF G-2, we found that a complementary effort by a separate analytic cell focused on CI and HUMINT lends itself well to intelligence operations in the competition phase. Examples of this are the USAREUR-AF daily intelligence update, the G-2X foreign intelligence threat assessments, and special assessments. Make no mistake—these are not exclusive entities operating in isolation. They are complementary efforts working toward a common intelligence picture. As evidence, this CI and HUMINT analytic effort began developing a methodology for combining and collating multiple information streams to focus intelligence operations in competition by looking at where USAREUR-AF lives and works rather than focusing on adversary countries. We anticipate that this will further aid competition targeting for nonlethal effects like information operations by providing an ability to focus efforts in more precise locations rather than spreading finite resources in large areas. Additionally, the USAREUR-AF G-2 initiated a program of analysis to streamline and quantify our European partners' intelligence requests for information as a means to shape our SECRET Releasable production with our NATO partners. By producing intelligence that is actionable and shareable, we reach our end state to have a more tailored series of releasable products driven by our allies' and partners' intelligence priorities.

Two major factors influencing the production cycle are the continued efforts to refresh or reset USAREUR-AF collection assets across all single-source intelligence disciplines and the sustained efforts to develop or enhance existing partnerships with European and African allies. Using SIGINT as a model, SIGINT production is shared not just among a consortium of U.S. joint military units and intelligence agencies; rather, the USAREUR-AF G-2 employs its Intelligence and Security Cooperation branch to set conditions for combined SIGINT collection operations or to forge intelligence-sharing agreements. Indeed, the Intelligence and Security Cooperation branch is central to all partner initiatives in all phases of the intelligence cycle.

With regard to another intelligence discipline, geospatial intelligence (GEOINT), the 66th MI Brigade's Integrated GEOINT

Division (IGD) in Darmstadt, Germany, and Fort Gordon, Georgia, perform GEOINT production for USAREUR–AF. The IGD has proactively engaged with various intelligence disciplines and external data providers to increase its ability to inform the commander. To support HUMINT and CI efforts, the IGD has assisted multiple teams in visualizing foreign intelligence entity locations to inform operations and planning and has generated geospatial data to enable the automated detection of nefarious activities in the Joint Security Area. The IGD also coordinates with a Defense Intelligence Agency measurement and signature intelligence (MASINT) capability to gain awareness into adversary interests in the Joint Security Area. The geospatial outputs from the system enable the IGD to visualize and analyze the data in existing tools, and a GEOINT/MASINT product line is now in development. An explosion of commercial imagery sources also provides the IGD with many different avenues to pursue unclassified GEOINT production and adds new ways to publicly expose the adversary activities. Through the Predicative GEOINT Program, the IGD has already tasked commercial imagery satellites and generated baseline GEOINT products disseminated through the Protected Internet Exchange to support theater OSINT operations. Through an Army technology demonstration, the IGD is also assessing commercial synthetic-aperture radar imagery technologies for MI applications where speed and releaseability are of highest importance.

Disseminate

For intelligence to be relevant, it must be appropriately and rapidly shared with consumers. U.S. intelligence doctrine is clear on this point, stating, “Timely dissemination of intelligence and finished intelligence products is critical to the success of operations.”¹³ Example products from our regular intelligence dissemination include a daily intelligence update, G-2X threat assessments, SIGINT reporting,

Epigraph


Office of the Chairman of the Joint Chiefs of Staff, Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, 3 June 2019), 1–2.

Endnotes

1. Sun Tzu, *The Art of War* (London, UK: Chartwell Books, 2011), 17.
2. Department of the Army, *The Army in Military Competition, Chief of Staff Paper #2* (Washington, DC, 1 March 2021), 2.
3. Andrew Radin, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston, and Austin Long, *The Future of the Russian Military* (Santa Monica, CA: RAND Corporation, 2019), 10–13.
4. The authors adapted the graphic from two sources: Office of the Chairman of the Joint Chiefs of Staff, Joint Doctrine Note 1-19, *Competition Continuum*, 2–6; and Kelly McCoy, “In the Beginning, There Was Competition: The Old Idea behind the New American Way of War,” Modern War Institute (West Point, NY: April 11, 2018), <https://mwi.usma.edu/beginning-competition-old-idea-behind-new-american-way-war/>.

and regular intelligence briefings for the commanding general. Individually or combined, the family of intelligence products help to provide situational awareness to leaders of problem sets on two continents, encompassing more than 100 countries and 2.1 billion people. These products are routinely shared via links between the Distributed Common Ground System-Army and the U.S. Battlefield Information Collection and Exploitation System, which supports the point-to-point server federation and the dissemination of Foundation GEOINT data to allies and coalition partners. Additionally, the European GEOINT Edge Node uses cloud technology to disseminate Foundation GEOINT data and services in support of theater operations.

Conclusion

Sun Tzu understood the value of intelligence writing—“foreknowledge cannot be found by consulting the spirits.”¹⁴ Today, some 2,500 years after he wrote *The Art of War*, military leaders require predictive and timely intelligence to succeed across the spectrum, within competition, crisis, or conflict. Providing intelligence is the daily mission of the USAREUR–AF G-2. USAREUR–AF intelligence operations in the European and African theaters occupy a greater competitive space and encompass actions that can be taken to achieve objectives vis-à-vis an adversary.¹⁵ While many of the factors associated with intelligence operations in competition do not differ from other theaters, our proximity to adversaries makes it unique. This proximity further requires the intelligence warfighting function to actively cooperate and participate with allies and partners. Ultimately, these factors as executed in the model of the intelligence process give way to a specific framework for intelligence operations in the competition phase in USAREUR–AF. 

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

6. Ibid., 3-2.

7. Mark Galeotti, “Russian intelligence operations shifting tactics not goals,” NATO Review (April 26, 2019), <https://www.nato.int/docu/review/articles/2019/04/26/russian-intelligence-operations-shifting-tactics-not-goals/index.html>; and Michael Schwartz, “Top Secret Russian Unit Seeks to Destabilize Europe, Security Officials Say,” *New York Times*, October 8, 2019, <https://www.nytimes.com/2019/10/08/world/europe/unit-29155-russia-gru.html>.

8. Department of the Army, ADP 2-0, *Intelligence*, 3-3.

9. Ibid., 3-5.

10. Christopher Woody, “The US Navy’s top admiral in Europe says China is copying Russia’s interference playbook there,” Business Insider, June 26, 2020, <https://www.businessinsider.com/top-navy-admiral-in-europe-china-copies-russias-influence-playbook-2020-6?r=DE&IR=T>; and Diana Stancy

Correll, "How AFRICOM plans to counter Russian, Chinese influence in Africa," Military Times, January 20, 2020, <https://www.militarytimes.com/news/your-military/2020/01/20/how-africom-plans-to-counter-russian-chinese-influence-in-africa/>.

11. Department of the Army, ADP 2-0, *Intelligence*, 3-5.

12. Ibid., 3-6.

13. Ibid.

14. Sun Tzu, *The Art of War*, 91.

15. Department of the Army, *The Army in Military Competition*, 11.

COL Jay Haley is the U.S. Army Europe and Africa (USAREUR-AF) G-2. He was commissioned in the Military Intelligence (MI) Corps branch and detailed to the field artillery in 1996. He has commanded at all levels from company to brigade. He holds a bachelor's degree from the University of Arizona and master's degrees from Webster University and the Joint Advanced Warfighting School.

LTC Christopher Heatherly enlisted in the U.S. Army in 1994 and earned his commission via Officer Candidate School in 1997. He has held a variety of assignments in special operations, Special Forces, and armored and cavalry units. His operational experience includes deployments to Afghanistan, Iraq, South Korea, Kuwait, Mali, and Nigeria. He holds master's degrees from the University of Oklahoma and the School of Advanced Military Studies.

Mr. Matthew Skilling is assigned to 66th MI Brigade-Theater as Chief of Open-Source Intelligence Operations, Army Europe Open Source Center, Wiesbaden, Germany. During his time in Germany, he has held a variety of positions within 66th MI Brigade-Theater and USAREUR-AF. Before becoming a Department of the Army Civilian, he served as a noncommissioned officer in the U.S. Army with one deployment to Afghanistan. Mr. Skilling holds a juris doctorate from Valparaiso University School of Law.

Ms. Laura Rettle is the USAREUR-AF G-2 Networks Operations Division Chief. She joined the Civil Service in 2010 after supporting U.S. Air Force and U.S. Navy operations as a contractor for 8 years. She has managed information technology development, implementation, and integration projects for a wide range of Department of Defense departments around the world. Since 2013, she has supported USAREUR operations in both the G-2 and G-6. She holds a bachelor's degree from Purdue University.

CPT Phillip Hoying enlisted as an intelligence analyst in 2010 and deployed to Iraq. Since 2012, he has served in numerous roles as an intelligence officer, most recently as the G-2 executive officer to USAREUR-AF. He holds a bachelor's degree from Hamilton College and a master of business administration from Germany's EBS Universität.

Mr. Ronald Bijeau entered the Civil Service in 1986 and has provided geospatial subject matter expertise as a member of the Engineer Regiment and MI Corps. Mr. Bijeau has held leadership roles with Army major commands, Army G-2 Staff, Army Geospatial Center, and the 60th Geospatial Planning Cell. Mr. Bijeau has been a proponent for advanced geospatial enterprise capabilities and geospatial engineer and geospatial intelligence integration throughout his career.

Mr. Jon Sadowski is an Army Civilian and veteran who served as an electric bass guitar player and imagery analyst. He has performed geospatial intelligence collection management roles as a Soldier, contractor, and civilian in a variety of organizations, including U.S. Africa Command, National Geospatial-Intelligence Agency, Defense Intelligence Agency, and National Reconnaissance Office. He holds a bachelor's degree from Portland State University in East Asian Studies.



U.S. ARMY NORTH INTELLIGENCE: AMERICA'S INTELLIGENCE

By Colonel Laura Knapp and Major John Holland

Introduction

Maintaining intelligence readiness and supporting unified land operations in the U.S. homeland requires the U.S. Army North (ARNORTH) (Fifth Army) intelligence enterprise to operate in a complex and contested theater. Nation-state competitors develop and advance capabilities that specifically aim at perceived seams in our homeland defenses and operate through a framework of constant global competition in every domain. While their influence may be declining, non-state adversaries pose a persistent threat to American interests—at home and abroad. The routine occurrence of natural and manmade disasters threatens U.S. communities everywhere, testing the resilience of whole-of-nation responses to save lives and alleviate suffering.

The ARNORTH headquarters, when directed by U.S. Northern Command (NORTHCOM) and resourced by Headquarters, Department of the Army, may serve as the theater Joint Force Land Component during crisis and conflict. In competition, the ARNORTH intelligence enterprise is responsible for executing the NORTHCOM commander's daily operational requirements—*Set the Theater* for intelligence and be prepared to *Set the Joint Operational Area* for intelligence for crisis and conflict. In conflict, the ARNORTH intelligence enterprise provides intelligence support to operational forces in order to deter, detect, and defeat foreign threats against the United States and the American people. Additionally, the intelligence enterprise provides intelligence support in coordination with partners and Services to protect and defend Department of Defense (DoD) assets and capabilities required to actively project combat power around the globe. Although the ARNORTH G-2 team is the smallest of all regional Army Service component commands, it has a very important mission—to provide intelligence for homeland defense.

ARNORTH's Intelligence Enterprise

ARNORTH's intelligence priorities are linked with the ARNORTH commander's priorities for the theater. Those intelligence priorities are—

- ◆ **People first**—The resiliency, readiness, and protection of the intelligence workforce and those we support are the cornerstone for everything we do.

- ◆ **Intelligence support to homeland defense**—Provide situational understanding for a multitude of foreign peer and near-peer threats to achieve the command's complex mission.
- ◆ **Intelligence support to defense support of civil authorities (DSCA)**—Rapidly respond in support of lead federal agencies, as well as local, state, tribal, and territorial governments, to save lives, prevent human suffering, and mitigate property damage by providing situational awareness, damage assessment, and incident awareness and assessment.
- ◆ **Intelligence support to theater security cooperation**—Remain the land-based security partner of choice by building regional security with our allies and partners through intelligence training and by supporting situational understanding of the operational environment.

From competition through conflict, the ARNORTH intelligence enterprise requires additional intelligence capabilities, which are outlined in combatant command operational plans. Military intelligence (MI) theater enablers, under operational control of ARNORTH, conduct mission command, intelligence collection, and single-source and all-source analysis, production, and dissemination. The 505th MI Brigade (U.S. Army Reserve MI brigade-theater [MIB-T]), headquartered at Camp Bullis, Texas, is the theater MI brigade support for ARNORTH and under operational control by ARNORTH when mobilized. The 505th MIB-T routinely trains with the ARNORTH team to build mission readiness and annually mobilizes a small portion of the brigade in direct support of the ARNORTH G-2. ARNORTH's assigned Theater Intelligence Operations Detachment comprises 35 Soldiers who, along with the annual mobilization of the 505th MIB-T U.S. Army Reserve Soldiers, form the theater analysis and control element and the theater G-2X.

The ARNORTH intelligence enterprise conducts analytic exchanges and authorized liaison with DoD, federal, foreign, state, local, and territorial partners in regard to defense-related foreign and counterintelligence activities. The ARNORTH intelligence enterprise also interfaces with key partners during DSCA missions for "other than intelligence

activities” to assist decision makers with government-provided information for damage assessment and situational awareness in an event expected to be declared an emergency or natural disaster.

Partner Integration—Joint, Interagency, and Multinational

The ARNORTH Assistant Chief of Staff G-2 relies on joint and interagency partnerships for nearly all operational and planning efforts. As the G-2 works to expand counterintelligence and human intelligence operations in a complex operating environment, constant coordination with NORTHCOM, U.S. Army Intelligence and Security Command (INSCOM), and our federal agency partners is crucial to ensure adherence to all applicable laws and policy. Additionally, our partnerships with intelligence elements of federal law enforcement agencies enhance our ability to obtain timely and relevant data pertaining to threats to the homeland and allow us to submit time-sensitive requests for information directly to the agents best suited to answer them. The G-2X requirements in Alaska require close coordination with multiple partners, including U.S. Army Pacific, Alaska Command, U.S. Army Alaska, and the 500th MIB-T. The G-2X currently has a liaison officer embedded with the Army Counterintelligence Center and five counterintelligence agents embedded with INSCOM supporting operations throughout the NORTHCOM area of responsibility. The G-2X also has three human intelligence collectors attached to NORTHCOM headquarters to support operations in Colorado Springs, Colorado.

The ARNORTH G-2 maintains a strong relationship with the U.S. Defense Attaché Office in Mexico and our Canadian partners in order to support theater security cooperation efforts between the United States and our partners. The ARNORTH G-2 coordinates and conducts intelligence subject matter expert exchanges, mobile training teams, and exercises with partner nations’ military and security forces to increase their intelligence capabilities and capacities. Our intelligence security cooperation efforts are linked to securing the land approaches from the north and south and support competition-phase engagement and homeland defense preparation.

To the north, ARNORTH G-2 focuses on interoperability with Canadian Armed Forces (CAF) for regional and global operations enhancement. Increased regional cooperation with CAF improves coordination and synchronization of cross-border operations. Moreover, we seek to improve interoperability with CAF for global (North Atlantic Treaty



United States and Canadian Soldiers work together through the Military Oriented Protective Posture decontamination process during DECON operations at Maple Resolve 18-01, Canadian Forces Base, Wainwright, Alberta, Canada, May 19, 2018. U.S. Army North and the Canadian Armed Forces plan year round for the Canadian Army's Exercise Maple Resolve, the largest allied exercise conducted in North America.

U.S. Army photo

Organization and coalition) operations in order to secure the homeland from abroad. Canada is not only a key defense ally of the United States but also shares electrical grids, fiber-optic networks, and oil and natural gas pipelines with the United States, as well as our longest common border.

With our partners to the south, ARNORTH seeks to bolster the defense and security of the U.S. southern approach. The ARNORTH G-2 led efforts to support the institutional capability growth, operational effectiveness, and interoperability of both the Secretaría de la Defensa Nacional (Secretariat of National Defense) and the Secretaría de Marina (Secretariat of the Navy) as a defense partner with the United States and in the region. Mexico remains an important defense partner for the United States, and we share a 2,000-mile land border where over one million legal border crossings occur each day—the most border crossings in the world. Mexico is also the country with the largest number of native Spanish speakers and is a key regional leader in Latin America.

Intelligence Support to U.S. Army North Operations

The ARNORTH intelligence enterprise is keenly aware of the trust the American people place in its military as well as the policies and sensitivities associated with conducting intelligence activities in the U.S. homeland. The ARNORTH intelligence enterprise mission in the homeland supports and complies with DoD and Service policies governing intelligence activities, as our intelligence efforts are linked to defense-related foreign and counterintelligence activities. ARNORTH policies and orders provide specific guidance to

safeguard against unauthorized collection against U.S. persons. Special emphasis is given to the protection of the constitutional and privacy rights of U.S. persons.

Intelligence in Homeland Defense

We expect attacks against our critical defense, government, and economic infrastructure to be one of the first actions our competitors take in an escalating crisis. The National Defense Strategy states that defending the homeland from attack is the number one defense objective. Understanding this, the ARNORTH G-2 continues to advance planning for the employment of intelligence capabilities to provide collection and analysis of indications and warnings of any such potential attacks by those competitors or other non-state threat actors who desire to harm our critical capabilities.



U.S. Army photo by SPC Brian Pearson

Bus carrying Soldiers from Urban Augmentation Medical Task Force 801-2 arrive at the Marriot Hotel Renaissance Center in Detroit, MI, April 10, 2020. U.S. Northern Command, through U.S. Army North, is providing military support to the Federal Emergency Management Agency to help communities in need.

ARNORTH, when operating as a Joint Force Land Component Command, executes homeland defense by detecting, deterring, preventing, and defeating threats from actors of concern associated with the land domain. Defending the homeland in the land domain neither begins nor ends at U.S. borders, so ARNORTH planning is guided by the construct of an active, layered defense that aims to deter and defeat aggression abroad and simultaneously

protect the homeland. It is a defense-in-depth that relies on the collection, analysis, and sharing of information and intelligence and the ability to rapidly generate and project warfighting capabilities to defend the United States, its allies, and its interests. Virtually all strategic threats to the homeland are based in areas of responsibility for other geographic combatant commanders; however, these threats can be employed against the U.S. homeland with a few computer keystrokes from any location, the deployment to international waters off our coasts, or the launching of an adversary's intercontinental ballistic missile. As the threats to the U.S. homeland are worldwide, cooperation in homeland defense intelligence operations hinges upon timely and accurate information and intelligence sharing.

Intelligence in DSCA—COVID-19 Support and Hurricane Recovery Efforts

DoD Directive 3025.18, *Defense Support of Civil Authorities (DSCA)*, defines DSCA as "support provided by U.S. Federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces...in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events."¹ In supporting DSCA events, the ARNORTH G-2 incorporates reporting from all classification levels from sources not normally associated with an Army Service component command headquarters. To be successful in a DSCA operating environment, the ARNORTH G-2 Operations Division facilitates information and intelligence sharing among various federal, state, and local entities in order to alleviate human suffering. Examples include damage assessments after a catastrophic event, such as a hurricane or the rupture of a dam, and line of communication analysis to aid agencies such as the Federal Emergency Management Agency (FEMA), enabling the ingress and egress to flooded areas.


During the coronavirus disease 2019 (COVID-19) pandemic response, the ARNORTH G-2 supported 5 division-level task force commands and 10 defense coordinating elements by deploying 15 counterintelligence special agents and more than 20 all-source intelligence officers and analysts. Their task and purpose were to provide foreign threat indicators and warning, conduct counterintelligence support to Title 10 of the U.S. Code force protection, aid in situational awareness, and manage requests for information to assist the forward-deployed forces. By forward-deploying intelligence teams throughout the United States, the ARNORTH G-2 was able to coordinate and liaise with multiple members of the intelligence community and federal law enforcement to ensure all responding Title 10 Soldiers understood the operating environment and received appropriate force protection support. The G-2's key contributions included

providing situational awareness of foreign-produced counterfeit N95 masks, foreign-based disinformation and misinformation related to the pandemic, and information supporting the establishment of a no-fly zone covering a deployed Army field hospital.

ARNORTH G-2 supports other DSCA events such as natural disasters, including hurricane strikes. In order to provide appropriate support, all ARNORTH G-2 operations officers are both DSCA I and DSCA II certified, providing them the knowledge and understanding of the FEMA-led joint, interagency operating environment in which providing life-saving capability and aid to state and local municipalities is the number one priority. Additionally, the G-2 works closely with the ARNORTH contingency command post as well as other mission command headquarters such as the three division-level task forces of the Defense Chemical, Biological, Radiological, and Nuclear Response Enterprise. The ARNORTH G-2 supports these commands by providing weather and environmental impacts information to the operating environment, line of communication analysis,

force protection support as required, and coordination of information assessment and awareness aerial platforms for the task force commander. During the 2017 response to Hurricane Maria, the ARNORTH G-2 was instrumental in providing accurate updates on lines of communication throughout Puerto Rico, enabling the timely delivery of federal aid to the island.

Conclusion

History has shown the ingenuity of our adversaries to challenge us on our own soil. The Black Tom Ammunition Depot bombing in World War I, Operation Pastorius in World War II, the 9/11 attacks, Iran's failed assassination plot against the Saudi ambassador in 2011, and the massive Russian cyber-attack in 2021 all serve as examples of the cunning strategies employed within the United States. Threats to the homeland are real. The ARNORTH G-2 continues to detect and illuminate threats, ensuring our command is able to respond and defeat our adversaries. 

A History of Foreign Adversary Attacks in the United States

Black Tom Ammunition Depot bombing, World War I: The explosion at the Black Tom depot in New Jersey occurred on July 30, 1916, blowing out tens of thousands of windows across the harbor in Manhattan. Because the blast occurred at 2:08 a.m. on a Sunday, fewer than 10 people were killed; however, the blast destroyed a massive amount of military goods. The United States had not yet entered World War I and was officially neutral which allowed American munitions dealers to legally sell to any of the warring nations. Most of the arms, were going to Britain, France, and Russia because the British navy had blockaded Germany. The initial investigation concluded that the explosion was an accident; however, in the 1930s, New York lawyer John McCloy amassed enough evidence to prove that the explosion had in fact been the work of German saboteurs.²

Operation Pastorius, World War II: Operation Pastorius was a failed 1941 Nazi plan, in which German submarines put two teams of infiltrators ashore in New York and Florida to sabotage defense-related industries in the United States. All of the saboteurs had been born in Germany, lived in the United States, and then returned to their homeland. However, before they could strike, one of the participants foiled the plot by revealing the details to the Federal Bureau of Investigation. The eight saboteurs who had already entered the United States were subsequently arrested.³

9/11 attacks: September 11 attacks, also called 9/11 attacks, were a series of airline hijackings and suicide attacks committed in 2001 by 19 militants associated with the Islamic extremist group al-Qaeda against targets in the United States, the deadliest terrorist attacks on American soil in U.S. history.⁴

Iran's failed assassination in 2011: On 11 October 2011, two men with ties to Iran were charged with planning to assassinate Adel al-Jubeir, the Saudi ambassador to the United States. According to the U.S. Justice Department, the aim was to bomb a restaurant in Washington, DC, frequented by Jubeir. The plot was thwarted by U.S. officials.⁵

Endnotes

1. Department of Defense Directive 3025.18, *Defense Support of Civil Authorities (DSCA)* (Washington, DC, December 29, 2010, incorporating Change 2, March 19, 2018), 18.
2. James M. Lindsay, "TWE Remembers: The Black Tom Explosion," *The Water's Edge* (blog), *Council on Foreign Relations*, July 30, 2014, <https://www.cfr.org/blog/twe-remembers-black-tom-explosion>.
3. *Encyclopaedia Britannica Online*, s.v. "Operation Pastorius," accessed October 28, 2021, <https://www.britannica.com/topic/Ex-Parte-Quirin#ref1197098>.
4. *Encyclopaedia Britannica Online*, s.v. "September 11 attacks," accessed October 28, 2021, <https://www.britannica.com/event/September-11-attacks>.
5. Ewen MacAskill, "Iranians charged in US over plot to assassinate Saudi ambassador," *The Guardian*, October 11, 2011, <https://www.theguardian.com/world/2011/oct/11/iranians-charged-us-assassination-plot>.

COL Laura Knapp serves as the G-2 for U.S. Army North (Fifth Army). Her previous assignments include various tactical and strategic positions, most recently as Assistant Joint Staff J-2 and Commander, 504th Expeditionary-Military Intelligence Brigade. She is a graduate of the U.S. Military Academy and holds a graduate degree from the Air Command and Staff College.


MAJ John Holland is a strategic intelligence officer serving as the Deputy Analysis and Control Element Chief for the U.S. Army North (Fifth Army) G-2. He most recently served as the U.S. Central Command Deputy J-5 Executive Officer. MAJ Holland is a graduate of the University of Houston and holds a graduate degree from the National Intelligence University.



ARMY DOCTRINE PUBLICATION (ADP) AUDIOBOOKS

ADP 1 THE ARMY	ADP 2-0 INTELLIGENCE
ADP 3-0 OPERATIONS	ADP 3-05 ARMY SPECIAL OPERATIONS
ADP 3-07 STABILITY	ADP 3-19 FIRES
ADP 3-28 DEFENSE SUPPORT OF CIVIL AUTHORITIES	ADP 3-37 PROTECTION
ADP 3-90 OFFENSE & DEFENSE	ADP 4-0 SUSTAINMENT
ADP 5-0 THE OPERATIONS PROCESS	ADP 6-0 MISSION COMMAND: COMMAND & CONTROL OF ARMY FORCES
ADP 6-22 ARMY LEADERSHIP & THE PROFESSION	ADP 7-0 TRAINING

U.S. Army Combined Arms Doctrine Directorate (CADD)
<https://usacac.army.mil/organizations/mccoe/cadd>



HAVE YOU DOWNLOADED THE DOCTRINE APP?
IT'S FAST & IT'S EASY!

DOCTRINE COMPREHENSIVE GUIDE	AUDIO BOOKS	DOCTRINE APP	BREAKING DOCTRINE PODCAST

ARMY OPERATIONS IN THE ARCTIC

American and Canadian personnel participate in a simulated aerial assault as part of Arctic Warrior 21. A detachment from the Royal Canadian Air Force's 450th Tactical Helicopter Squadron, based out of Petawawa, Ontario, joins elements of 1st Battalion, 52nd Aviation Regiment, and 1st Attack Reconnaissance Battalion, 25th Aviation Regiment, both from Fort Wainwright, AK, for the flight.

Mr. Michael Gearly

Introduction

The Arctic region is a place of vast natural resources, ever-changing climactic conditions, and international strategic competition. The U.S. Army seeks to regain a footing of Arctic dominance in order to maintain peace and prosperity in the Arctic as part of U.S. national security interests. Tactical operations in the Arctic environment pose challenges not only to Army equipment but also to the human element—Soldiers—as well.

Before we begin to discuss the details of human and equipment factors in cold weather regions and climates, let us first consider the question, Why conduct military operations in the Arctic?

The Department of Defense (DoD) updated its strategic objectives for the Arctic in the 2019 *Report to Congress, Department of Defense Arctic Strategy*, to reflect the evolving Arctic security environment and the release of the 2018 National Defense Strategy. The report states, “DoD’s desired end-state for the Arctic is a secure and stable region in which U.S. national security interests are safeguarded, the U.S. homeland is defended, and nations work cooperatively to address shared challenges.”¹ The DoD Arctic strategy “is informed by the 2017 National Security Strategy and anchored in the priorities of the 2018 National Defense Strategy (NDS) and its focus on competition with China and Russia as the principal challenge to long-term U.S. security and prosperity.”²

As an Arctic nation, the United States is responsible for providing Arctic-capable forces to support multi-domain operations in defense of national security interests from regional as well as global threats. The Army must also be able

and ready to provide and sustain Arctic-capable forces for employment outside the region if necessary. This requires the Army to provide its Soldiers with the appropriate equipment, training, and doctrine to operate in extreme cold weather conditions.

Security Implications in the Arctic Region

The United States is an Arctic nation. The Arctic security environment has direct implications for U.S. national security interests. Geographically, the Arctic comprises the northern approaches of the United States and represents a potential vector both for attacks on the homeland and for U.S. power projection. Approaches to the Arctic Ocean on both the east and west of the United States form strategic corridors for maritime traffic. Arctic sea routes transit through the Bering Sea between the United States and Russia, while the Greenland, Iceland, United Kingdom, and Norway gap (also known as the GIUK–N gap) is a strategic corridor for naval operations between the Arctic and the North Atlantic.³

The Arctic region comprises eight nations with sovereign territory in the Arctic: Canada, Denmark (including Greenland), Finland, Iceland, Norway, Russia, Sweden, and the United States. Excluding Russia, these Arctic nations are North Atlantic Treaty Organization allies. Additionally, China’s increased presence in the Arctic and Russia’s growing economic and military ambitions in the region highlight how both nations have long-term strategic designs for the Arctic. By 2035, an increased military presence by both countries can be expected.⁴

Russia is the largest Arctic nation by landmass, population, and military presence above the Arctic Circle. Russia formed

the Northern Fleet Strategic Command in 2014 to coordinate its renewed emphasis on the Arctic. Russia has gradually strengthened its presence by creating new Arctic units, refurbishing old airfields and infrastructure in the Arctic, and establishing new bases along the Arctic coastline. There is also a concerted effort to establish a network of air defense and coastal missile systems, early warning radars, and a variety of sensors.⁵

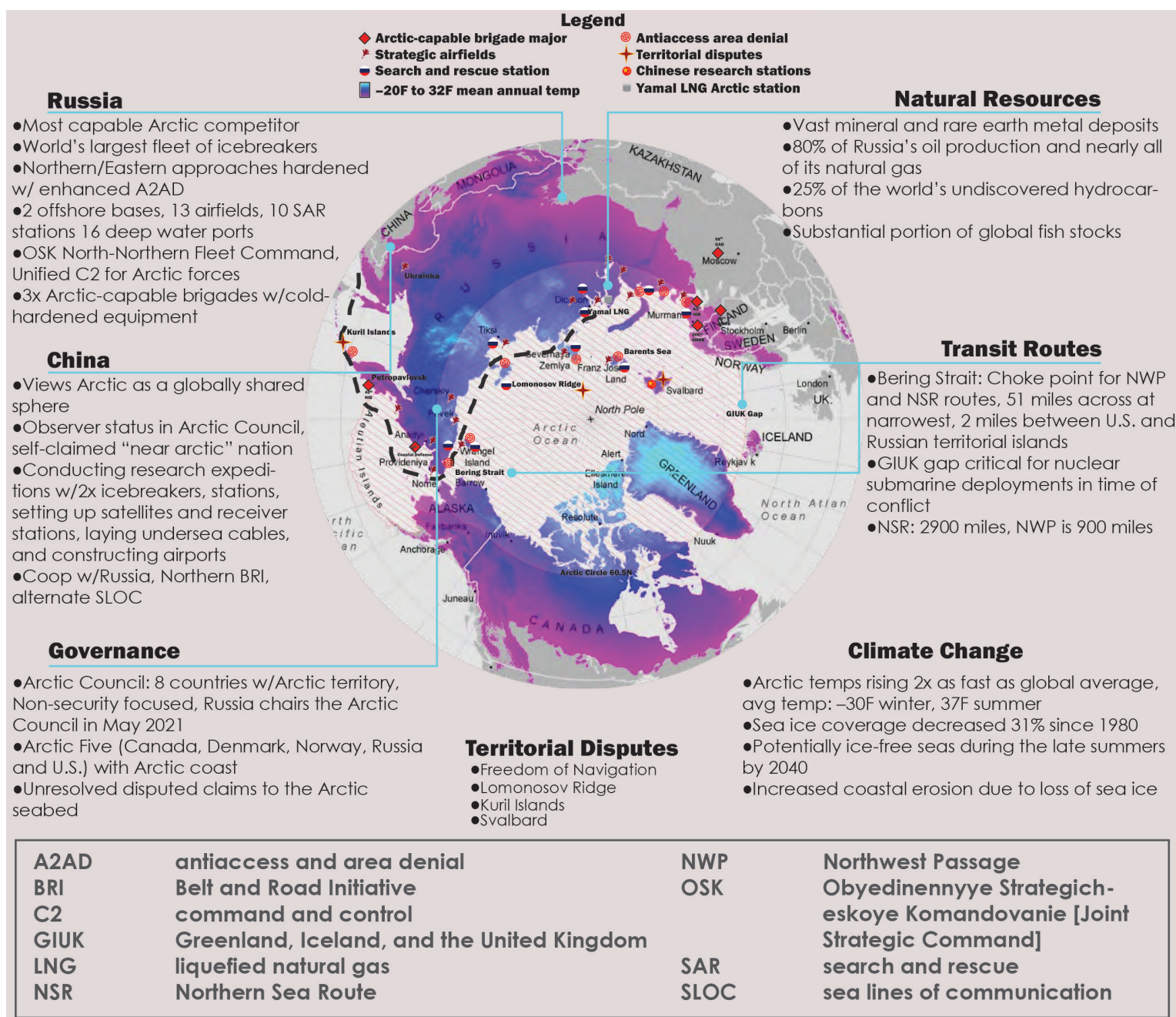
The DoD's desired end state for the Arctic is a secure and stable region where U.S. national interests are safeguarded, the U.S. homeland is defended, and nations work cooperatively to address shared challenges. Protecting U.S. national security interests in the Arctic will require the joint force to sustain its military advantages in the Indo-Pacific and Europe, identified in the National Security Strategy as key

regions of strategic competition, and to maintain a credible deterrent for the Arctic region. The DoD must be able to quickly identify threats in the Arctic, respond promptly and effectively to those threats, and shape the security environment to mitigate the prospect of those threats in the future. The 2019 DoD Arctic Strategy outlines three strategic ways that support the desired Arctic end state:

- ◆ Building Arctic awareness.
- ◆ Enhancing Arctic operations.
- ◆ Strengthening the rules-based order in the Arctic.

Historical Perspective

From a historical perspective, especially during World War II, Alaska was an extremely active Arctic theater of operations. During World War II, the United States Army



Great Power Competition in the Arctic⁶

administered the construction of the 1600-mile Alaska-Canada military highway and an array of 300 airfields and posts throughout the territory that supported the war in the North Pacific and enabled the delivery of Alaska-Siberia Lend-Lease aircraft to the Soviet Union. Additionally, units assigned to the 7th Infantry Division assaulted and defeated Japanese forces on the Aleutian island of Attu in May 1943. The 87th Infantry Regiment (later assigned to 10th Mountain Division) led the Allied assault of Kiska in August 1943. Both assaults were key in preventing Japanese forces from gaining footholds on American soil in the Aleutians.

When the Berlin Wall fell in 1989, the subsequent dissolution of the Soviet Union signified an end to the Cold War and portended a shift in Alaska's military significance. During the 1990s, the Army inactivated the 6th Infantry Division and resurrected U.S. Army Alaska as a component of a newly reestablished Alaskan Command.

U.S. Army photo by SSG Alex Skripnichuk



A paratrooper with 3rd Battalion, 509th Parachute Infantry Regiment, 4th Infantry Brigade Combat Team (Airborne), 25th Infantry Division, secures his equipment during an airfield-seizure operation at Donnelley Training Area, AK, February 7, 2021.

The Soviet Union and later Russia never lost interest in the Arctic—beginning in 2010, Russia invested over \$1 billion to refurbish 13 airfields, enhance search and rescue capabilities, and upgrade radar stations to improve awareness in the air and maritime domains. These systems create a “protective dome” across Russia's vast Arctic coastline and improve its operational capability to detect and track vessels and aircraft.

The Arctic Environment

The real enemy in the Arctic, many experts say, is the Arctic environment itself. Temperatures exceeding minus 60 degrees Fahrenheit are common during winter months. Windchill factors can be well below minus 150 degrees Fahrenheit, depending on ambient temperatures and wind speeds. However, the complexity of conducting military operations in the Arctic environment of Alaska is compounded

not only by the extreme cold but also by the inescapable trend of global warming.

Today, the entire vast region north of the Arctic Circle is warming twice as fast as the rest of the world, opening up new opportunities for natural resources, shipping routes, and commercial fishing. While long-term trends point to a more consistently navigable Arctic, other factors make it difficult to predict what the near-term environmental conditions will be. Though the Arctic continues to lose increasing amounts of multiyear sea ice, the remaining ice is becoming less predictable. For example, heavy pack ice conditions rendered the Northwest Passage impassable for some ships in 2018, despite its being one of the warmest periods on record. Furthermore, decreased sea ice and glacial mass will open access to currently unclaimed natural resources. These factors combined make the region a potential hotbed of activity, economic competition, and possible miscalculation of intentions or actions.

The challenges of the Arctic, however, are not only due to extremely cold temperatures. In many cases, mobility is actually at its highest state in the Arctic winter. Summer months pose significant challenges for many wheeled vehicles, while the most challenging period is the spring thaw when ground movement becomes impossible across vast swaths of tundra. Regardless of season, mobility by air is critical to Army operations. Today and for the foreseeable future, the Arctic presents a harsh and demanding environment for Army operations.

U.S. Army End State

Today, our Army exists to protect our Nation and to preserve the peace. To meet that essential requirement, the Army must man, train, equip, and organize to win in the Arctic. The Arctic is simultaneously an area of competition, a line of attack in conflict, a vital area holding many of our natural resources, and a platform for global power projection.

Army Arctic Strategy End State

The U.S. Army is able to rapidly generate and project multi-domain forces that are specifically trained, equipped, and sustained to fight, survive, and win in extreme cold weather and mountainous conditions over extended periods.

The *DoD Arctic Strategy* calls for the Arctic to remain a secure and stable region where our national security interests are safeguarded, as set forth in three objectives:⁷

- ◆ Defend the homeland.
- ◆ Compete when necessary to maintain favorable regional balances of power.
- ◆ Ensure common domains remain free and open.

The initial drive toward the Army end state will be investing in a Multi-Domain Task Force-enabled division headquarters, along with specially trained and equipped combat brigades to regain U.S. Army cold weather dominance. In order to meet these objectives, the Army will conduct five lines of effort:


- ◆ Improve Arctic Capability—Building the basic Arctic capability across the force, addressing persistent problems from Arctic-stationed organizations, and anticipating and mitigating the impact of a changing environment on infrastructure and operations.
- ◆ Compete in the Arctic and Globally—Achieving a strengthened network of allies and partners to compete in the Arctic, and identifying and partnering with local and foreign indigenous forces.
- ◆ Defend the Far North in Crisis and Conflict—Deterring or defeating land threats to the far north.
- ◆ Build Arctic Multi-Domain Operations—Experimenting and advancing combined joint all-domain command and control in support of multi-domain operations, and projecting multi-domain effects across the region.
- ◆ Project Power across the Arctic—Projecting power to dynamically employ Army forces in crisis and conflict.⁸

The Army will regain cold weather, high altitude, and high latitude dominance by adapting how the Army generates, postures, trains, and equips our forces to execute extended, multi-domain operations in extreme conditions. Restoring dominance also mandates an inherently multicomponent approach with significant contributions for the Army Reserve and National Guard. The Army will implement integrated solutions that emphasize readiness for operations in extreme cold and mountainous environments and bolster the resiliency of our Soldiers, our people, and our installations. The Army is committed to a Total Army approach to meeting joint warfighter requirements around the globe. This restored dominance provides key and critical options to the joint force commander to employ decisive land warfare capabilities in support of worldwide operations.

Conclusion

The Army requires Arctic-capable units, regardless of where they are stationed, able to deploy to any extreme cold weather, snowy, high latitude, or high altitude environment. These units require appropriate equipment, individual and unit proficiency, and appropriate doctrine. Additionally, the Army must have the capability to deploy and sustain these

forces in combat operations. The most challenging aspect of making Arctic units combat-ready will be ensuring sufficient individual and collective training to achieve and maintain proficiency. Soldiers must possess special skills, have the physical and mental endurance, and undergo extensive training to build expertise in extreme cold weather conditions. Units must have undergone rigorous training under realistic conditions.

A prime example of this type of rigorous, realistic training recently took place at Donnelly Training Area near Delta Junction in central Alaska. In February 2021, 4th Infantry Brigade Combat Team (Airborne), 25th Infantry Division, completed exercise Arctic Warrior 21, a large-scale exercise to test the Army's capabilities in extreme cold weather. This experience showed firsthand how the harsh arctic environment could affect every facet of military operations, including military intelligence. For the military intelligence community, preparation for the battlefield becomes even more complex when accounting for unknown factors. Temperatures exceeding minus 50 degrees Fahrenheit and windchill factors exceeding minus 80 degrees Fahrenheit affected equipment, personnel, and operations in a way that was difficult to forecast. To survive and win in combat, in an arctic environment, military intelligence Soldiers must maintain an in-depth understanding of limitations and effects, remain alert, and always work as a team. 

Endnotes

1. Department of Defense, *Report to Congress, Department of Defense Arctic Strategy* (Washington, DC, June 2019), 2, <https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF>.
2. Ibid.
3. Department of the Army, *Regaining Arctic Dominance: The Army in the Arctic* (Washington, DC, 19 January 2021), https://www.army.mil/e2/downloads/rv7/about/2021_army_arctic_strategy.pdf.
4. Department of the Army, *The Arctic through 2035: An Overview of the Operational Environment and Competitor Strategies for U.S. Army Training, Doctrine, and Capabilities Development* (Fort Leavenworth, KS: U.S. Army Training and Doctrine Command, July 2020), https://oe.tradoc.army.mil/wp-content/uploads/2020/07/U-The-Arctic-Through-2035_20200721.pdf.
5. Department of the Army, *The U.S. Army in the Arctic Version 2.0, Draft 2.1* (Washington, DC: n.d.).
6. U.S. Army Training and Doctrine Command, "MI Lessons Learned Forum," PowerPoint presentation, 20 May 2021.
7. Department of Defense, *Report to Congress*, 6–7.
8. Department of the Army, *Regaining Arctic Dominance*, 28.

Mr. Michael Gearty is a collector and analyst on the U.S. Army Intelligence Center of Excellence's Lessons Learned team. He previously served as an Army military intelligence officer with the 6th Infantry Division (Arctic Light) in Alaska and the 10th Mountain Division, Fort Drum, NY, in addition to other light infantry division assignments.



UNDERSTANDING EMERGING SPACE DOMAIN THREATS AND THEIR EFFECTS ON LAND-BASED OPERATIONS

By Captain Andrew Compean and Mr. Daniel Selman

Introduction

Today's battles cannot be fought, nor the battlespace properly visualized, without being enabled by space—that's the bottom line and irrefutable reality of modern warfare. Our military today is as critically reliant on space as the ancient Greek army was on the phalanx to dominate that era's battlefields. Without crucial space-enabled capabilities ubiquitously supporting the various warfighting functions to joint, Service, and emerging multi-domain operations forces, the U.S. military would likely be unable to effectively plan, execute, sustain, or decisively win wars. By extension, the U.S. Army likely could not effectively conduct the breadth of land-based operations it must undertake to seize, control, and dominate that domain and defeat the enemy on the ground. Competition and conflict in the future will be reliant even more heavily on space. Coalition warfare further highlights the criticality and force-multiplying effects of space-enabling technologies by providing command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), and common operational pictures informed synergistically by space systems of the United States and many coalition partners.

Emerging Space and Counterspace Threats

When Army intelligence officers train for land operations, the reality of how space can affect both enemy and friendly

actions, sometimes decisively, is virtually absent and is unwittingly taken for granted. This is because since the 1960s, the United States has maintained the world's largest and most sophisticated constellation of satellites in support of the Department of Defense and national policy; no other country was even close, with the exception of the Soviet Union during the bipolar era. In today's multipolar world, the battlespace is rapidly evolving, and space is no longer the exclusive domain of two dominant world powers to uniquely enhance all military operations. Nor is it the sanctuary it once was.

Competitors are developing and fielding sophisticated technologies that contest American space power. Global technology trends, and greatly reduced costs of commercial space technologies and launch services since the early 1990s, have supported explosive growth in the number of objects in space, provided near-universal access to space, and enabled even second- and third-world countries to acquire advanced technologies. Global technology trends are also creating or boosting nascent or developing scientific and engineering capacities that are countering the U.S. competitive advantage.¹ Some argue that in aspects of space utilization and technological advancements, Russia and China are on par with or have even surpassed the United States. Those same advanced commercial technologies

are used for military applications and support military and warfighting functions. Moreover, the increasing dual-use capabilities of these commercial systems can obscure end users and intent, and challenge the ability of the United States to provide unambiguous and advanced warning between peaceful and potentially hostile intent/use.²

Counterspace

Counterspace is a mission, like counterair, that integrates offensive and defensive operations to attain and maintain the desired control and protection in and through space. These operations may be conducted across the tactical, operational, and strategic levels in all domains (air, space, land, maritime, and cyberspace), and are dependent on robust space situational awareness and timely command and control. Counterspace operations include both offensive counterspace and defensive counterspace operations. Counterspace is also referred to as “space control.”³

We, as intelligence professionals, must be aware of the existing and emerging space and counterspace threats that could significantly alter or affect the operational environment worldwide. With the recent re-establishment of U.S. Space Command and the creation of the U.S. Space Force, this sea change within the Department of Defense highlights the space domain’s maturation and its vital concern for the United States—not only how the United States views space, but also how the adversary views and uses space. We will further discuss adversary and global advancement of space capabilities and the planning considerations that an Army intelligence professional should undertake when supporting land operations.

Space-Based Support for Military, Commercial, and Civilian Applications

Over the past couple of decades, the use of space has dramatically expanded in both the number and types of satellites in orbit, as well as commercial entities making access to space and the various services they provide more affordable. Access to space is becoming more common and attainable by state and non-state entities that previously did not have the money, influence, or industrial and technological capacity to do so. As with any new advancement and opportunity, new risks are also introduced. Countries worldwide, regardless of economic status, are

introducing, advancing, and expanding their space access and utilization after observing the revolutionary benefits of space applications, principally by the United States. They are achieving these feats by the use of diplomatic, information, military, and economic, also known as DIME, spheres, particularly for education, technology, and military sectors. In the military realm, it should come as no surprise that any new type of technological capability or advancement can be applied for both defensive and offensive purposes, and space-enabled capabilities are no exception. Figure 1 shows countries that have on-orbit satellites, the capabilities of those satellites, and the numeric representation of the satellites they own.

Protests to U.S. Space Operations

Both China and Russia, the United States main competitors in space, have taken overt and deliberate steps to challenge and restrain the United States use of and operations in space because both view the United States as seeking to dominate and militarize space. Both countries have openly protested, most notably and formally at the United Nations, the United States use of space as hostile. Both continued their protest by stating that any action they undertake in space is in direct response to their perceptions of the U.S.

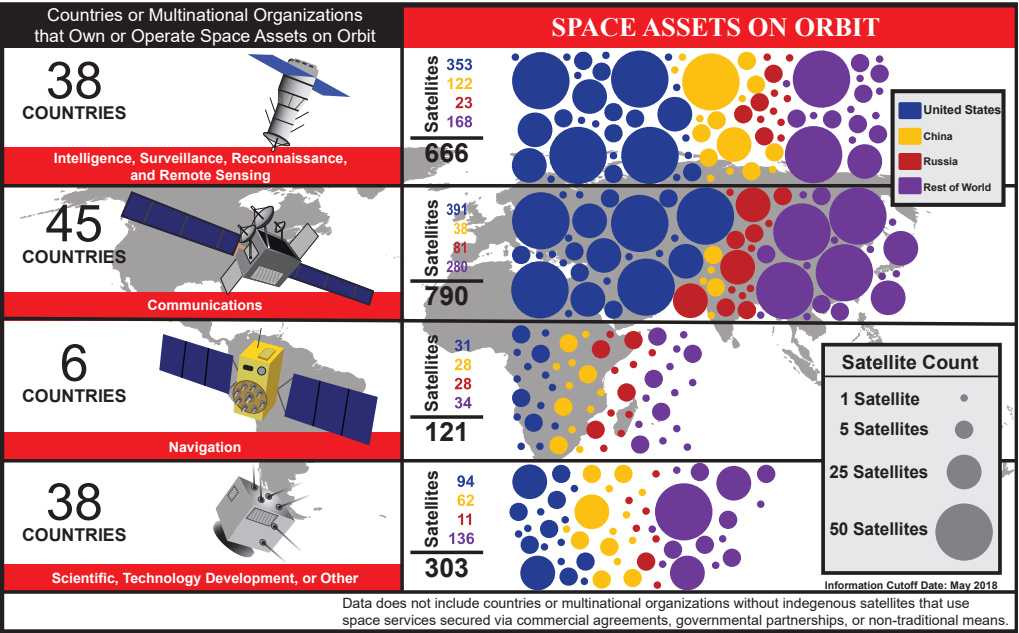


Figure 1. Space Assets on Orbit⁴

threat and is defensive in nature. In the following sections, you will see that their statements, actions, and protestations are hypocritical and ironic.

Chinese and Russian Views of Space and Counterspace

With the evolution and advancement of space-based capabilities, both Chinese and Russian military doctrines view space as an essential force multiplier and both view

counterspace capabilities, ironically, as a means to reduce United States and allied operational effectiveness. In 2015, both countries reorganized their militaries and emphasized the utilization of space for modern military operations.⁵ Both countries developed or consolidated specialized space units and committed significant national funds to improve essential space services such as space lift, satellite communications (SATCOM), satellite navigation (satnav), space-based ISR, space domain awareness, satellite control, and infrastructure. The advancement and employment of these capabilities will more effectively enable their governmental organs to conduct strategic communications, diplomatic functions, and economic strategies. They will also enable their military's ability to execute deployment; sustainment; maneuver; command, control, and communications; and full spectrum military operations regionally and worldwide. These capabilities will also enable them to search, track, identify, monitor, and possibly target U.S. and allied military forces operating in any area of operations. They are pursuing the same ability to maintain awareness of the space domain, particularly for U.S. and allied space assets.⁶ Both countries have put a premium on the ability to search, track, identify, characterize, and monitor satellites in all orbits. Having

this capability critically supports both Chinese and Russian space and counterspace programs. Having space domain awareness is the foundation of space and counterspace operations, and the counterspace continuum of threats, which range from reversible to nonreversible effects against space systems and supporting ground systems and infrastructure through kinetic and non-kinetic means. Both countries continue to develop a full range of counterspace capabilities, which include offensive jamming and cyberspace weapons, directed-energy weapons, on-orbit systems, and ground-based direct-ascent antisatellite missiles. Figure 2 shows the counterspace continuum that represents the range of threats to space-based capabilities, arranged from reversible to nonreversible effects. Reversible effects are nondestructive and temporary, while nonreversible effects can cause physical and permanent damage.

Russian Space and Counterspace Policy and Capabilities

Russia's space program is a source of national pride. Moscow views itself as a world leader in space development and particularly prides itself as being the first nation in space in 1957. After the Soviet Union dissolved in 1991, Russia inherited the extensive space infrastructure, technology, and the former Soviet Union's place among the global space powers.⁸ However, at the end of the Cold War, a combination of budgetary constraints, an economic implosion, and technological setbacks caused a decay of Russian space capabilities.⁹ Despite these setbacks, Russia implemented a set of programs and initiatives over the last decade to regain many of its Cold War-era space and counterspace capabilities and former prominence. Its counterspace program includes extensive electronic warfare (EW) systems to deny, degrade, and disrupt communications and Global Positioning System (GPS)/positioning, navigation, and timing (PNT); ground-based, mobile missiles to directly attack satellites in low Earth orbit; and directed-energy weapons to deny the use of space-based imagery.¹⁰

Russia's military doctrine and authoritative writings clearly articulate that Moscow views space as a warfighting domain and that achieving supremacy in space will be a decisive factor in seizing the initiative and winning future conflicts.¹¹ Russia considers the "intention to place weapons in outer space," an allusion to the United States military space program, a main external military danger, and describes establishing "an international treaty on [the] prevention of placement of any types of weapons in outer space" as a principal task for the Russian state in its military doctrine.¹² Moscow views space as a key enabler of U.S. precision strike and military force projection capabilities. When

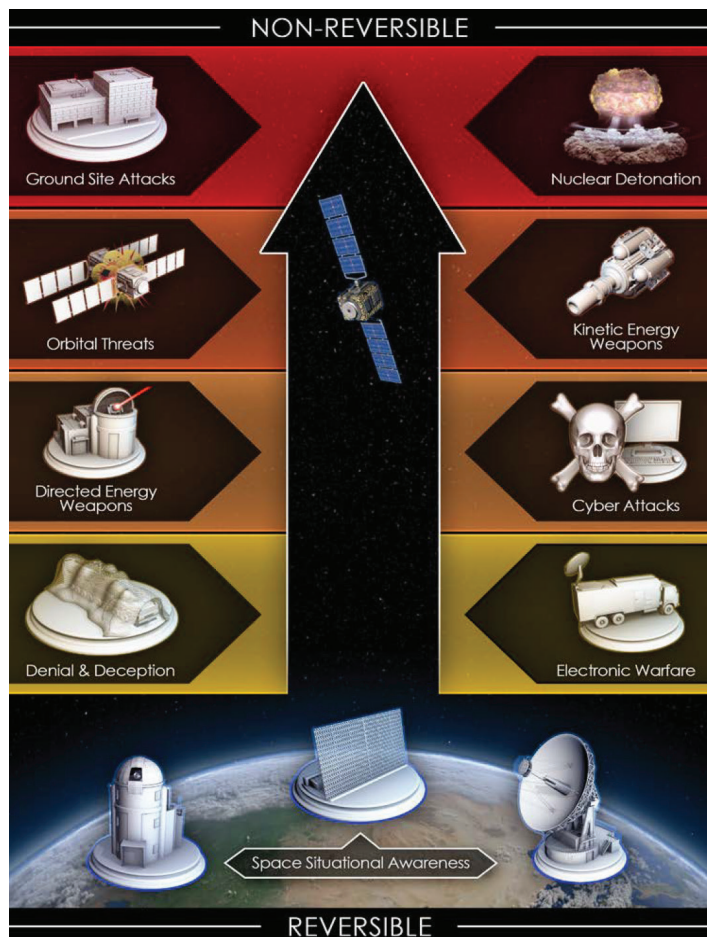


Figure 2. Counterspace Continuum—From Reversible to Nonreversible Effects⁷

paired with United States missile defense systems, Russia believes United States space-enabled, conventional precision strike capabilities undermine Russia's strategic stability.¹³ At the same time, Russia views America's perceived dependence on space as the "Achilles' heel" of American military power, which can be exploited to achieve Russian conflict objectives.¹⁴ Russia is, therefore, pursuing counterspace systems and employment strategies to neutralize, deny, or limit United States military and commercial space-based services to offset a perceived United States military advantage.¹⁵

Russian counterspace capabilities that directly affect United States and allied land operations will principally be EW attacks against GPS and SATCOM. The Russian military views EW as an essential tool for gaining and maintaining information superiority over its adversaries, allowing Russia to seize the operational initiative by disrupting adversary command, control, and communications; battlespace awareness; GPS/PNT; and intelligence capabilities. Russia has operational experience in the use of counterspace EW capabilities from recent and ongoing expeditionary military campaigns, enabling continual refinement of its tactics, techniques, and procedures, as well as use in Russia to protect strategic locations and VIPs.¹⁶ Russia has fielded a wide range of ground-based EW systems to counter GPS, tactical communications, SATCOM, and radars. Mobile systems include radar and SATCOM jammers. Russia aspires to develop and field a full spectrum of EW capabilities to counter Western C4ISR and weapons guidance systems with new technology, data transfer, and capabilities for peacetime and wartime use in the near term.¹⁷ Russia has a multitude of systems that can jam GPS receivers within a local area, potentially interfering with the guidance systems of manned aircraft, unmanned aerial vehicles, guided missiles, and precision-guided munitions, but it has no publicly known capability to interfere with the GPS satellites themselves using radio-frequency interference.¹⁸ Russian GPS jammers could also affect many United States military communications and other equipment enabled by the GPS timing function. Despite overwhelming evidence that Russia has operationally employed mobile,

ground-based EW counterspace weapons both within its borders and abroad, the Russian state has repeatedly denied any wrongdoing.¹⁹ Russia is expected to continue developing ground-based EW weapons, and new evidence suggests Russia may be developing high-powered space-based EW platforms to augment the ground-based platforms.²⁰

Satellite command and data distribution networks expose space systems, ground infrastructure, users, and the links connecting these segments to cyber threats. Being aware of these vulnerabilities, Russia also considers offensive cyber capabilities as a key asset for maintaining military advantage, and as a result, is researching and developing cyber capabilities to affect these elements.²¹

United States and allied forces operating in areas with known Russian forces must be aware and expect that EW will most likely be encountered, intentionally or unintentionally. Having equipment properly encrypted and knowing the signs of an EW attack will help mitigate the effects. Military intelligence professionals can assist by helping to understand adversaries' EW capabilities and employment tactics, techniques, and procedures, and by anticipating and planning for their effects during the military decision-making process, and more specifically during the intelligence preparation of the battlefield (IPB) process. Putting forth an inject of jammed SATCOM or GPS during unit training and exercises will cause the planners, operators, and leaders to think about how military operations are affected by this asymmetric threat, and their response to these non-kinetic effects. As intelligence professionals, it is our responsibility to account for and characterize adversary non-kinetic capabilities and potential effects, and the way in which they enable adversaries' kinetic capabilities in support of their broader military operations.



Russia has invested heavily in developing sophisticated electronic warfare capabilities, including this Krashuka-4 jammer.

Photo courtesy of Russia Ministry of Defense via Creative Commons 4.0

Chinese Space and Counterspace Policy and Capabilities

China is rapidly growing its space program by continually developing and operationally deploying new and technologically advanced space and counterspace capabilities. Beijing now has a goal of “[building] China into a space power in all respects.”²² China is second only to the United States in the number of operational satellites, which are a source of national pride and part of President Xi Jinping’s “China Dream” to establish a powerful and prosperous China.²³ China deploys both space and counterspace capabilities for both civil and military means. China officially advocates for peaceful use of space and is pursuing agreements at the United Nations on the non-weaponization of space.²⁴ Though it advocates for the peaceful use of space, China continues to improve its counterspace weapons’ capabilities and has enacted military reforms to better integrate cyberspace, space, and EW into joint military operations.²⁵

The People’s Liberation Army (PLA) views space superiority as the ability to control the information sphere and deny adversaries the same; these are key components of conducting modern “informatized” wars.²⁶ The PLA uses “informatized” warfare to describe the process of acquiring, transmitting, processing, and using information to conduct joint military operations across the domains of land, sea, air, space, cyberspace, and the electromagnetic spectrum during a conflict.²⁷ The PLA historically has managed China’s space program and continues to invest in improving China’s capabilities in space-based ISR, SATCOM, and satnav, as well as human spaceflight and robotic space exploration.²⁸ As part of the military reforms announced in 2015, China established the Strategic Support Force to integrate cyberspace, space, and EW capabilities into joint military operations.²⁹ The Strategic Support Force forms the core of China’s information warfare force, supports the entire PLA, and reports directly to the Central Military Commission, China’s highest military governing body. The Strategic Support Force is likely responsible for the research and development of certain space and counterspace capabilities.³⁰

The PLA considers EW capabilities key assets for modern warfare, and the PLA’s doctrine emphasizes using

EW weapons to suppress or deceive enemy equipment.³¹ Currently, China has the ability to jam common SATCOM frequency bands and GPS signals, and it has made the development and deployment of satellite jamming systems a high priority.³² China is further developing jamming systems that will target a large range of commercial SATCOM frequencies, as well as United States military-protected communication bands.³³ The PLA routinely incorporates jamming and anti-jamming techniques against multiple communication systems, radar systems, and GPS satellite systems in exercises.³⁴ In 2018, the Strategic Support Force even carried out advanced military exercises simulating a complex EW environment with the “[Strategic Support Force] SSF base pitted against five PLA Army, Air Force, and Rocket Force units.”³⁵



This Chinese *Yuan Wang* space tracking ship, which supports space launch operations from positions in the Pacific, is part of China's Space Situational Awareness network.

As with Russia, China considers offensive cyber capabilities as a key asset for maintaining military advantage and integrated warfare.³⁶ China is also researching and developing cyber capabilities to threaten satellite command and data distribution networks, space systems, ground infrastructure, users, and the links connecting these segments.³⁷

Although official Chinese statements on space warfare and weapons have remained consistently aligned to peaceful purposes, China has recently designated space as a military domain.³⁸ PLA military writings state that the goal of space warfare and operations is to achieve space superiority using offensive and defensive means in connection with their broader strategic focus on asymmetric cost imposition, access denial, and information dominance.³⁹ At its current and projected pace of advancement and employment, China’s space and counterspace programs present one of the most profound threats to United States and allied space

operations for the foreseeable future. China will continue to advance these capabilities to more effectively enable and directly support land and maritime operations, particularly within its regional sphere of influence, and to support its broader and long-term global strategic, military, diplomatic, and economic goals.

United States forces and allies operating within the United States Indo-Pacific Command area of responsibility have likely encountered Chinese space and counterspace effects. The ongoing geopolitical dispute within the South China Sea highlights China's resolve to obtain regional superiority. Regarding its counterspace systems within the South China Sea, China has deployed military-grade, truck-mounted jamming equipment in its buildup of military installations on its manmade islands. As of April 2018, U.S. officials confirmed two islands in the Spratly Island chain are equipped with jamming systems for targeting communications and radars.⁴⁰ China will continue to use these systems as a deterrence for any future conflict within the region.

Other Emerging Counterspace Threats

Many other countries, some with small or no space programs, are also developing counterspace capabilities to defend their existing assets or to counter perceived adversary threats in the electromagnetic spectrum. GPS and SATCOM jamming systems are the most prevalent counterspace weapon worldwide. These technologies are becoming easier to access, are more cost effective, and are simpler to operate for non-peer adversarial and lesser-developed countries than the more advanced counterspace weapons/technologies—direct-ascent antisatellite missiles, directed-energy weapons, or on-orbit systems. Nonetheless, some are being developed outside of China and Russia. For example, India became the fourth country to successfully test a direct-ascent antisatellite missile, becoming the only other country to conduct a debris-producing test since China in 2007.⁴¹ Though the satellite that was destroyed was one of its own in low Earth orbit, all spacefaring nations rebuked this test as an unnecessary debris-causing event. In the end, India's strategic messaging goal, probably intended for Beijing, was most likely accomplished—to be seen as a space power. And by actually performing a kinetic test, New Delhi proved it has the means to acquire, track, and engage on-orbit targets. Though India's counterspace capabilities technically pose a threat to United States space systems in low Earth orbit, they are not considered a direct threat.

Two other primary adversaries of the United States, Iran and North Korea, continue to advance their rudimentary counterspace capabilities, primarily with GPS and SATCOM

jamming systems, to affect these critically enabling technologies for United States and allied operations, within their areas of influence.

Iran has publicly recognized the strategic value of space and counterspace capabilities and will likely attempt to disrupt or deny the United States and allied forces' use of space capabilities during a conflict to the extent it is technically able to do so. Tehran also views its space program as a source of national pride, technological and economic development, and military modernization.⁴² Counterspace capabilities such as jamming and spoofing are considered regular tools in Iran's weapons arsenal. There are confirmed, documented cases of Iran using these capabilities against international and regional television broadcasts. In 2010, Iran jammed BBC and Voice of America SATCOM signals transmitting into Iran.⁴³ It has publicly acknowledged that the Iranian government engaged in the jamming of foreign broadcast satellites and claimed the ability to spoof GPS receivers.⁴⁴ Iran has continually demonstrated successful EW attacks against both foreign government and civilian systems; United States and allied forces operating within Iran's regional influence will likely continue to experience these effects. Iran has expanded its development of EW counterspace capabilities, and it will likely further advance those capabilities to target a greater range of SATCOM frequencies used by the United States and allied militaries.

North Korea views denying the United States and its allies the ability to use space during a conflict as a top priority. Similar to Iran, North Korea has employed EW attack capabilities, as well as GPS and SATCOM jamming, against adversaries within the region; however, North Korea keeps its counterspace doctrine and operational concepts largely under wraps.⁴⁵ North Korea continually states that its space capabilities are for peaceful use and development and has spoken to the United Nations about its space program, seeking the acceptance and respect of its space program's right to help the country grow economically.⁴⁶ Despite continued statements that it only uses space for peaceful purposes, North Korea has acquired EW systems and conducted EW attacks against space systems. In 2010, South Korea's Defense Minister stated in a speech to parliament that "North Korea has imported vehicle-mountable devices capable of jamming GPS signals, from Russia." That same year, South Korean forces experienced GPS jamming but were unable to locate the jammers at the time because the jamming lasted only 10 minutes in each instance.⁴⁷ Since 2010, numerous GPS interference events have been attributed to North Korea, which affected both civil and military systems, including aircraft and maritime vessels. North Korea is

improving its EW capabilities, as demonstrated in continued GPS jamming and spoofing operations. U.S. and allied forces within the region are likely to experience these capabilities during combined exercises and border patrols, and possibly other high-interest peninsular events. Accounting for these EW capabilities through the IPB process, for North Korea, Iran, or any other potential adversary, will better position United States Army intelligence professionals to support operational planning and assist in mitigating these effects.

Despite the increasing, worldwide proliferation of counterspace systems, the greatest and most direct threats to United States and allied forces space operations are China and Russia. While both are pursuing, expanding, and fielding these capabilities, each has different employment strategies, doctrines, and end states, but all with the goal of denying U.S. freedom of action in space.

Conclusion

Persistent and reliable satnav/PNT, SATCOM, ISR, and other key space-enabled services have come to be expected and virtually assumed in peacetime and throughout the spectrum of conflict; however, these critical services are threatened globally today and are no longer assured. This reality can be worrisome and could mean the difference between victory and defeat, but too often, it is overlooked or dismissed until it occurs. Our adversaries are placing a premium on both space-enabled operations and counterspace applications, and we, as Army intelligence professionals, must be aware of their potential effects on land-based operations. When most intelligence officers participate in their formation's war games or combined arms rehearsals, the injects are often based on traditional kinetic strikes on a friendly formation or possibly some sort of external force (weather, terrain, or unforeseen civilian interaction) that could halt or alter a formation's movement.

The operational environment has forever changed, and we challenge Army intelligence professionals to now look and think outside the traditional box and present nontraditional injects and analytic processes based on real-world developments and activities. Presume the opposing force will employ GPS and SATCOM jamming during the operation. We must think like, and ahead of, the adversary in order to provide our leadership with greater insight into the



Leadership and staff members from battalions across the 1st Armored Brigade Combat Team, 1st Infantry Division, based out of Fort Riley, KS, participate in a combined arms rehearsal prior to a live fire event during Combined Resolve XII on August 5, 2019.

U.S. Army photo by SGT Jeremiah Woods, 358th Public Affairs Detachment

adversary, the new threat paradigm, and a route toward mission success.

Today's Army intelligence professionals must continue to think critically and holistically about the negative or inhibiting effects that could be seen and experienced in the modern battlespace. In the landscape of military domains, space has emerged as a vital enabler for the spectrum of modern military operations, and we must now, more than ever, be aware of and understand its unique nature and threats. Therefore, it is our responsibility to characterize and advocate for incorporating the reality of these new threats to this newest domain. Ultimately, we must support the commanders, planners, and operators at every level and in every forum with accurate, timely, and actionable intelligence on adversary space and counterspace capabilities and intentions. We must assist their ability to operate in spite of, and through, these new and evolving threats. 🌟

Endnotes

1. Department of the Air Force, *Competing in Space* (Wright-Patterson Air Force Base, OH: National Air and Space Intelligence Center, December 2018), 2.
2. Ibid., 25.
3. Department of the Air Force, Annex 3-14, *Counterspace Operations* (Washington, DC: U.S. Government Publishing Office, 27 August 2018), 9.
4. Department of the Air Force, *Competing in Space*, 4.
5. Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC, January 2019), iii.
6. Ibid.
7. Department of the Air Force, *Competing in Space*, 14.

8. Maxim V. Tarasenko, "Transformation of the Soviet Space Program after the Cold War," *Science & Global Security* 4, no. 3 (1994): 339–361.
9. Asif Siddiqi, "Russia's Space Program Is Struggling Mightily," *Slate*, 21 March 2017.
10. Defense Intelligence Agency, *Challenges to Security*, 24.
11. Ibid., 23.
12. "The Military Doctrine of the Russian Federation," Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland website, December 25, 2014.
13. Defense Intelligence Agency, *Challenges to Security*, 24.
14. "This is the Achilles' Heel of Washington's Military Power," *Sputnik News Online*, 30 January 2016.
15. Defense Intelligence Agency, *Challenges to Security*, 24.
16. Brian Weeden and Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment* (Washington, DC: Secure World Foundation, April 2020), 7.
17. Defense Intelligence Agency, *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC, 2017).
18. Weeden and Samson, *Global Counterspace Capabilities*, 7.
19. "Russia denies role in Israeli airport GPS jamming," *BBC News*, June 27, 2019; Thomas Nilsen, "Norway tired of Russia's electronic warfare troubling civilian navigation: 'Unacceptable and risky,'" *Barents Observer*, January 20, 2019; and "Russia denies disrupting GPS signals during NATO Arctic exercises," *Guardian*, November 12, 2018.
20. Weeden and Samson, *Global Counterspace Capabilities*, 7.
21. Defense Intelligence Agency, *Challenges to Security*, 29.
22. The State Council of the People's Republic Of China, *Full text of white paper on China's space activities in 2016* (Beijing, 28 December 2016), quoted in Defense Intelligence Agency, *Challenges to Security*, 13.
23. Defense Intelligence Agency, *Challenges to Security*, 13.
24. Office of the Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community* (Washington, DC, 13 February 2018).
25. Defense Intelligence Agency, *Challenges to Security*, 13.
26. Ibid., 14.
27. Ibid.
28. Ibid.
29. Ibid.
30. Ibid.
31. Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC, 2 May 2019).
32. U.S.-China Economic and Security Review Commission, *2015 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC, 2015), 297–298.
33. Defense Intelligence Agency, *Challenges to Security*, 20; Lin Jinshun, Feng Tao, Chen Binhui, and Jiang Chunshan, "Study on countermeasure against satellite adaptive null-steering technique," *Aerospace Electronic Warfare* 26, no. 3 (March 2010): 1–4; and H. Wang, "Analysis on Anti-jamming Measures of Mobile User Objective System," *Radio Communications Technology* 35, no. 2 (2009): 46–49.
34. Department of Defense, *Annual Report to Congress*.
35. Ibid., 23.
36. Defense Intelligence Agency, *Challenges to Security*, 20.
37. Department of the Air Force, *Competing in Space*, 19.
38. Weeden and Samson, *Global Counterspace Capabilities*, 6.
39. Ibid.
40. Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, and Makena Young, *Space Threat Assessment 2020* (Washington, DC: Center for Strategic & International Studies, March 30, 2020), 15.
41. Ibid., 44.
42. "DM: Iran to Give Crushing Response to Enemies' Space Threats," *Fars News Agency*, 13 November 2018.
43. Harrison, Johnson, Roberts, and Young, *Space Threat Assessment 2020*, 32.
44. Ibid., 33.
45. Ibid., 37.
46. "Stronger Rules Must Guarantee Outer Space Remains Conflict-Free, First Committee Delegates Stress, Calling for New Laws to Hold Perpetrators Accountable," *United Nations website*, 17 October 2017.
47. "N. Korea's jamming of GPS signals poses new threat: defense minister," *Yonhap News Agency*, October 5, 2010.

CPT Andrew Compean is an intelligence officer for the U.S. Army Space and Missile Defense Command (USASMDC) G-2 Current Intelligence Branch. He has more than 9 years of military intelligence experience, working primarily in support of tactical-level operations. In his current assignment, he focuses his analysis on adversarial space-counterspace intelligence, and he provides intelligence analytical expertise in foreign ballistic and cruise missiles and cyberspace. CPT Compean holds a bachelor of arts in history from Bowling Green State University.

Mr. Daniel Selman is the senior intelligence analyst and foreign space-counterspace subject matter expert for the USASMDC G-2 Current Intelligence Branch. Mr. Selman has 39 years of military intelligence experience. He served 11 years as an active duty U.S. Air Force (USAF) intelligence officer and 13 years as a USAF reserve intelligence officer, retiring with the rank of lieutenant colonel. He has been a U.S. Government civilian on the U.S. Space Command J-2 staff for 11 years as a foreign space-counterspace intelligence analyst, and on the USASMDC G-2 staff for more than 17 years as the G-2's principal space-counterspace intelligence analyst. He has also provided intelligence analytical expertise in foreign ballistic and cruise missiles, cyberspace, intelligence support to force protection, and counterintelligence. Mr. Selman holds a bachelor of science in geology from Southeast Missouri State University and a master's degree in management from Webster University.



Bringing the Army Team to Africa

BY Colonel Bill Bestermann

&

Lieutenant Colonel James A. Crump

Introduction

Our Nation's interests in Africa are as varied as the 53 nations that compose U.S. Africa Command's (AFRICOM's) area of responsibility (AOR). Within that AOR, AFRICOM's focus is on engaging in strategic competition, countering violent extremism, and combatting instability through humanitarian assistance and disaster relief. These challenges take place amidst a competitive landscape that is rapidly evolving both politically and economically. Complex as these challenges are, the benefits of American engagement are equally plentiful as we seek to promote economic development, strengthen partnerships, and challenge our strategic competitors' expansion on the continent in the coming years.

Bringing the Army Team to Africa

As the operational Army headquarters for AFRICOM and subordinate command of U.S. Army Europe and Africa (USAREUR-AF), the U.S. Army Southern European Task Force, Africa (SETAF-AF), has been tasked with—

- ◆ Setting and shaping the theater to gain and maintain operational access, presence, and influence.
- ◆ Maintaining an expeditionary combined joint task force command and control capability ready to execute contingency requirements.
- ◆ Developing land force institutions of African partners to accomplish security cooperation objectives, increasing U.S. influence and access.

SETAF-AF's lines of effort closely align with those of AFRICOM. This common approach, shared understanding, and similar objectives are critical, as SETAF-AF seeks to become the instrument by which AFRICOM can best compete in the land domain in indirect and narrative competition, and should the need arise, in direct competition (armed conflict) against global competitors. Through SETAF-AF's efforts to set the theater and maintain force posture through contingency locations and cooperative security locations on the continent, SETAF-AF ensures that AFRICOM experiences

improved operational conditions in the ever-present potential for crisis and armed conflict in Africa. This effort to gain an advantage is the direct manifestation of SETAF-AF's central role in AFRICOM's approach to indirect competition in Africa.

Following the consolidation of U.S. Army Africa and U.S. Army Europe, SETAF-AF transitioned its Army Service component command tasks to USAREUR-AF. MG Andrew Rohling, Commander of SETAF-AF and Deputy Commanding General for USAREUR-AF, was tasked to make capable a combined joint task force headquarters that could lead limited duration, small-scale contingency operations in Africa or Europe. The key is SETAF-AF's flexible and adaptable force packages, which provide a rapidly deployable command and control architecture for crisis response through the establishment of scalable command posts for small, medium, and large-scale contingencies.

Within the intelligence warfighting function, SETAF-AF remains consistently engaged in the African theater, supporting a full spectrum of military-to-military engagements, building partner capacity, and providing intelligence support to force protection across the continent. In the last 2 years, the 207th Military Intelligence (MI) Brigade supported half of the Secretary of Defense's named operations in Africa, deploying more than 200 collectors, agents, and analysts, which resulted in a 700 percent increase in intelligence reporting. The 207th established Field Office Africa to more efficiently provide intelligence support to chiefs of mission and defense attachés while executing the first U.S. Code Title 10 counterintelligence operations on the continent. The 207th's Africa Data Science Center provides tailored data analytics to support AFRICOM, SETAF-AF, and the wider intelligence community. Headquartered in Vicenza, Italy, the Africa Data Science Center serves as the United States Army Intelligence and Security Command's prototype for an expanded data-driven capability within MI brigades-theater.

SETAF–AF’s annual joint, multinational exercises on the African continent serve to adapt and expand SETAF–AF’s joint task force capability. The goal is to provide combatant commanders with a trained, validated, and rapidly deployable joint task force headquarters capable of conducting operations in Africa and potentially on European soil. These operations would be for small-scale humanitarian assistance/disaster response and noncombatant evacuation. Additionally, SETAF–AF contributes to the execution of AFRICOM’s campaign plan with the employment of land forces in engagements, exercises, and security cooperation with African partner nations.

AFRICOM’s and SETAF–AF’s flagship exercise in Africa is African Lion—the largest annual exercise on the African continent, featuring 3,300 U.S. Service members and a total of approximately 7,800 combined members of the Royal Moroccan Armed Forces, Tunisian Armed Forces, and Senegalese Armed Forces, and military members from Italy, the United Kingdom, and the Netherlands. African Lion is a multinational, multi-domain, large-scale global exercise involving numerous partner countries, executed across the three African host nations: Morocco, Tunisia, and Senegal. Led by SETAF–AF, African Lion is the premier joint force training event for the AFRICOM joint exercise program and is a strategic demonstration of partner commitment, interoperability, and strategic readiness.

The purpose of the exercise is to set the theater for access and interoperability among partner nations against adversarial networks intent on destabilizing the region and threatening freedom of movement and strategic access. African Lion is a Master Scenario Events List–driven, simulation-supported, live, virtual, and constructive exercise in which the training audience faces a near-peer adversary during large-scale combat operations in North Africa, along the North Atlantic Treaty Organization’s (NATO’s) Southern Flank. African Lion is a strategic demonstration of partner commitment to regional stability in North Africa and is an excellent opportunity to conduct realistic, dynamic, and collaborative readiness training in an austere environment at the intersection of four geographic combatant commands, strategic maritime choke points, and global shipping lanes. For the SETAF–AF G-2 and 207th MI Brigade, the exercise represents an opportunity to incorporate African, NATO, and joint partners into intelligence collection planning, analysis, and production. African Lion 21 featured the tactical deployment of the 207th MI Brigade’s deployable intelligence support element onboard Moroccan C-130s from Aviano Airbase, Italy, to Agadir, Morocco.

Building on the successes of African Lion 21, African Lion 22 is set to include more European and African partners

and more Europe-based United States units. It will feature increasingly sophisticated aspects of multi-domain operations, including missile and air defense and cyberspace defense activities. SETAF–AF will continue to coordinate the DEFENDER-Europe and African Lion exercise scenarios based on the tenets of large-scale combat operations methodology.

Building Partner Capacity through the Intelligence Warfighting Function

The SETAF–AF G-2 MI Defense Institution Program is an indispensable tool to foster a capable regional intelligence enterprise of allies and partners. Such programs have proven instrumental in building institutional capacity, and such routine engagements facilitate the development of intelligence partners, enhance partner collection capabilities, and expand SETAF–AF’s intelligence enterprise and influence across the continent. The SETAF–AF G-2 MI Defense Institution Program is the U.S. Code Title 22 funded program to establish and develop professional MI curricula and to facilitate instructors for African partners at partner MI schoolhouses.

The objective of our MI programs is to team with partner nations that have similar security needs and interests, have a will and desire to partner with us, and have the near- and long-term potential to export regional security. Our success in meeting our objectives is readily demonstrated in multiple African partner countries where these programs have been successful at helping partners build improved MI schoolhouses and intelligence capabilities. Our key partners in meeting this objective are the AFRICOM J-2, 2nd Security Force Assistance Brigade (SFAB), 207th MI Brigade, U.S. Army Intelligence Center of Excellence (USAICoE), Human Intelligence Training-Joint Center of Excellence, Army National Guard State Partners, Defense Intelligence Agency, National Geospatial-Intelligence Agency, State Department, country teams, and National Security Agency. They all provide valuable capabilities and training opportunities to enhance what SETAF–AF, SFAB, and 207th MI Brigade are able to provide.

For example, in Ghana, the SETAF–AF G-2 MI Defense Institution Program focuses on Ghanaian MI Corps cadre training and professionalization for Ghanaian Forces at the MI school. The SETAF–AF G-2 is currently developing a secondary program to establish an Intelligence Fusion Center by providing needed materials, equipment, and instructional guidance for the implementation of equipment and software training within a 3-year period. We hope to integrate SFAB capabilities to enhance our ability to deliver quality intelligence partnership over the next several fiscal years.

In Kenya, SETAF–AF assists the Kenyan Directorate of Military Intelligence to refine curriculum and training programs at the MI Defense Intelligence Academy in order to better prepare the Kenyan Defense Forces’ (KDF) officers and soldiers to contend with regional terrorism concerns and develop an enhanced MI capability within the KDF. SETAF–AF support includes assisting the KDF in intelligence collection, sharing, and processing, exploitation, and dissemination capabilities. USAICoE has been instrumental in supporting our relationship building in Kenya. From 2019 to the present, the SETAF–AF G-2, USAICoE, and 207th MI Brigade have jointly conducted a total of 18 weeks of training and mentoring for more than 40 KDF Army officers, warrant officers, and senior noncommissioned officers. Common core concepts included language and tactics and techniques to improve intelligence support to stability operations through multiple intelligence disciplines. The students represented a cross section of the KDF intelligence enterprise, from all the services, from the strategic to the operational and tactical levels. Students and senior KDF officials said the skills and knowledge they gained had an immediate impact on the enterprise in the field, enabling intelligence-driven operations in Somalia. Senior KDF MI officers requested further training to enhance doctrine development at the Defence Intelligence Academy and to further streamline intelligence fusion at the operational level to better drive tactical operations.

intelligence support to Tunisian military doctrine, training exercises, and operations.

The Nigerian Army Intelligence and Cyberwarfare School Curriculum Development Program is a multiyear, joint endeavor to develop a common professional military education standard for all Nigerian MI professionals through a facility and staff development program. The California National Guard has been pivotal to our efforts in Nigeria to sustain and improve our intelligence partnership. The SETAF–AF G-2 coordinated with the California National Guard to help modernize the Nigerian Army Intelligence School curriculum. The California National Guard supported four train-the-trainer events, advising and instructing the Nigerian school faculty and cadre. The SETAF–AF G-2 assisted in building a 7-week resident course covering tactical intelligence for officers and enlisted personnel. The SETAF–AF G-2 also assisted in building a 14-week resident course equivalent to USAICoE’s MI Basic Officer Leader Course.

Finally yet importantly, in Burkina Faso, SETAF–AF provides the Burkinabe Military Intelligence Directorate with basic and advanced intelligence training for officers and noncommissioned officers to set the conditions for the eventual establishment of an MI school. This training is critical to assisting partners in an area under heightened pressure from violent extremists.

Leveraging the SFAB in Competition

SFAB operations in Africa are at the cutting edge of both narrative and indirect competition on the continent through military-to-military training events designed to improve the reputation of the United States, increase leverage, or expand influence. Recently, the 2nd SFAB began its latest rotational employment of advisors to SETAF–AF’s headquarters in Vicenza, Italy, in order to enable the assistance of mission command and provide situational awareness of advisor teams in the AFRICOM AOR. Typically, SFAB intelligence support teams include the force package intelligence noncommissioned officer, who serves as the liaison between the SETAF–AF G-2 and advisor teams deployed to their respective assigned countries in Africa. The intelligence section at the SFAB battalion and brigade proved critical to the execution of the SETAF–AF G-2’s priority of providing intelligence support to force protection across Africa. This liaison helped to convey a better understanding of the capabilities of the SFAB teams. The close association of the SFAB’s intelligence architecture within that of the SETAF–AF G-2 enterprise enables intelligence planners to incorporate the SFAB teams into long-term military-to-military engagement planning, defense institution building, and future advising missions in Africa. The SFAB’s knowledge of the atmospheric and working relationships with partners on the ground render SETAF–AF better prepared to set the theater.



U.S. Army photo by Rebecca Farmer

A Cameroonian intelligence officer refines her group’s modified combined obstacle overlay, which is a visual depiction of terrain and key features, part of their intelligence preparation of the operational environment at the Regional All-Female Basic Intelligence Course, Tunis, Tunisia.

SETAF–AF, in cooperation with the 2nd SFAB, is providing training at the Intelligence Security Agency for defense school instructors to assist Tunisia in developing its MI capabilities in order to enable successful integration of Tunisian

With the assistance of the 207th MI Brigade and SETAF–AF theater analysis and control element in Wiesbaden, Germany, the SETAF–AF G-2 provides analytical intelligence support in the form of operational and tactical intelligence products to SFAB intelligence advisors on the ground in locations such as Tunisia, Senegal, Ghana, and Kenya. Advisors continue to work through the Office of Security Cooperation and the Ministry of Defense to better integrate and sustain collection efforts across the country. Because of the lack of adequate, forward-deployed resources and analytical systems at the intelligence advisor’s disposal, this reachback support has proven critical to the SFAB’s mission success in the intelligence warfighting function. This mutually beneficial, symbiotic relationship enables the SETAF–AF G-2 section to gain a better operational perspective of the missions in which the 2nd SFAB is involved, increase the situational awareness of the advisor teams on the ground, and extend the operational reach of the SETAF–AF intelligence enterprise.


In a relatively short period, SFABs have proven their worth repeatedly on the African continent and will become increasingly capable over time with consistent planning and allocation. As SETAF–AF continues to transform security force assistance to maximize efficiency and effectiveness, certain security force assistance responsibilities previously executed only by SETAF–AF can and should transition to the SFAB, being careful to ensure that those responsibilities do not exceed the capabilities or the intended role of the SFAB as it was designed.

Maintaining SETAF–AF’s ability to execute a robust engagement strategy, including maximum incorporation of the SFAB’s capabilities, is critical to keep an adequate level of diplomacy across Africa and to counter growing Chinese and Russian influence on the continent. Thus, in a region with ever-lower confidence in governance and institutions, the American flag increasingly represents a set of ideals

to which our partners can aspire. In narrative competition, SETAF–AF’s engagement strategy, along with its SFAB partners, serves to generate, expand, and improve upon the reputation of AFRICOM, the U.S. Army, and the United States as the security partner of choice among developing nations in Africa.

The Way Ahead

AFRICOM’s responsibilities in Africa center on expanding U.S. access and influence, countering violent extremists, strengthening relationships with security partners on the continent, and responding effectively to crisis. SETAF–AF, as a deployable, joint-capable headquarters, is a tailor-made organization purpose-built for crisis response in Africa or in Europe under certain conditions. The tools the United States will leverage must be as flexible and adaptable as is necessary to meet challenges regardless of scope and scale. SETAF–AF is fully capable of commanding and controlling small-scale, short-duration contingency operations anywhere in Africa or Europe. Through SETAF–AF’s persistent engagement on the continent, our African partners will view the U.S. Army as a reliable partner; and SETAF–AF’s actions support the efforts of AFRICOM and USAREUR–AF, enabling competition and enhancing regional security and stability. SETAF–AF advances U.S. influence, access, and partnerships, enabling the campaign and competition objectives of AFRICOM and USAREUR–AF in the AFRICOM AOR.

Through flexibility and adaptability, SETAF–AF will continue to serve as a tool by which AFRICOM advances U.S. influence, access, and partnerships across an increasingly critical theater of operations. By providing a trained, validated, and rapidly deployable joint task force headquarters capable of conducting small-scale humanitarian assistance, crisis response, and noncombatant evacuation operations, **SETAF–AF will remain the headquarters that brings the Army team to Africa.** 

COL Bill Bestermann is the Assistant Chief of Staff, G-2, for Southern European Task Force, Africa, stationed in Vicenza, Italy. His previous assignments include Director/Multi-Service Commander, U.S. Africa Command J-2 Molesworth, and Director, Plans, Targets, and Operations (J-235) for Headquarters, Resolute Support. He holds a bachelor of science from the U.S. Military Academy, a master of science in management from Troy State University, a master of science in strategic intelligence from the National Intelligence University, and a master of arts in national security and strategic studies from the Naval War College.

LTC James Crump is the Chief of the Intelligence Operations Division for the Southern European Task Force, Africa, stationed in Vicenza, Italy. His previous assignments include the Maneuver Center of Excellence, Fort Benning, GA, and Chief, Joint Intelligence Support Element, Operation Inherent Resolve. He holds a master’s degree in international relations from The Bush School of Government, Texas A&M University, and a master’s degree in strategic intelligence from the National Intelligence University.



An African student fires an M240 machine gun from a Special Operations Craft–Riverine boat as part of the Lake Chad Basin Initiative, November 15, 2017, at the Naval Small Craft Instruction and Technical Training School at Stennis Space Center, MI. The objective of the iteration is to increase partner nations' abilities to project force against violent extremist organization safe havens within the Lake Chad region. (Photo courtesy of Department of Defense Michael Bottoms; Graphic by Jonathan S. Dinger, MIPB)

Throughout history, we see nations with allies thrive, and nations without allies wither.

—Gen. James Mattis (Retired) Former U.S. Secretary of Defense

Introduction

Prosporous nations do not operate in a vacuum, and they cannot operate effectively in an environment foreign to them without the cooperation of allies.

In a 2019 interview, former Secretary of Defense James Mattis emphatically highlighted the importance of maintaining alliances with other nations. He emphasized our allied partners' contributions and support not only in military operations but also in the pursuit of national security goals worldwide.¹ An example of this is in Africa, where several nations, including those in the Lake Chad Basin region, have formed alliances to combat the violent activities of Boko Haram militants. To be effective, these alliances must include intelligence sharing among the partner nations; however, in some cases, the sharing has proved to be more difficult than expected, contributing to a lack of coordination when conducting offensive operations.

Who Are Boko Haram?

Boko Haram is a terrorist group operating primarily in the Muslim majority of northern Nigeria, but in 2014, Boko Haram's reign of terror spread throughout the countries surrounding the Lake Chad Basin—Chad, Cameroon, and

Niger. Boko Haram, which roughly translates to *Western education is forbidden*, has been conducting a de facto war with the government of Nigeria since 2009.² In the spring of 2014, Boko Haram militants kidnapped more than 200 schoolgirls in northeastern Nigeria. The kidnapping of the girls in a secondary school was not only symbolic in nature but also demonstrated the great lengths Boko Haram would pursue to prove a point. The Nigerian Army claimed an aggressive approach to search the Sambisa Forest in northeast Nigeria where the kidnapped girls were taken.³ A video circulated immediately after the kidnappings, indicating the group's opposition to Western education and, specifically, its opposition to girls receiving an education. Boko Haram advocated the strictest interpretation of their version of Sharia law but also called for the return of the Sokoto Caliphate.

From 1804 to 1830, tribal dynasties fought among themselves to form the Sokoto Caliphate.⁴ The caliphate encompassed most of current day northeast Nigeria and Lake Chad and lasted until colonial forces conquered the area in 1903, dividing it among the British, French, and German powers. Individual jihadist movements in the region were not synchronized but overwhelmed most of the area in an effort to Islamize the population.⁵ In a similar fashion, random acts of violence in the Lake Chad Basin increased exponentially in 2015, and other countries started to experience Boko Haram firsthand with greater

frequency. Although the majority of the violence centered on northeast Nigeria, most of the skirmishes and battles spilled into the border towns of Chad, Cameroon, and Niger. Daily armed conflicts in all the border areas resulted in more than 30,000 deaths and 10 times that number in displaced persons. Boko Haram was not even a blip on the U.S. Government's radar at the time.

Multinational Cooperation

In 2014 and 2015, the Integrated Country Strategy, formulated by the U.S. Embassy in N'Djamena, Chad, did not mention Boko Haram specifically. The Integrated Country Strategy is the foreign policy framework led by a U.S. ambassador but developed in a collaborative effort through the in-country interagency process.⁶ The Department of Defense's representative in this interagency process is the defense attaché office at the U.S. Embassy, led by the senior defense official, typically the defense attaché. The senior staff at the U.S. Embassy in Chad were well aware of the incipient threat from Boko Haram, but the staff's focus was on building partner capacity in military capabilities, humanitarian assistance, and development projects. The embassy's efforts were on supporting the Chadian contribution to the United Nations Multidimensional Integrated Stabilization Mission in Mali and the mass refugee exodus from the Central African Republic into Chadian territory at the height of the Central African Republic Civil War.

The kidnapping of the schoolgirls gained worldwide publicity, and collaboration efforts led to France, the United Kingdom, and the United States establishing an ad hoc coalition, known as the P3. Additionally, the French had started Operation Barkhane in 2014, an expeditionary operation aimed at conducting counterterrorism missions in the Sahel region. It was not a new operation; Barkhane was a reorganization of Operation Serval, which the French had formed at the request of the Mali government in 2013 to oust Islamic militants from the north of Mali. Under the command structure of Operation Barkhane, the French military's premier planning organization, known as the CPCO,

created a coordination and liaison cell, the CCL.⁷ With 3,000 French military forces and associated weapons systems, the French were adequately postured to support any counter-Boko Haram efforts. The CPCO invited the P3 partners to provide advisors. Subsequently, the CPCO asked the military

leaders from Cameroon, Niger, Chad, and Nigeria to contribute to the CCL. The CCL's charter was to share intelligence related to Boko Haram among the partner nations. The P3 partners would facilitate the use of organic intelligence, surveillance, and reconnaissance (ISR) elements to share among the CCL partners.

In May 2014, former President Barack Obama notified the United States Congress of the deployment of United States ISR assets to

Chad to support missions over Northern Nigeria and the Lake Chad Basin.⁸ Before U.S. intelligence can be shared with partner nations, a system needs to be in place to facilitate access as outlined by Department of Defense Instruction 5530.03, *International Agreements*. The process begins with the establishment of an international agreement and/or a memorandum of agreement or understanding. In this case, an international agreement must outline the conditions for sharing with foreign partner nations and the U.S. Government.⁹ First, initial negotiations must determine whether an agreement to share intelligence is in the best interest of the U.S. Government. Then, once the need is clearly articulated, the groundwork starts at the U.S. Embassy to discuss the international agreement with the host country's Ministry of Foreign Affairs.

France had been providing logistics and intelligence directly to Niger and Chad before CCL's formation.¹⁰ Intergovernmental discussions with the P3 slowly transformed into a more tangible contribution. The French divested control of the CCL, and it is now a rotational command among the P3 partners.¹¹ The French focus remains on battling Al Qaeda in the Islamic Maghreb (AQIM) instead of Boko Haram. AQIM, with its support structure of arms traffickers and the coopting of local tribes, disrupts governance among the G5 Sahel partners (Mauritania,



A California National Guard Special Forces Soldier from Los Alamitos-based Special Operations Detachment-U.S. Northern Command and Company A, 5th Battalion, 19th Special Forces Group (Airborne), reviews a sand table map with a Nigerian soldier in Nigeria, June 2014. The training is to help the Nigerian Army counter Boko Haram. (U.S. Army photo by CPL Danielle Rodrigues)

Mali, Burkina Faso, Niger, and Chad), an intergovernmental cooperation framework that seeks to fight insecurity and support development with a view to opening up the region. Although France has invested heavily in the G5 Sahel, it considers Boko Haram a localized threat, and the implied task of sharing intelligence has proved to be more difficult than expected.

Currently, Chad and Niger have organic ISR assets to support their counter-Boko Haram efforts; however, establishing a reliable network of sources in the Lake Chad Basin is problematic. Oftentimes, people living along the lake are fearful of reporting Boko Haram activity because they might endanger family members or close friends who may have joined the cause for economic reasons. In Cameroon, some people believe that high-level political leaders have supported Boko Haram. Cameroon security forces arrested a former member of parliament in December 2020 for supplying goods and cattle to known Boko Haram operatives.¹² While this scenario highlighted a success in obtaining actionable intelligence, sharing with partner nations is not second nature. Each country operates well independently, but sharing intelligence is not a priority at this time. The lack of intelligence sharing may be attributed to each country in the Lake Chad Basin focusing on its own national interests and internal conflicts. Additionally, during the CCL's early stages, it was a daily struggle to get the partners to share because each partner nation had a different procedure for the disclosure of intelligence.

One of the most gratifying features of recent work in intelligence, and one that is quite unique in its long history, has been the growing cooperation established between the American intelligence services and their counterparts throughout the Free World which make common cause with us as we face the common peril.¹³

**—Allen Dulles, former Director
of the Central Intelligence Agency**

The Multinational Joint Task Force

The Nigerian government, which has been dealing with Boko Haram since the early 2000s, decided to form the Multinational Joint Task Force (MNJTF) in Baga, Nigeria.¹⁴ In its infancy, the force consisted mostly of Nigerians with perfunctory contributions from Chad and Niger. The Boko Haram attacks increased in frequency and intensity, and the

MNJTF had to relocate in 2015 when the Baga headquarters was destroyed.¹⁵ It relocated to N'Djamena, Chad, after a series of meetings with Africa Union representatives and contributing forces from Chad, Nigeria, Niger, and Cameroon. Benin also contributed forces but not in a combat capacity.¹⁶ The political and military frameworks formed after contentious discussions but still lacked a more comprehensive intelligence cell. As with normal multinational operations, the MNJTF needed each partner nation to share intelligence with others and to coordinate receiving intelligence from their respective forces.¹⁷

At the beginning, the relocation and reorganization of the MNJTF from Nigeria to Chad was problematic. Although these countries are neighbors, they inherently distrust each other; however, after an intervention by the Africa Union and the P3, partnerships soon developed and refocused their threat perspectives toward a common enemy.¹⁸ With the political framework solidified, the military reallocation needed to take effect. The MNJTF reorganized into four sectors, keeping national borders intact.¹⁹ Each country took command of its sector, not only with parochial interests at heart but with those of the MNJTF as well. Since the situation affected the Nigerian population the most, and the Nigerian Army had the most resources, it was decided unanimously that the Nigerians should take command of the MNJTF.

The MNJTF enhanced intelligence sharing by offering the partners a forum to generate greater dialogue, resulting in a more collaborative effort on the ground.²⁰ P3 advisors were dispatched and embedded themselves with the MNJTF. The contributions of France and the United Kingdom were substantial. France facilitated logistics nodes for the MNJTF, and the United Kingdom helped with episodic ISR contribution. The United States focused its contribution on countering violent extremism by increasing military-to-military engagements and training exercises through funding channels within the Department of Defense and the Department of State.²¹ With the involvement of U.S. Africa Command's Office of Security Cooperation, military engagements doubled in size from 2013 to 2017. Various forms of security force assistance programs were introduced, assuring expanding partner capacity. Although it is a multinational effort, Chadian military forces and their special operations forces (the Special Antiterrorism Group) have conducted most of the military campaigns since 2015.

The Special Antiterrorism Group's commanding general, Brigadier General Abdelrahman Youssouf Mery, expressed his view on the Nigerian contribution and resolve by saying, "Nigeria needs to commit and be ready to engage."²² A

long-held view is that Nigerian forces lacked the ferocity and violence of action required to take key terrain. More often than not, Nigerian forces would overwhelmingly take a town from Boko Haram but would rarely place stay-behind forces to repel counterattacks. Consequently, Boko Haram insurgents would return to the town after Nigerian forces had left. Although a smaller force compared to the Nigerian force, Chad's armed forces were more deliberate with their military campaigns, and their resolve influenced Niger, which dispatched 2,000 troops to fight along the Nigerian border.²³

The lack of intelligence sharing among the partner nations still contributes to the lack of coordination when conducting offensive operations, as battle tracking and taskings lie solely with each nation's organic command and control entities. The francophone countries readily contribute, but at times, they neglect to share with the Nigerian military.

Conclusion

In this current geopolitical landscape, intelligence continues to be the driving force in enabling military operations. Challenges in the operational environment will remain constant, increasing in intensity as power vacuums expand or develop. Alliances and partner nations are needed to obtain a situational understanding of any conflict. Joint, allied, and combined operations present challenges as each nation looks after its own interests as part of the overall mission set. Therefore, the formation of multinational partnerships that include cooperative intelligence sharing cells is one of the first steps in obtaining a clearer picture. The mere presence and establishment of these cells show the world a coordinated effort to quell conflicts. The formation of multinational intelligence cells are necessary to obtain actionable intelligence in support of coalition operations. ✨

Intelligence deals with all the things which should be known in advance of initiating a course of action.²⁴

—Second Hoover Commission Report on Intelligence Activities, 1955

The Death of Idriss Déby Itno, President of Chad
20 April 2021

Single-handedly, no country can overcome this threat [Boko Haram] and therefore pooling our resources together...we are going to overcome this challenge.²⁸

—Idriss Déby Itno

Long-time Chadian President Idriss Déby Itno died when visiting Chadian troops fighting in the frontlines on 20 April 2021. Chadian forces were repelling an attack from a rebel group called Front for Change and Concord in Chad. Déby had just received 79 percent of the votes in his unprecedented and controversial sixth term in office a couple of days before his death. A transitional military council led by Déby's son, Lieutenant General Mahamat Idriss Déby Itno, will govern the country for 18 months, with the promise of holding "free and democratic" elections once the transition period is over. The former Chadian president ruled for 30 years and was a long-time ally of France and other Western nations in the fight against jihadist groups in the Sahel region of Africa. The future security of the Sahel is now more precarious during this transition.²⁹

Epigraph

James Mattis, "Jim Mattis: 'Nations With Allies Thrive, Nations Without Allies Wither,'" interview by Greg Myre and Steve Inskeep, *Morning Edition*, NPR, September 2, 2019, <https://www.npr.org/2019/09/02/756681750/jim-mattis-nations-with-allies-thrive-nations-without-allies-wither>.

Endnotes

1. James Mattis, "Nations With Allies Thrive."

2. Fidelis Mbah, "Nigeria's Chibok schoolgirls: Five years on, 112 still missing," Al Jazeera, 14 April 2019, <https://www.aljazeera.com/news/2019/04/nigeria-chibok-school-girls-years-112-missing-190413192517739.html>.

3. Michael M. Phillips and Drew Hinshaw, "Chad's Army Helps Turn Tide Against Boko Haram," *Wall Street Journal*, February 24, 2015, <https://www.wsj.com/articles/chads-army-helps-turn-tide-against-boko-haram-1424823134>.


4. Roland Oliver and Michael Crowder, eds., *The Cambridge Encyclopedia of Africa* (London: Cambridge University Press, 1981).


5. Ibid.
6. U.S. Department of State, *Integrated Country Strategy–Chad* (2020), 3, <https://www.state.gov/integrated-country-strategies/>.
7. The CPCO is the Centre de Planification et de Conduite des Opérations, the French military planning cell for operations attached to the Etat Major des Armées (EMA), or general staff. The CCL is the cellule de coordination et de liaison, a combined French, British, and U.S. organization that coordinates international support in an attempt to ensure support is complementary and effective.
8. Cheryl Pellerin, “DOD Sends UAV, 80 Airmen to Help Nigerian search,” U.S. Air Force website, May 22, 2014, <https://www.af.mil/News/Article-Display/Article/485009/dod-sends-uav-80-airmen-to-help-nigerian-search/source/GovD/>.
9. Department of Defense (DoD), DoD Instruction 5530.03, *International Agreements* (Washington, DC, December 4, 2019).
10. Phillips and Hinshaw, “Chad’s Army.”
11. Christopher Hurlburt, U.S. Africa Command (AFRICOM) J-5, email to author, August 14, 2020.
12. Moki Edwin Kindzeka, “Cameroon Says Boko Haram Infiltrates Top Business and Political Leaders,” Voice of America, December 19, 2020, <https://www.voanews.com/africa/cameroon-says-boko-haram-infiltrates-top-business-and-political-leaders>.
13. Allen W. Dulles, *The Craft of Intelligence* (New York, NY: Harper & Row, 1963).
14. “About the Force,” Multinational Joint Task Force website, accessed 13 August 2021, <https://www.mnjtffmm.org>.
15. Ibid.
16. Ibid.
17. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 5 July 2017).
18. Ibid.
19. “Sectors,” Multinational Joint Task Force website.
20. Hurlburt, AFRICOM J-5, email.
21. U.S. Department of State, *Integrated Country Strategy–Chad*.
22. Phillips and Hinshaw, “Chad’s Army.”
23. Ibid.
24. The Hoover Commission Task Force, *Report by the Task Force on Intelligence Activities of the Commission on Organization of the Executive Branch of the Government* (1955), quoted in Dulles, *Craft of Intelligence*.
25. Phillips and Hinshaw, “Chad’s Army.”
26. Ibid.
27. Oliver and Crowder, *Cambridge Encyclopedia of Africa*.
28. “Central, West African leaders to meet over Boko Haram in April,” Reuters, March 18, 2015, <https://www.reuters.com/article/us-nigeria-boko-haram-summit-idUSKBNOME2V120150318>.
29. “Chad’s President Idriss Déby dies in clashes with rebels,” BBC, April 20, 2021, <https://www.bbc.co.uk/news/world-africa-56815708>.

CW4 Mark Benitez is an instructor and course developer at the military intelligence (MI) warrant officer training branch, 304th MI Battalion, 111th MI Brigade, Fort Huachuca, AZ. Mr. Benitez is a tenured member of the Defense Attaché Service, and he has served at U.S. embassies in locations around the world. His military education includes Security Cooperation Program Manager, J2X Operations Course, Defense Strategic Debriefing Course, Joint Military Attaché School—Staff Course, and other required professional military education.



Military Intelligence Soldier Heritage Learning Center






The Army Intelligence Museum acts as custodian and repository for artifacts significant to the history of intelligence organizations, operations, and individuals and provides military history education. The museum highlights the role of Military Intelligence within the U.S. Army from 1775 to the present day and honors the achievements of Soldiers acting in intelligence roles. Museum exhibits include a World War II German Enigma cipher machine, a large fragment of the Berlin Wall, a vehicle operated by the U.S. Army Military Liaison Mission during the Cold War, and signals intelligence gear used by the Army Security Agency. The museum also displays manned and unmanned intelligence aircraft at the outdoor Air Park on Hatfield Street.

Check out the MI Soldier Heritage Learning Center website at:
https://history.army.mil/museums/TRADOC/fortHuachuca_MI



Introduction

The coronavirus disease 2019 (COVID-19) changed the way we, at U.S. Army Central (USARCENT), engaged with our partners and redefined our engagement strategy. For over a year, we ceased all face-to-face partner activities in the Middle East, and by March 2020, the global COVID-19 pandemic had significantly degraded our partnership activities in support of the U.S. Central Command (USCENTCOM) Theater Campaign Plan. Specifically, we were unable to sustain regional partnerships in the Middle East because of travel restrictions and our partners' need to focus on their national pandemic response. The result was the loss of placement and access required to facilitate the U.S. defense posture and enable USARCENT's freedom of movement and action in the region. The risk of losing years of progress toward building rapport, trust, and mutual benefit was staring down on us.

Searching for a Solution

In order to mitigate further degradation in partner relationships, we desperately searched for answers to important questions: How does one safely conduct a global conference spanning eight time zones? What system and technology are common across a dozen foreign partner organizations? How do we get partners excited about a multilateral intelligence discussion? In order to find a solution, we decided to take a chance and leverage technology born from the pandemic. By late fall of 2020, the USARCENT G-2 augmented its engagement strategy with virtual enhancements, including the creation of the Virtual Land Forces Intelligence Conference, using Microsoft Teams.

We were uncertain how our partners would react. To our surprise, we learned they were excited and exuberant about

virtual engagements and conferences. "The Intelligence Conference was a great opportunity to share information and stay connected. We at [Ministry of National Guard] MNG look forward to continuing this relationship and look forward to upcoming conferences," said Saudi Arabian Brigadier General Majed Al Osaimi, incoming deputy intelligence director of the Saudi Arabian Ministry of National Guard.¹ Not only did they respond positively, but our last two conferences also led to more feedback and contributions to our intelligence partnerships than ever before. During a Senate Armed Services Committee posture statement in April 2021, GEN Kenneth F. McKenzie Jr., Commander, USCENTCOM, said, "While many events were cancelled due to COVID-19, partners remain committed."² The USARCENT G-2 remains committed to our intelligence partners and used these virtual events as proof.

Key strategic documents codify the importance of maintaining essential partnerships in order to secure U.S. national interests abroad. In March 2021, the White House released the Interim National Security Strategic Guidance, identifying *partnerships* as a priority for the U.S. Government.³ The National Defense Strategy identifies "enduring coalitions and long-term security partnerships, underpinned by our bedrock alliances and reinforced by our allies' own webs of security relationships" as a line of effort.⁴ Before the 2021 transition of the U.S. Administration, the Secretary of the Army and the Chief of Staff of the Army signed the inaugural *Army Strategy for Allies and Partners*, making allies and partners within the Service a priority.⁵ The Army's senior intelligence officer published her four priority lines of effort, one of which is the commitment to strengthen our relationship with allies and partners. In his April 2021

posture statement before the Senate Armed Services Committee, GEN McKenzie affirmed his commitment to allies and alignment to the new Interim National Security Strategic Guidance.⁶ USARCENT's direction on partnership is no different. In support of USCENCOM, USARCENT's partnership program in the Middle East is based on a tiered system focused on access, basing, and overflight. To execute this guidance, we developed the Theater Intelligence Engagement Strategy (TIES).

Senior Leader Engagements (SLE) –

The USARCENT G-2, intelligence, SLEs focus on CG-directed contact with our priority access-focused partners. The frequency is based on direct guidance from the USCENCOM and USARCENT CGs. The level of engagements is based on each individual country's intelligence organization, but ideally the primary partner is the land domain G-2. In the past, SLEs have been conducted up echelon and down echelon based on the need to sustain or improve access.

Military Engagement –

Military engagement in the USARCENT focus area is the most visible and requested aspect of the support from our regional land domain partnerships. This pillar of the TIES focuses on intelligence doctrinal and tactics development. This supports the growth of intelligence organizations within our regional partner formations. The USARCENT G-2 TIES includes the Army's ASAP tools, personnel exchanges, and PME as a component of military engagement.

Interoperability –

The interoperability pillar focuses on developing common training goals to communicate and execute the intelligence warfighting function bilaterally. Partner system architecture within the region is relatively immature based on relatively new intelligence organizations at all levels from tactical to strategic. This pillar includes Army ASAP tools, advise and assist; armaments cooperation, and exercises; and collective training.

Intelligence Sharing –

The final pillar of the USARCENT G-2 TIES is intelligence sharing. While there are unique agreements in place that allow USARCENT to share through delegated authorities, USARCENT G-2 primarily shares finished intelligence. This sharing is mainly a means to create a common understanding of similar threats.



Theater Intelligence Engagement Strategy Pillars

Creating the Necessary TIES

In 2018, the USARCENT G-2 created an intelligence engagement strategy to apply USCENCOM's and USARCENT's theater security cooperation guidance to partnerships within the region. In 2019, we focused this strategy on four pillars:

- ◆ Senior leader engagements.
- ◆ Military engagement.
- ◆ Interoperability.
- ◆ Intelligence sharing.

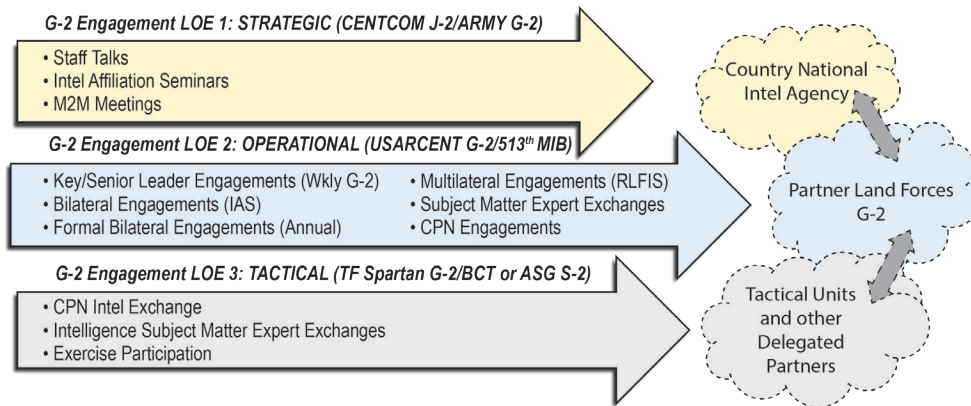
These pillars are in line with current security cooperation tools identified in the *Army Strategy for Allies and Partners*.⁷ The first pillar, senior leader engagements, emphasizes ensuring predictable, relationship-focused engagements between the USARCENT G-2 and the land forces equivalent senior intelligence representative. Next, our military engagement pillar encompasses activities that build Army-to-Army relationships and facilitate increased understanding of organization, tactics, and doctrine. Third, the interoperability pillar harnesses technology and relationships to execute the intelligence warfighting function at the speed of war with our partners. Finally, the intelligence sharing pillar enables the sharing of finished releasable intelligence under the guidance and authority of the country embassy teams and USCENCOM J-2.

During the development of the partnership strategy, we identified factors that affected its execution: physical distance from our headquarters to our partners', our regional partners' military intelligence force capacity, and USCENCOM and USARCENT command guidance on gaining and maintaining access in the region. First, the physical distance of USARCENT, headquartered at Shaw Air Force Base, South Carolina, was addressed by the delegation of

intelligence partnership activities to forward down-trace units. We managed this delegation of the engagement authority from the USARCENT G-2 staff and validated it during our weekly theater intelligence battle rhythm events. Additionally, the TIES program documented the alignment of the appropriate echelon of U.S. Army intelligence organizations with the relevant partner land domain organizations. The second factor affecting the USARCENT G-2 strategy was our partners' intelligence capacity. Through our experience, we realized that the U.S. Army's intelligence footprint could overwhelm a partner's capacity quickly and unintentionally. Finally, the need to gain and maintain access in support of the commander's guidance was the most important influence on the TIES. The commander's guidance directed the use of relationships between partners to enable the broader theater partnership plan. The critical task was to deconflict engagements with other theater Service components and the USCENCOM J-2. This was executed by "echeloning" the engagements into tactical, operational, and strategic levels, while identifying specific activities and partners for each echelon. We created an intelligence engagement program that—

- ◆ Gave partners routine and predictable access to the USARCENT intelligence enterprise.
- ◆ Gained familiarity with intelligence exchanges to include receiving finished U.S. intelligence.
- ◆ Advanced federated/distributed intelligence through partners at the speed of war.

Overall, this strategy served us well in the region with land domain intelligence partners, before the pandemic, leading into early 2020.



USARCENT G-2 Engagement Lines of Effort

The Pandemic

The pandemic had a universal degradation on USARCENT partners; however, the pandemic did not degrade regional threats to U.S. and partner interest in the Middle East. To compound the problems, regional governments had to respond to their internal demands on resources and the reallocation of military intelligence personnel to respond to the pandemic. The impacts on the defense forces, and specifically on the intelligence professionals across the Middle East, highlighted common themes within our region. Themes included the degradation of intelligence partnership activities, decreased access to networks and connectivity challenges, and the balancing of internal security and pandemic response requirements against maintaining a common intelligence picture of the regional threats. We quickly worked on solutions to adjust the TIES program to meet these pandemic-driven challenges.

At the onset of the pandemic, we decided to reassess our own TIES program. The most direct impact on the program was the degradation of partnerships from cancelling in-person partner engagement activities. Before the pandemic, regional partners preferred in-person bilateral and multilateral events to manage the intelligence capacity. Once the pandemic restrictions were in place, we cancelled all planned in-person events because of the constraints that government policies imposed, limiting travel. Our answer to the degradation of engagements was a virtual connection with partners using existing unclassified and classified network tools to augment in-person events when regional restrictions allowed. While we identified virtual engagements early on as an answer to the problem, a network tool that our regional partners could use was not as clear.

A number of network connectivity challenges were identified when transitioning to a virtual program during the pandemic. While the USARCENT G-2 TIES accounted for virtual connectivity options, it did not initially account for other challenges identified during the pandemic:

◆ **Unclassified domain.**

The intelligence warfighting function is rarely executed over unclassified commercial applications; however, during the initial stages of the pandemic, the unclassified domain was the only way to communicate with partners in some cases.

◆ **Network tool standardization.** Unclassified network tools such as Microsoft

Teams were not standardized nor had they been tested with partners before the pandemic.

◆ **Language barriers.** The user-interface language of the unclassified network tools was a problem, although we benefited from our intelligence partners having a fairly good command of the English language.

◆ **Security.** Partner national security structures severely limited the use of network tools. Our partners' host nations restrict the use of unclassified network tools such as Microsoft Teams.

Virtual events benefited most partnered nations whose intelligence forces were challenged both to meet their national pandemic response and to provide intelligence to their own land forces during times of uncertainty and attack escalation. Experiences during the first virtual multilateral event and a series of virtual subject matter expert exchanges demonstrated that partners sometimes preferred the virtual options for three reasons:

◆ **Balance.** Partners were able to manage their intelligence engagement time against the needs of their national response to the pandemic.

◆ **Attendance.** The ease of attendance allowed for larger audiences, and very little funding and travel were required. The only limitations were room restrictions during the pandemic.

◆ **Senior engagement.** In addition to higher attendance numbers, more senior-ranking officials participated. We found that partner senior intelligence officers viewed shorter events as more focused, less resource-intensive, and a better use of their time. From our experience, we rarely hosted the actual partner land domain G-2 (colonel equivalent) during the in-person symposiums (5-day event), but during the virtual conference (3-hour event), three-fourths of the invited senior G-2s were in attendance.

The Sustains

While the pandemic forced a change to the USARCENT G-2 TIES program, not all the changes were seen as temporary. We decided to apply two lessons from the pandemic to future intelligence engagements. Before COVID-19, the USARCENT G-2's capstone multilateral event was the Regional Land Forces Intelligence Symposium. However, the pandemic made any in-person multilateral event unrealistic. Using a series of government-provided tools, we were able to connect virtually with our intelligence partners. Conducting a bilateral engagement in this way was quite simple; but how do you scale this to allow multiple partners and have meaningful engagement discussions with senior intelligence professionals? We decided to host a virtual event to mimic the Regional Land Forces Intelligence Symposium based on emerging academic experience on large-scale virtual conferences. This event was the Virtual Land Forces Intelligence Conference. While it was limited to an unclassified forum, it allowed maximum engagement with partners.

The second lesson we will continue to include in the TIES is to complement virtual events with bilateral in-person intelligence activities between the theater G-2 and partners. Partners in the region, because of security and network usage concerns, have long preferred in-person bilateral events. The pandemic was a forcing function to push our partners through these challenges. While the theater G-2 benefits from a theater network called the CENTCOM Partner Network (CPN), partners have not fully embraced the network. The CPN is a collateral network designed to provide a platform for bilateral operations between partners. The theater G-2 was able to capitalize on the partners' need for intelligence partnership during the pandemic to reinforce the use of CPN at the G-2 echelon. Over the course of the pandemic, partners started to appreciate the ease of CPN video teleconferences when weighed against the competing national pandemic response requirements. Going forward, in-person partnership activities will be augmented by a larger virtual presence.


The Virtual Land Forces Intelligence Conference and virtual augmentation to in-person bilateral events validated the strength of USARCENT's commitment to partners in the USCENCOM region during a challenging time. The positive reception of these events by all those involved led to their incorporation in the TIES. The Virtual Land Forces Intelligence Conference will now augment the annual Regional Land Forces Intelligence Symposium. Additionally, virtual bilateral events will complement in-person events. These two additions to the strategy reinforce existing bilateral events,



USARCENT Virtual Land Forces Intelligence Conference


On 27 October 2020, 11 partner nations and 12 U.S. intelligence organizations, comprising more than 60 attendees, virtually connected in the first Virtual Land Forces Intelligence Conference. The USARCENT G-2 hosted this 3-hour virtual conference with the intent to reaffirm USARCENT's commitment to existing regional partners amid the global pandemic. This reaffirmation was necessary because of the almost universal reduction in military-to-military partnerships across the globe resulting from COVID-19. USARCENT designed the event to replicate an in-person symposium, as close as possible, with materials, presentations, and speakers. The intent was to "conduct a multilateral partnered conference to discuss virtual intelligence operations under COVID-19 conditions in order to advance federated/distributed intelligence support to warfighters, while assuring existing foreign intelligence USARCENT's commitment to relationships within the Middle East."

All partners attended using Microsoft Teams, a connectivity tool for unclassified virtual communications. Representatives included senior intelligence professionals from Australia, Bahrain, Canada, France, Jordan, the Kingdom of Saudi Arabia, Kuwait, New Zealand, the United Arab Emirates, the United Kingdom, and the United States. Several U.S. organizations were represented, including the Department of the Army G-2, U.S. Army Intelligence Center of Excellence, U.S. Central Command, and U.S. Army Intelligence and Security Command. Major General Chris Field, Australian Army, USARCENT Deputy Commanding General for Operations, opened the event with a discussion about the impact of COVID-19 and the evolving nature of operations due to COVID-19. He also presented his perspective, as an Australian military commander, on serving as part of a coalition. USARCENT is fortunate to have a coalition leader within its formation. His appointment to a senior position highlights the importance both the Australian and the United States leadership place on allies and their input into the overall USARCENT strategy. Following Major General Field's opening remarks, attendees discussed the strategies their organizations and nations have taken to overcome COVID-19-related impacts. During the conference, the partners provided an overview of their organizations and the way in which their specific organizations fit into their nation's COVID-19 response strategy, specific efforts to maintain partnerships with allies during the crisis, and their way forward in a COVID-19-dominated environment. A highlight of the conference was a panel presentation led by a team from the National Defense University. The panel led a discussion on the impacts of COVID-19 in the land warfare domain. Through this discussion, common regional concerns and interest were identified, confirming the need to continue virtual connectivity events like this Virtual Land Forces Intelligence Conference in the future. The second Virtual Land Forces Intelligence Conference occurred on 23 and 24 March 2021, covering emerging threat trends in the region. The event was expanded to cover 2 days and allow more partner participation.



multilateral events, and partnerships through virtual forums, which support the overall USARCENT intelligence engagement strategy. USARCENT will continue to strengthen partner relationships in the Middle East region through a robust bilateral and multilateral program augmented by virtual engagements.

Conclusion

The USARCENT G-2 took restrictions from the COVID-19 pandemic and turned them into opportunities for increased success. We used available tools to change a situation that could have stopped our TIES completely into a plan to engage more robustly with our partners. Moreover, the broader USARCENT staff incorporated virtual engagement across other warfighting functions, giving the headquarters seamless and persistent connection to allies and partners. Virtual integration fostered low-cost, wide participation events, which enhanced the relationships that COVID-19 restrictions threatened, and underscored USARCENT's commitment to our partners at all times. Going forward, USARCENT will maintain the virtual connection opportunities to overcome the tyranny of distance regardless of the circumstances. Distributed intelligence, engagement, and mission command are the way our future Army will do business. 

Epigraph

Nikki Glanton, "U.S. Army Central hosts inaugural virtual intelligence conference," U.S. Army Central, 31 October 2020, <https://www.usarcent.army.mil/News/Article/2401108/us-army-central-hosts-inaugural-virtual-intelligence-conference/>.

Endnotes

1. Glanton, "Inaugural Virtual Intelligence Conference."
2. *Posture Statement of General Kenneth F. McKenzie, Jr., Commander, United States Central Command before the Senate Armed Services Committee 22 April 2021*, U.S. Central Command, 19, <https://www.centcom.mil/ABOUT-US/POSTURE-STATEMENT/>.
3. White House, *Interim National Security Strategic Guidance* (Washington, DC, 3 March 2021), <https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf>.
4. Office of the Secretary of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, n.d., 9, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
5. Department of the Army, (U) *The Army Strategy for Allies and Partners (ASAP) 2020* (Secret) (Washington, DC, 30 October 2020).
6. *Posture Statement of General Kenneth McKenzie*.
7. Department of the Army, *Army Strategy*, foreword.

COL John Chu is the former Assistant Chief of Staff for Intelligence, U.S. Army Central (USARCENT). He has more than 5 years of experience in the U.S. Central Command (USCENTCOM) region, most recently having served as the Commander of National Security Agency–Georgia. He has deployed to Iraq and Afghanistan. He holds a masters of arts in national security and strategic studies from the Naval War College and served as an Army War College military fellow at Stanford University.

LTC Quentin McCart is the Deputy Director, Intelligence Support Division, USARCENT G-2. He has more than 6 years of experience in the USCENTCOM region as an Air Force intelligence officer, Defense Intelligence Agency Civilian, and Army officer. He has more than 3 years of experience directly working the foreign engagement strategy within the USCENTCOM region. He holds a master of science in strategic intelligence from National Intelligence University.





United States Army aircraft assigned to the 1st Battalion, 228th Aviation Regiment, perform in-flight formation movements as part of a battalion continuity of operations (COOP) training exercise over Honduras and El Salvador, May 28, 2020. The battalion COOP is an effort to ensure essential functions continue to be performed in the case of an emergency in which Joint Task Force-Bravo would be called upon to assist. It also ensures readiness for pilots and the battalion as a whole. (U.S. Air Force photo by SrA Jovan Banks, Graphic by MIPB Staff)

Introduction

The operational environment in Latin America presents layers of complexity. Central America shares many things in common with other countries throughout U.S. Southern Command's (USSOUTHCOM's) area of responsibility, but it also bears a uniqueness given its geographic location between South America and the United States. It serves as a natural bridge between the two major regions, providing a crucial distribution channel. Where we find adequate investment in infrastructure, we see the conditions established for effective governance, application of security, and support for the rule of law, all of which are essential for economic growth and development. However, the most significant of these is effective governance. Unfortunately, for a long time, Central American nations have been subject to corruption, polarization of wealth, and varying forms of social injustice. While many people struggle throughout the region, there is potential for improvement. We just have to ask, "Where do we target an investment strategy, and how can we use it to promote stability?"

Panama

Panama is one of our best examples of potential coming to fruition. Panama, located at the base of Central America, houses the most strategically important asset in the entire USSOUTHCOM area of responsibility—the Panama Canal. The Panama Canal supports the annual distribution of

approximately \$270 billion worth of goods.¹ Approximately 60 to 70 percent of Panama Canal traffic accounts for the United States import-export volume. Both its regional and global significance are without question. The Pan-American Highway also supports extensive trade and distribution in the region, but its reach throughout many Central American nations remains limited. Overall, Central American nations spend approximately an average of 2 percent of their gross domestic product on transportation and infrastructure, a significant limitation for improving commercial market reach and development.²

Both of these critical infrastructure items are only as effective as far as they can reach. Many regions throughout Central America remain isolated because they lack a connective infrastructure and do not realize the value created by the Pan-American Highway and Panama Canal. The resulting barriers to legitimate market entry are major contributors to the polarization of wealth, and nearly every Central American nation has this challenge. A few examples are Gracias a Dios, Honduras; Izabal, Guatemala; Puerto Limón, Costa Rica; and Darién, Panama.

Narcotics Trafficking

While each country has access to trade and distribution venues, regionally, each nation also retains areas within its sovereign borders that remain isolated from legitimate market flows, affecting select local economies. As a result, transnational criminal organizations offer an alternative

Examples of Isolated Regions

Gracias a Dios, Honduras. Gracias a Dios remains grossly isolated from the interior of the country. Puerto Lempira, the largest settlement, is adjacent to Laguna de Caratasca along the east coast. This city retains no connective infrastructure to the capital, nor does it have an established port that supports maritime trade. As of 2015, an estimated 94,450 local nationals and 6,100 square miles of terrain remain without support from government services. As a result, criminal activity goes undetected, with low-level corruption being a principal enabler.

Izabal, Guatemala. Like Puerto Lempira in Honduras, Izabal does not retain the amount of critical infrastructure needed to support inland exchange and distribution. Additionally, rough terrain makes inland movement challenging and often untimely. Izabal lacks the amount of necessary infrastructure to support investing activities, specifically near Lake Izabal. Criminal organizations use areas near the eastern shoreline for the transshipment of illicit products, which presents a lucrative alternative to those who struggle to meet day-to-day needs.

Puerto Limón, Costa Rica. While Puerto Limón remains connected via causeway to the Costa Rican capital of San José, the port city remains significantly less populated than the interior of the country. As such, security and investment remain marginal. Over the last decade, drug traffic through the port city has increased significantly, serving markets in both the United States and Europe. Additionally, the Limón province is the most violent in the country. Without adequate security presence, investment, and development, Puerto Limón will continue to be a major projection point for cocaine distribution worldwide.

Darién, Panama. The Darién province is a region known for the Darién Gap—about a 60-mile break in the Pan-American Highway, affecting the flow of goods and services into the region. The gap is caused by extensive vegetation and severely restrictive terrain. Given the lack of development from Metetí to the southwest, local communities are prone to criminal influence—supporting both narco-trafficking and human smuggling. Illicit migration continues to challenge the security apparatus of the Panamanian government, as does the movement of illicit product throughout this region.

to legitimate business enterprise—black market activity. Isolated segments within each nation become prone to exploitation by the criminal enterprise and less supportive or cooperative with host-nation governance. In essence, we see the theory of competitive control in action.³

In each of the isolated regions described above, narcotics trafficking, which has existed for many years, continues to flourish. With a growing demand for illicit products in Europe, Colombian traffickers have expanded their production and outflow to place product to market in regions beyond North America. With the drug trade thriving, criminal organizations are putting more effort and investment into protecting supply chains out of Costa Rica, particularly in Puerto Limón. For local inhabitants, this offers better opportunities than basic employment. With average incomes reported at approximately \$17,000 per year, additional cash from illicit activity is hard to resist.⁴

Like Puerto Limón, Gracias a Dios (Honduras) and Izabal (Guatemala) are two key areas where narco-trafficking efforts continue to prosper (Figure 1 on the next page). Both areas are extremely isolated from governing influence and support, and both have continued reports of illicit aircraft encroachments that contain large amounts of narcotics shipment. Illegal maritime trafficking occurs near these areas. Because of the long tracks that both aircraft and watercrafts make, corruption within host-nation security and

military forces is necessary to assure successful movement over land and can even enable port-to-port exchange via littoral movement.

Even without the presence of corruption, a lack of presence and infrastructure needed to sustain military operations severely degrades both countries' ability to detect and respond to illicit encroachments. With the recent passage of the new Air Sovereignty Law in Honduras, increasing support from the United States and many Central American partners (including Colombia) continues to be provided for the detection and monitoring of illicit aircraft encroachment; however, detection and interdiction are only part of the solution. Without infrastructure and subsequent economic development, members of local populace in both regions will remain complicit, and oftentimes cooperative, with the criminal organizations. "*Plata o plomo*" (silver or lead, i.e., money or bullets) becomes their only option, making the criminal enterprise the dominant influence on a region's inhabitants. In short, they forcibly become reliant on the criminal enterprise, or die. Without a stable alternative for the local people, they will continue to support black market activity, and drug trafficking will thrive.

China's "One Belt, One Road" Initiative—Picking Up Where We Left Off

In 2013, the Chinese government announced its One Belt, One Road initiative, also known as the Belt and Road



Figure 1. Population Density Study, NGA, 2019⁵

Initiative, aimed at developing infrastructure projects on an international scale to dominate global supply chains. With the United States historic efforts behind the construction of the Panama Canal and the Pan-American Highway, the Chinese have a predetermined roadmap for success. According to the American Enterprise Institute, the Chinese have invested approximately \$1.4 trillion (U.S. dollar equivalent) globally since 2013, with approximately \$3.8 billion worth of projects in Central America (Figure 2), with most of its development concentrated along areas either near or directly along the Pan-American Highway.⁶

Investments in Panama have been most notable, with Costa Rica and El Salvador heavily targeted as well. While the introduction of Chinese physical capital has supported economic development, it has also been arguably predatory. In general, Chinese investments gravitate mainly toward areas where distribution transcends one sovereign territory to the next, giving the Chinese greater ability to gain cost control over a nation's

imports and exports. This can be problematic in the event of a dispute with the Chinese government. Additionally, multiple cases have been reported implicating Chinese involvement in illegal logging, mining, and wildlife trafficking, alongside allegations of white-collar crimes such as bribery and corruption.⁸ The nature of Chinese business dealings has not been ethical, nor have these business dealings been in the best interest of the host nation, despite their appearance. However, the introduction of new infrastructure, capital, and employment has been effective in eroding the influence of criminal organizations. As mentioned previously, remote areas with little government reach are where there tend to be greater propensities for illicit activity.

Central America, Chinese Investments & Construction (2013-2020)	
Investing Activities, 2013 to 2020	
Belize	\$ -
Guatemala	\$ -
El Salvador	\$ -
Honduras	\$ 350,000,000.00
Nicaragua	\$ -
Costa Rica	\$ 470,000,000.00
Panama	\$3,000,000,000.00
CENTAM Total since 2013	\$3,820,000,000.00

Figure 2. Chinese Investment Outlays (in billions) from 2013 to 2020, Central America⁷

So how exactly does the growth of the Chinese business enterprise threaten United States interests? The answer is simple: If the Chinese control distribution, then they control the flow of imports into the United States, along with the flow of exports outward. The Chinese would essentially retain the ability to harness greater power over pricing mechanisms associated with product distribution in either direction. This can pose a direct threat to our economy. Additionally, where there are Chinese investments, the potential exists for an increasing Chinese military presence. Should the Chinese emerge as the partner of choice for our Central American partner nations, this will pose a direct threat to both United States national security and Central American regional security across all instruments of national power.

Nicaragua and the Waterfall Effect

After decades of political conflict, it is no surprise that Nicaragua has little to no ties with the United States. Since the 1980s, the United States has maintained its stern position with regard to the Sandinista regime and its past affiliation with the Soviet Union and now with the Russian government. In recent years, when Daniel Ortega (a long-time Sandinista) reclaimed power as President of Nicaragua, the United States reaffirmed its opposition toward the Sandinista regime and its alliance with the Russians, particularly on human rights violations that the Sandinista regime has committed. In late 2018, the Nicaraguan National Police and pro-Sandinista paramilitary groups were behind a series of massacres committed against various local populations during a string of protests against the regime.⁹ More than 300 Nicaraguan nationals were murdered during this time, warranting attention from the United Nations and subsequent sanctions imposed by the United States and European nations. Despite the outcry and criticism, the Sandinista regime has maintained its power and control of the government.

Since the massacres in 2018, migratory outflow has continued on a progressive trend into Honduras and Costa Rica. In a 2019 interview, Costa Rican Vice President Epsy Campbell Barr disclosed that approximately 86,000 Nicaraguan nationals had fled to Costa Rica seeking refuge from the oppressive Sandinista regime.¹⁰ A month later, she stated that this number had grown to approximately 106,000. With criminal activities increasing across Costa Rica, many government leaders believed that Nicaraguan nationals were seeking financial support via the criminal enterprise. In January 2020, the United States State Department elevated the travel advisory from level 1 (exercise normal precautions) to level 2 (exercise increased caution), drawing criticism

from Costa Rican President Carlos Alvarado Quesada. The change in travel advisory would have a significant impact on the tourism industry, as well as many of the structured engagements and exchanges between Costa Rica and the United States, striking a significant blow to the Costa Rican national economy.

Nicaraguan domestic policy and the subsequent “waterfall effect” of migratory outflows into Costa Rica have clearly warranted concern on a regional basis. In February 2020, then-Secretary of State Mike Pompeo visited with President Alvarado Quesada to discuss the challenges that Costa Rica was facing, focusing mostly on the reasons for the increase in reported crime. During this meeting, members of Sandinista opposition were also able to meet with the U.S. Secretary of State, highlighting the long-standing issues associated with the Sandinista regime and its need for U.S. involvement and promoting favorable policy measures.


In recent developments, mass migration continues to remain at the forefront of national discourse, especially in the wake of hurricanes Eta and Iota in Honduras. Hidden among these migratory caravans were human trafficking and smuggling efforts. There were also reports of members of criminal gangs attempting to blend in with large-scale movement. Furthermore, with the pandemic continuing to affect many communities globally, illicit pathways could further spread coronavirus disease 2019 (COVID-19) within the United States. Overall, because of the conditions of instability derived from poor economic development, corruption, internal regional isolation, and poor perception for the rule of law, many parts of Central America are largely responsible for numerous national security concerns that currently affect the U.S. southern border. With presence, influence, and increased investment, the conditions throughout the region can evolve toward those that are more favorable to all. The Chinese government has already recognized this situation and used this approach accordingly, especially since the emergence of the COVID-19 pandemic. However, their approach does not support diplomatic relationships between the United States and Central America—that is for us to develop.

Conclusion

So how do we proceed as a military force in the Central American region? Continued support to humanitarian assistance opens the doorway for our partners across the spectrum of government capabilities. In 2019 and 2020, USSOUTHCOM provisioned civil affairs teams to Joint Task Force-Bravo to develop a mechanism for persistent engagement. In concert with intelligence and public affairs offices, civil affairs teams help to initiate and integrate

efforts to promote U.S. goodwill, ergo incentivizing nations to view the U.S. Department of Defense as the regional partner of choice.

Furthermore, the presence of persistently engaged civil affairs teams will help identify local needs and investment opportunities for both U.S. Government interests and private enterprise. In the long term, this will be critical to

energize efforts to outperform the Chinese competitors and counter the influence of criminal organizations. Within the Department of Defense, we can project influence through increased security cooperation, global health engagements, and combined exercise initiatives. However, for these to make a positive impact, our engagement must be persistent. We simply need to “be there.”¹² 

Joint Task Force-Bravo

On 1 September 2019, Joint Task Force-Bravo (JTF-B) gained operational control of a U.S. Army Reserve Civil Affairs Company comprising five civil affairs teams and a company headquarters. Prior to this date, JTF-B had never had a civil affairs tactical capability. JTF-B, in partnership with USSOUTHCOM, developed funding, authorities, and permissions for each of the five civil affairs teams to be persistently deployed within JTF-B's named areas of interest across Central America. The civil affairs teams' mission was to first understand the threat—transnational criminal organizations and external state actors—by conducting civil reconnaissance and civil engagement with indigenous civilian stakeholders across the military, police, private industry, and provincial government. Upon understanding the friendly, neutral, and enemy situation, the civil affairs teams executed support to civil administration operations, activities, and investments to bolster the friendly indigenous networks, which in turn undermined, isolated, and disrupted threat influence over key populations.

One example of support to civil administration operations, activities, and investments is the civil affairs teams' combined COVID-19 response, which from March to July 2020 provided approximately \$1.3 million of aid to the northern triangle governments to fight the pandemic. All operations, activities, and investments were closely synchronized with the JTF-B public affairs office to amplify the effects across Central America. For COVID-19 response operations, activities, and investments, the tactical level effect (messaging) depicted that the indigenous government was directly aiding the populace, which legitimized local governance—indirectly delegitimizing transnational criminal organization political influence. The operational level effect (messaging) involved compiling all of the U.S. Government's COVID-19 response activities across JTF-B, the U.S. Embassies, and USSOUTHCOM to emphasize across the northern tier—that the U.S. Government was the partner of choice—indirectly delegitimizing external state actors' political influence.

Civil affairs operations were most symbiotic with the JTF-B J-2 and the public affairs office. The JTF-B J-2 determined the named areas of interest in which the civil affairs teams operated. Then the civil affairs teams' civil information management further illuminated threat activities and motivations within a named area of interest. Additionally, a singular civil affairs team COVID-19 response activity may only aid one village. However, by leveraging the public affairs media networks, the COVID-19 response activity was broadcast to influence thousands of people—amplifying effects at both the tactical and operational levels.

—LTC Jeffrey Uherka, JTF-B, Civil Affairs¹¹

Endnotes

1. Luke Kwong, “10 Facts about Economic Development in Central America,” The Borgen Project, September 7, 2019, <https://borgenproject.org/10-facts-about-economic-development-in-central-america/#:~:text=%2010%20Facts%20About%20Economic%20Development%20in%20Central,wake%20of%20Hurricane%20Nate%2C%20Costa%20Rica...%20More%20>.
2. Ibid.
3. David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (New York: Oxford University Press, 2013).
4. “Average Salary in Limon, Costa Rica,” Salary Expert, Economic Research Institute, accessed August 31, 2021, <https://www.salaryexpert.com/salary/area/costa-rica/limon>.
5. Alfonso Torres, “Landscan Image, Honduras-Guatemala 2019,” [map], 1/4,000,000 (San Antonio, TX: U.S. Army South, May 2021), using ArcGIS [GIS software], Version 10.7.1 (Redlands, CA: Environmental Systems Research Institute, Inc., 2010).
6. “China Global Investment Tracker,” American Enterprise Institute, 2021, <https://www.aei.org/china-global-investment-tracker/>.
7. Ibid.
8. “China’s Environmental Abuses,” U.S. Embassy Panama, October 5, 2020, <https://pa.usembassy.gov/chinas-environmental-abuses/>; and Bill Majcher, “Panama Papers reveal Hong Kong’s role in the world of tax havens,” Nikkei Asia, April 14, 2016, <https://asia.nikkei.com/Economy/Panama-Papers-reveal-Hong-Kong-s-role-in-the-world-of-tax-havens>.
9. Nina Lakhani, “Nicaragua used ‘weapons of war’ to kill protesters, says Amnesty International,” *The Guardian*, October 18, 2018, <https://www.theguardian.com/world/2018/oct/18/nicaragua-amnesty-international-police-killings-daniel-ortega>.
10. Nathaly Salas Guaithero, “Costa Rica: Los migrantes nicaragüenses ‘son una carga pesada’” [Costa Rica: Nicaraguan migrants are a heavy burden], *Voz de America*, 7 October 2019, <https://www.vozdeamerica.com/americas-latina/migrantes-costa-rica-nicaragua-asilo-honduras-carga-pesada-campbell>.
11. LTC Jeffrey Uherka, interview with author, February 20, 2021.
12. COL Gary Miskovsky, interview with author, November 7, 2019.

References

Jaccard, Nathan, Sol Lauría, David Tarazona, Mateo Yepes, and Lilia Saúl. "Illegal Chinese Cigarettes Flooding Latin America Flow Through Panama." Organized Crime and Corruption Reporting Project. June 22, 2021. <https://www.occrp.org/en/loosetobacco/china-tobacco-goes-global/illegal-chinese-cigarettes-flooding-latin-america-flow-through-panama>.

Mora, Jean Pierre. "Nicaraguan refugee heals wounds of persecution in Costa Rica." The UN Refugee Agency USA. 25 August 2020. <https://www.unhcr.org/news/stories/2020/8/5f3ea3734/nicaraguan-refugee-heals-wounds-persecution-costa-rica.html>.

Richelson, Jeffrey T. *The US Intelligence Community*. Boulder, CO: Westview Press, 2011.

Vardeman, Ella and Julie Velásquez Runk. "Panama's illegal rosewood logging boom from *Dalbergia retusa*," *Global Ecology and Conservation* 23 (September 2020). <https://www.sciencedirect.com/science/article/pii/S2351989419309126>.

MAJ Mark Medlock enlisted in the U.S. Army in 2003 serving as an intelligence analyst focused on Latin American affairs and support to counterterrorism. In 2006, he attended Officer Candidate School and commissioned as an intelligence officer. He currently serves as the Chief of Intelligence Planning for U.S. Army South G-2, Fort Sam Houston, TX, Joint Base San Antonio. MAJ Medlock's previous assignments include 2nd Infantry Division, the 75th Ranger Regiment, 1st Armored Division, the U.S. Army Intelligence Center of Excellence, U.S. Army North, and Joint Task Force Bravo. His overseas tours of duty consist of Korea, Iraq, Afghanistan, and Honduras. He is a graduate of Texas Tech University with bachelor's degrees in finance, accounting, and economics.

Contributor:

COL Gary Miskovsky is the G-2 Assistant Chief of Staff at U.S. Army South.

The Military Intelligence Training Strategy (MITS) series of publications are available for download from—



APD | ARMY PUBLISHING
DIRECTORATE

1. The Army Publishing Directorate at <https://armypubs.army.mil/>,
then - Publications - Doctrine and Training - Training Circulars

-or-



Directorate of Training

Customer Focus | Products & Outreach | Development & Integration | Educational Design & Development | Training the Team

2. The Intelligence Knowledge Network (IKN) at <https://ikn.army.mil/apps/dot>, select "MI Training Strategy (MITS)" link on the left side of the page.

Select "Links" under the MITS banner at the top of the page to access the training circulars plus a variety of other related resources.

Russian Tactical Correlation of Forces & Means Computation Updated for Modern Equipment and Capabilities

by Lester W. Grau, Ph.D., and Mr. Clint Reach

Editor's Note: This article is part two of a two-part series on the Soviet correlation of forces and means. Part one, titled "A Mathematical Probability of Success for Soviets in Cold War Confrontation," was published in the April–June 2021 issue of the Military Intelligence Professional Bulletin.

The authors assume responsibility for the veracity, accuracy, and source documentation of the material, including no use of classified material and conformity to copyright and usage permissions. The views expressed are those of the authors and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or U.S. Government.

Introduction

Russians have long pursued mathematizing battle, believing that the inherent values of various weapons and systems can be measured and compared against a single quantitative standard. The military professional may suspect the existence of such a relationship, but proving it has been difficult. The Soviet military sought to reduce tactical and technical aspects of military science to measurable, objective indices from which decisions could be made or otherwise substantiated. A sub-element of Soviet military operations research was the correlation of forces and means (COFM) methodology. COFM is still considered a powerful tool for

helping operational- and tactical-level commanders in their decision-making processes. The Russian definition of COFM is basically unchanged from the Soviet definition:

The Correlation of Forces and Means [Соотношение сил и средств] is determined by comparing the quantitative and qualitative characteristics of subunits, units, formations, weapons, military equipment, etc., of one's own forces with those of the enemy. This provides an objective indicator of the combat power and the operational/tactical potentials of the opposing sides and allows one side the opportunity to take measures to gain superiority over the other side. The correlation of forces and means (COFM) exerts great influence (sometimes the deciding influence) on operational and tactical plans during their preparation and refinement with the aim of the timely determination and support for the necessary superiority over the enemy on the selected axes.¹

As with all operations research-related techniques, COFM's focus is toward the ultimate "goal" of a particular task—specifically, the direct numerical comparison of forces. Its principal mechanisms are (1) the quantification of selected battlefield elements, and (2) the mathematical expressions (or formulae) that relate those elements in such a manner to support decision making. These mechanisms are used to develop conclusions about the status of opposing combatants at particular stages of the unfolding battle.²



Statue of the Russian double-headed eagle that is part of the Russian Federation's coat of arms. Saint Petersburg, Russia³

COFM Enters the 21st Century

The Soviet Union collapsed and a smaller, weaker Russia emerged. Still, the COFM methodology survived.⁴ Over time, the coefficients of commensurability were upgraded. Apparently, the upgraded system resembles the old system, only further computerized at the tactical level. The coefficients of commensurability (measurements of relative combat power) are derived using the standard methods of qualimetry, developed for quantitative measurement of the level of quality of industrial products.⁵ A subset of the Russian discipline of qualimetry is military potentialometry, which focuses on military applications. The combat potential or quality of an asset or formation represents the asset's value and reliability under general conditions.⁶

Some Russian scientific research institute analysts and academicians are examining ways to improve the system. To their way of thinking, the coefficients of commensurability (or combat power) for individual systems is a good start; however, the effectiveness of the overall system is not equal to the sum of the effectiveness of its elements. Not all systems can be brought to bear at once, and the value of various systems varies with the type of combat conducted. These analysts believe it is unacceptable to put an equal sign between two complex systems—between a weapon or piece of military equipment and a military formation, regardless of the level of hierarchy—and apply the same methods of assessment to them. The effectiveness of the system is not equal to the sum of the effectiveness of its elements.⁷

The Russians' new approach to COFM would assess the abilities of subunits and below to perform their missions in various types of combat. In the offensive, they would assess weapon sets when the armed forces break through prepared defenses, when attacking a hastily occupied defense, and in a counterattack; in the defense, they would assess the conduct of military actions in prepared positions, in a hasty defense, and when repelling the enemy's offensive by deploying to a prepared line.⁸

During combat, the quality of various weapons of various types varies during the different stages. During the fires preparation for the attack, the combat capabilities of missile and artillery units, as well as aircraft flying along a determined axis, are most apparent. At the beginning of the attack, in addition to the quality of the artillery assets, the combat capabilities of the attacking motorized rifle and tank subunits are of greatest significance. When repelling an enemy counterattack, the quality of antitank weapons, close-combat weapons, and small arms is significantly increased. Therefore, a step-by-step assessment of weapon sets makes it possible to consider interrelated combat situations. The assessment thereby creates conditions for a solid forecast

of the course of combat taking into account the influence of the weapons of each type on performing combat missions, and taking into account the counteractions of the enemy during each intermediate task.⁹

A proposed change to the current COFM is to use a BMP-3—based motorized rifle battalion tactical group (three motorized rifle companies and a tank company) as the standard or reference potential (base one) of the combined arms subunits of Russian troops. The combat potentials of other combined arms units should be determined in units of reference potentials.¹⁰ Expected casualties could be calculated to adjust the combat potential of the friendly and enemy units during each stage of the action. Currently, this is just a proposal, and the current tactical battle planning is calculated using mathematics based on those shown in Annex A.

There are some problems with this approach. First, an 85 percent equipment readiness rate is often common at the operational level, but it is spread over a large formation. An 85 percent equipment readiness rate at the tactical level is usually not evenly spread over the battalion or brigade. Smaller units tend to have things go badly wrong simultaneously in the same category of equipment. Second, a battalion tactical group very often includes an accompanying howitzer battalion. The responsiveness and effectiveness of direct support/attached artillery are much different from supporting artillery and would skew those COFM calculations using a BMP-3—based motorized rifle battalion tactical group. Assigning a 20 to 25 percent equipment and personnel loss per tactical event (as suggested in the study) does not take into consideration that the bulk of losses in tactical combat is in the maneuver elements, not the combat support elements. Using a standard unit as base one is easier when doing calculations, but basing COFM calculations on operable systems still seems the best approach for now.

A More Contemporary Example of COFM (Tactical Level)

Not all tanks are equal. How can one determine the winner in a tank-versus-tank fight or in an antitank-guided-missile-versus-a-tank fight? Modern combat is seldom an isolated duel between individual systems. Modern combat is fought between units and subunits wielding a variety of weapons for which aggregate combat power is a determining factor in the battle's outcome. Rough COFM equations are still used to verify tactical decisions by determining combat outcomes. In 2011, the Department of Tactics and General Military Training of the Belarus National Technical University published a low-level tactical text titled "Combat Capabilities of the Motorized Rifle (Tank) Platoon, Subunits (Tank), and Their Calculation." Belarus is an ally of Russia and uses Russian equipment and military theory. This text was designed for military cadets in university-level

training.¹¹ Annex A is a translated extract of the text. The following summarizes the main points:

Mathematics supports the tactical commander's development of a course of action by answering the following questions:

- ◆ How many and what kind of forces will be necessary to accomplish my mission?
- ◆ What tasks can be accomplished with the forces and resources at hand?
- ◆ What result can be expected from the composition of all sides involved in the confrontation?
- ◆ How do I best use my forces and resources in order to achieve my objectives with minimal losses?¹²

These questions are addressed by calculations of combat capabilities of small units by a comparison of the combat potential of resources involved in the fight. Combat capabilities are quantitative and qualitative indicators that characterize the capabilities of military tactical units (platoon, company, battalion, and brigade).

Combat capabilities depend on—

- ◆ Number of personnel and level of their readiness for combat.
- ◆ Availability, condition, and quality of weapons and combat and other equipment.
- ◆ Ability of the commander and staff to lead the combat units.
- ◆ Organizational structure of forces and their logistical support.
- ◆ Composition and characteristics of enemy opposition, condition of the surroundings.
- ◆ Meteorological conditions, weather, time of year, and day during which combat occurs.

Particular indicators are realized in the combat capabilities of combat units of different types of troops:

- ◆ The width of the front lines (size of the stronghold).
- ◆ Depth of combat objective of the combat unit.
- ◆ Speed of movement of the combat unit.
- ◆ Depth of direct fires; effects on enemy targets.
- ◆ Effective radius of offensive weapons.
- ◆ Time required for subdivision to prepare (direct fires resources) to open fire.

The summed combat capabilities are—

- ◆ Fires capabilities—the total volume of fires tasks that can be accomplished.

- ◆ Strike capabilities—the capability of combat units to destroy the enemy through the combination of fires and maneuver.
- ◆ Maneuverability capabilities—the level of mobility and ability to move quickly.¹³

Russian scientific research institutes calculated the data to produce standard reference weapons. During the Cold War, the base standard reference weapon was the Soviet T-55 tank and was base one. Other ground forces equipment was rated against this weapon and assigned standard values. A similar process was used for air-to-air, air-to-ground, and naval combat.¹⁴

With the advances in technology, survivability, and fire-power, there is a new set of standard reference weapons with base one as the T-72A tank.

How these values are used is demonstrated in the set of extracted student problems reproduced in Annex A. The future platoon leader would not necessarily have the time to do all of the math every time he put his platoon in position. The purpose of the training is to make the student comfortable and proficient with the system. The mathematics would be done regularly at battalion and brigade.

Modernizing for Today

Combat systems, sensors, communications, computers, targeting procedures, and onboard defensive systems have all evolved dramatically since the collapse of the Soviet Union. The COFM system was designed to provide predictability in military engagements. Today's world is more complex than during the Cold War, but the need for predictability still exists for tactical, operational, and strategic engagement—as well as nuclear use. Many of the aspects of the Soviet COFM system may appear clunky and outdated, but indications are that the Russians are attempting to provide military predictability using the computational power of modern computers.

It is clear that operational-tactical calculations are key during the commander's decision making when determining force composition and mission accomplishment.¹⁵ In 2002, Major General Vorobyev, who once served in the Science Division of the Soviet General Staff, wrote—

*The use of computers plays a decisive role in performing operational-tactical calculations to coordinate interaction and model combat. They assist in rapidly determining the combat potential of units and subunits; their quantity and quality; the correlation of forces and means on a given axis; the COFM on subsequent missions; the effect of nuclear and conventional fire strikes on the enemy; the optimum composition of fire systems; the optimum methods for employing artillery, air defense and army aviation; the capabilities of reconnaissance and electronic warfare, and the organization of engineer supply and maintenance support.*¹⁶

An automated command and control system is a key development to allow Russia to obtain information dominance on the modern battlefield. It allows the Russian commander to quickly gain situational understanding, draft and transmit plans, and effectively execute combat more quickly than his adversary. The Russians believe that in high-intensity maneuver warfare, it is better to execute a satisfactory plan

early than a custom-designed plan late.¹⁷ The wide-scale computerization effort within the Russian Armed Forces supports their effort to continue to improve their COFM approach to modern combat and operations. Some of this is still murky, and there is a dearth of complete contemporary models; however, a look at Russia's COFM antecedents provides some clues. What's past is prologue.¹⁸

Standard Reference Weapons of Foreign Militaries

TYPE OF ARMOR & COMBAT EQUIPMENT	POTENTIAL
BMP, BTR, TANKS	
M1 "Abrams"	1.47
M1 A1 "Abrams"	1.87
M60 A2	2.60
"Leopard" 1A4	0.88
"Leopard" 2	1.90
"Leopard" 3	2.80
"Chieftain" MK-5	0.92
AMX-30-B2	0.65
"Leclerc" 1	1.80
IFV "Bradley" M2	0.55
BRM-M3 (armored recon vehicle)	0.55
"Marder"	0.26
IFV "Marder" A1(A2)	0.45
"Lux" APC w/antitank guided missile	0.26
APC w/o antitank guided missile	0.06

ANTITANK WEAPONS

"Hot"	0.58
"Tow"	0.56
"Milan"	0.46
"Dragon"	0.32
"Vigilant"	0.24
"Jagdpanzer"	0.37
120mm Recoilless Rifle	0.14
106mm BO	0.16
90mm Recoilless Rifle	0.07
"Panzerfaust" 3	0.20

Standard Reference Weapons of Russian Manufacture

TYPE OF ARMOR & COMBAT EQUIPMENT	POTENTIAL
BMP, BTR, TANKS	
T-64A	0.88
T-64B	1.24
T-72	0.88
T-72A	1.00
T-72B	1.65
T-80	1.06
T-80B	1.65
T-80 UD	1.85
BMP-1	0.47
BMP-2	0.43
BMP-3	0.65
BMPT-T	0.88
BMD	0.47

ANTITANK WEAPONS

"Konkurs" [AT-5 Spandrel]	0.45
"Fleyta" [AT-2 Swatter]	0.46
"Falanga" [AT-2A Swatter]	0.41
"Malyutka-P" [AT-3 Sagger]	0.39
"Fagot" [AT-4B Spigot]	0.36
"Fagot" [AT-4A Spigot]	0.32
"Shturm" [AT-6 Spiral]	0.58
100mm antitank gun MT-12	0.38
SPG-9 recoilless rifle	0.15
RPG-7B	0.07
RPG-16	0.09
RPG-7B (with tandem PG)	0.20

ANNEX A

Authors' Note: The following is an extract from student text showing the mathematical determination of low-level tactics from the 2011 Belarus National Technical University's "Combat Capabilities of the Motorized Rifle (Tank) Platoon, Subunits (Tank), and Their Calculation."¹⁹

1.1 Initial Data for Evaluating Fires Capabilities in Combat against Enemy Armor Vehicles

Many countries employ armaments for their militaries. These armaments include tanks, infantry fighting vehicles, armored vehicles, and antitank weapons (antitank guided missile systems, handheld, and mounted antitank grenade launchers) that possess different tactical and technical characteristics, e.g., different quality, and more importantly, modern versions of different types of equipment surpassing by two times and more the fire power, defense armor, mobility, and accuracy of rockets (warheads). For example, the modern tank T-72B surpasses T-72D because of the installation of a more perfected stabilizer, guided weapons, dynamic defense, and a more powerful engine. Installing the active defense system "Shtora" [curtain], "Drozd" [thrush] immeasurably increases their survivability (T-80UD, T-90S).

At the same time, the militaries of foreign governments are armed with combat equipment that is constantly modernized based on the combat experience of such equipment in local wars and conflicts and the use of new technology. The primary emphasis is on increasing the destructive range (kill radius), armor penetration, and crew protection. For example, the U.S. Army's BMP M2 "Bradley" is being modernized in the following ways:

- ◆ increased survivability—dynamic defense (the equivalent of armor in the front up to 550 to 650 mm) is being installed; the use of composite materials based on fiberglass to build the frame, which increases survivability by 25 percent, decreases weight by 40 percent.
- ◆ increased fire power—installation of the 40 to 50 mm automatic cannon and TOW-2(3) antitank guided missiles, and the use of more modern ammunition.

Thus, the calculation of the capabilities of combat units in combat with enemy tanks and armored vehicles must take into account the quality of the weapons and combat equipment of own troops and the troops of the enemy. This is accomplished by establishing a standard reference weapon against which every weapon and piece of military equipment is measured.

Standard reference weapon is an established value for measuring the combat potential of weapons and military equipment. Calculations use the combat potential of the T-72A tank. All other weapons and equipment (ours and foreign militaries'), such as tanks of other makes, BMPs, antitank weapons, and so on, are compared to the combat potential of the T-72A tank under the conditions of direct engagement (equal conditions) (Tables 1 and 2).

Authors' Note: Tables 1 and 2 show combat potentials (also known as coefficients of commensurability) for various North Atlantic Treaty Organization and Russian/Belarus systems.²⁰

Table 1.
Combat Potential of Weapons of Foreign Militaries

TYPE OF ARMOR & COMBAT EQUIPMENT	POTENTIAL
BMP, BTR, TANKS	
M1 "Abrams"	1.47
M1 A1 "Abrams"	1.87
M60 A2	2.60
"Leopard" 1A4	0.88
"Leopard" 2	1.90
"Leopard" 3	2.80
"Chieftain" MK-5	0.92
AMX-30-B2	0.65
"Leclerc" 1	1.80
BMP "Bradley" M2	0.55
BRM-M3 (armored recon vehicle)	0.55
BMP "Marder"	0.26
BMP "Marder" A1(A2)	0.45
"Lux" BTR w/antitank guided missile	0.26
BTR w/o PTUR	0.06

ANTITANK WEAPONS

"Hot"	0.58
"Tow"	0.56
"Milan"	0.46
"Drakon"	0.32
"Vigilant"	0.24
"Yagdpanther"	0.37
120mm BO [Recoilless Rifle]	0.14
106mm BO	0.16
90mm RPTR [reactive antitank gun]	0.07
RPG [hand-held antitank grenade launcher] "Panzerfaust" 3	0.20

Table 2.
Combat Potential of Weapons of the National Military

TYPE OF ARMOR & COMBAT EQUIPMENT	POTENTIAL
BMP, BTR, TANKS	
T-64A	0.88
T-64B	1.24
T-72	0.88
T-72A	1.00
T-72B	1.65
T-80	1.06
T-80B	1.65
T-80 UD	1.85
BMP-1	0.47
BMP-2	0.43
BMP-3	0.65
BMPT-T	0.88
BMD	0.47

ANTITANK WEAPONS

"Konkurs" [AT-5 Spandrel]	0.45
"Fleyta"	0.46
"Falanga" [AT-2A Swatter]	0.41
"Malyutka-P" [AT-3 Sagger]	0.39
"Fagot" [AT-4 Spigot]	0.36
"Fagot" mobile	0.32
"Shturm" [AT-6 Spiral]	0.58
100mm PTP MT-12	0.38
SPG-9	0.15
RPG-7B	0.07
RPG-16	0.09
RPG-7B (with tandem PG)	0.20

In calculating the fires capabilities in combat with armored vehicles, it is also necessary to account for the coefficients of combat effectiveness (Table 3).

Table 3. Coefficients of Combat Effectiveness

TYPE OF ARMOR & MILITARY EQUIPMENT	NUMBER OF PIECES OF EQUIPMENT	COEFFICIENT OF COMBAT POTENTIAL	COMBAT POTENTIAL (NUMBER OF STANDARD REFERENCE WEAPONS)
<i>Small arms</i> AKS-74, AKS-74U, AK-74, SVD	102	0.01	1.02
RPK-74, PKM, PKT	23	0.04	0.92
GP-25 grenade launcher	27	0.02	0.52
PM pistol	20	0.01	0.20
Combat Potential			2.66
Tanks, BMP, BTR, C2 Veh. BMP-2	10	0.53	5.30
BMP-2K	1	0.53	0.53
SBR 3 (BRM-3k)	1	0.03	0.03
Combat potential			5.86
Mobile ATGM, SPG, RPG	9	0.07	0.63
RPG-7B			
Combined combat potential			0.63
Total combat potential			9.15

Table 3 presents the combat potential for a standard Belarus motorized rifle company equipped with the BMP-2 Infantry Fighting Vehicle. The first block shows the combat potential of the company's small arms, machine guns, and automatic grenade launchers (2.66). The second block shows the combat potential of the 12 organic fighting vehicles (5.86) and the combat potential of the nine dismounted RPG-7 antitank weapons (0.63). The expected enemy force's combat potential can be determined from Table 1 and the standard table of organization and equipment intelligence reports.

These show the number of tanks and BMPs that can be destroyed under different battlefield conditions before our [Belarus] antitank assets (tanks, antitank weapons, BMP) sustain battlefield damages.

Using the standard set of the weapons and military equipment within combat formations, potential combat capabilities of combat formations can be calculated in advance taking into account the quality, tactical and technical characteristics, and the required amount of supply held in reserve. This will result in the maximum capability, calculated in ideal conditions, without accounting for enemy counteractions, possible losses, and so on.

Typical combat capabilities are calculated based on average, e.g. typical, conditions. Real combat capabilities are calculated in preparation for battle, when military formations receive specific combat tasks and the situational conditions in which these tasks are to be executed are known.

Real combat capabilities of a combat unit in a defensive action are understood to be quantitative and qualitative indicators that characterize the ability to repel a strike from a specific enemy force grouping and to inflict significant losses while at the same time holding a defensive area with the condition that the preservation of combat capability of friendly forces is preserved at a level at which the defense can be ensured going forward.

Real combat capabilities of a combat unit in an offensive action are understood to be quantitative and qualitative indicators that characterize the ability to destroy a certain force grouping of a defending enemy and to capture an important area (vector) in an established timeframe with the condition that the preservation of combat capability of friendly forces is preserved at a level at which the offensive can be ensured going forward.

Depending on the level of the impact of enemy actions and incurred losses, combat capability may be maintained, partially lost, or completely lost. In this instance, the combat unit—

- ◆ Maintains combat capability, having sustained personnel and combat equipment losses up to 20 percent.

- ◆ Becomes partially (limited) combat capable, having sustained losses up to 50 to 60 percent and maintains command and control.
- ◆ Completely loses combat capability, having lost command and control and sustained damage to 50 to 60 percent of forces and means.

The foundation of combat capabilities of military formations is the combat potential of these formations, which is determined based on existing armament and military equipment, and personnel with appropriate materiel resources, based on standard supply norms.

1.2 Combat Capabilities of a Company in the Defense and Their Calculation

Combat capabilities of a company in the defense are characterized by fires and maneuver capabilities and by strike capabilities during counterattacks.

Knowledge of combat capabilities allows the company commander to assign combat missions intelligently and correctly use weapons in combat.

The definition of *fires capabilities* includes the ability of the company to use its antitank assets to destroy advancing tanks and other enemy targets, and to destroy personnel using small arms and other fires assets of the enemy.

The calculation of the capabilities of a company in combat with enemy armored vehicles during defensive combat is based on the use of the combat potential of armor and combat equipment and the coefficients of combat effectiveness of antitank weapons in different types of combat.

The capabilities of a company are expressed through the number of tanks and BMPs, the attack of which must be repelled while maintaining its combat effectiveness, e.g., without losing more than 50 percent of its forces and means and retaining command and control.

To Destroy Tanks:

$$K_t = (BP_{bmp} + BP_{rpg}) \times K_e / BP_{ptr}$$

To Destroy BMPs:

$$K_{bmp} = (BP_{bmp} + BP_{rpg}) \times K_e / (BP_{bmp\ pr} + BP_{ptrk\ pr})$$

Company fires capabilities in battle with enemy armored vehicles can be calculated using the following formula:

where

- ◆ K_t , K_{bmp} represent the number of enemy tanks (BMP) that can be destroyed.
- ◆ BP , BP_{pr} are the combat potential (CP) of the weapons and equipment in force-on-force [duel] combat of our side [BP] and the enemy [BP_{pr}] according to the different CP types (BP_{bmp} , BP_{rpg} , $BP_{bmp\ pr}$, $BP_{ptrk\ pr}$). ***Infantry fighting vehicles= bmp, shoulder-fired antitank weapons=rpg, ptrk=antitank guided missiles (ATGM), pr=enemy.***
- ◆ K_e is the coefficient of effectiveness of weapons in force-on-force [duel] combat.

1.3 Defensive Combat Capabilities of a Platoon and Their Calculation

Knowledge of combat capabilities allows the platoon commander to assign combat missions intelligently and correctly use weapons in combat.

The definition of fires capabilities includes the ability of the platoon to use its antitank weapons to destroy advancing tanks and other armored enemy targets, and to destroy personnel using small arms and other fires assets.

To Destroy Tanks:

$$K_T = 0.7(\sum BP_{Ni}) \times K_e \times K_{PN} / BP_{Tpr}$$

To Destroy BMPs:

$$K_{BMP} = 0.3(BP_{bmp} \times N_{bmp} + BP_{rpg} \times N_{rpg}) \times K_e \times K_{PN} / (BP_{BMPpr} + BP_{PTRKpr})$$

Platoon fires capabilities in battle with enemy armored vehicles can be calculated using the following formula:

where

- ◆ 0.7 is the portion of force-on-force [duel] combat weapons necessary for defeating enemy tanks (value obtained through trials).

- ◆ 0.3 is the portion of force-on-force [duel] combat weapons necessary for defeating enemy BMPs (value obtained through trials, meaning that 70 percent of fires will be used for fighting tanks and 30 percent with enemy BMPs).
- ◆ N_i is the number of friendly force-on-force [duel] combat weapons, according to their type (MT—tanks, Kbmp—BMP, Mrpg—RPG, and others).
- ◆ K_T, K_{BMP} —number of enemy tanks (BMP), which can be defeated, per weapon.
- ◆ BP_{pr} (enemy), BP are the combat potentials of the weapons in force-on-force [duel] combat of each side by type, per weapon.
- ◆ Ke is the coefficient of effectiveness of force-on-force combat weapons under different conditions, per weapon.
- ◆ K_{pN} is allowable level of losses, per weapon/personnel.

2. Methodology to Evaluate Company Capabilities to Repel the Enemy using Small Arms Fire

The mathematical expectation of damage inflicted on enemy personnel is the primary indicator of the capabilities of the platoon to repel the enemy using small arms fire.

The calculation is based on comparing the density of small arms fire of the opposing sides, expressed as the number of bullets per 1 meter of the front in a specified sector of fire in a given timeframe (1 minute).

The density of fire depends on the number of weapons, weapons types, rate of fire, and width of the area within which the fire is conducted.

The sequence of calculating company fire capabilities to repel the enemy using small arms fire is the following:

1. Calculate the number of automatic rifles, machine guns, and other small arms and their total combat rate of fire:

$$\Sigma BS_{VZ} = K_a \times BS_a + K_{p1} \times BSp1 + K_{p2} \times BSp2 + K_{p3} \times BSp3 + K_{SVD} \times BS_{SVD}$$

where

- ◆ ΣBS_{VZ} is the total combat company rate of fire.
- ◆ K_a —number of automatic rifles in a company.
- ◆ K_{p1} —number of machine guns RPK-74 in a company.
- ◆ K_{p2} —number of PKT [antitank Kalashnikov] machine guns in a company.
- ◆ K_{p3} —number of PKM [modernized Kalashnikov] machine guns in a company.
- ◆ K_{SVD} —number of SVD [Dragunov sniper rifle] in a company.
- ◆ BS_a —combat rate of fire for automatic rifles.
- ◆ $BSp1$ —combat rate of fire for RPK-74.
- ◆ $BSp2$ —combat rate of fire for PKT.
- ◆ $BSp3$ —combat rate of fire for PKM.
- ◆ BS_{SVD} —combat rate of fire for SVD.

2. Determine the total combat rate of fire considering personnel and weapons losses during enemy fire preparation actions (up to 20 percent):

$$\Sigma BS_{VZ}^P = \Sigma BS_{VZ} \times 0.8$$

3. Determine the width of the front of company fire support (ShF):

$$Sh_F = F + 0.5(P1 + P2)$$

where

- ◆ Sh_F is front width of a unit's fire support, in meters.
- ◆ F is the front of platoon stronghold, in meters.

◆ Sh in P2 are the distances of separation between neighboring units, in meters.

4. Calculate small arms fire density (PIOSO) per 1 meter of the front in 1 minute considering losses, N bullets/meters (number of bullets per one meter of the front):

$$\text{PIOSO} = \Sigma \text{BS}_{\text{vz}} / \text{Sh}_F$$

5. Determine enemy forces, which can advance toward the front of the company's fire support operations, calculating their total combat rate of fire and fire density per 1 meter of front considering losses (10 percent) sustained from artillery fire (similar method).

6. Compare friendly and enemy fire density, and draw conclusions.

Example calculation of fire capabilities of motorized rifle platoon [msv] on BMP using small arms fire to repel the enemy.

A motorized infantry company has AK-74—90 rifles, RPK-74—9, PKM—3, PKT—3, SVD—12.

1. Calculate the number of automatic rifles, machine guns, and other fires methods and their total combat rate of fire $\Sigma \text{BS}_{\text{vz}}$:

$$\Sigma \text{BS}_{\text{vz}} = 90 \text{AK} \times 100 + 9 \text{RPK} \times 1501 + 1 \text{PKM} \times 250 + 3 \text{PKT} \times 250 + 12 \text{SVD} \times 30 = 12210/\text{minute}$$

2. Determine the total combat rate of fire considering personnel and weapons losses during enemy fire (up to 20 percent):

$$\Sigma \text{BS}_{\text{vz}} = 0.8 \times 12210 = 9768/\text{minute}$$

3. Determine the front width of company fire support (Sh_F):

$$\text{Sh}_F = 1500 + 0.5(500+500) = 2000 \text{ meters}$$

4. Calculate small arms fire density (PIOSO) per 1 meter of front in 1 minute considering losses:

$$\text{PIOSO} = 9768/2000 = 5 \text{ bullets per minute per 1 meter of front}$$

5. Determine fire density of enemy forces per 1 meter of front considering losses (10 percent) from artillery fire:

Up to 2 motorized antitank units can advance within a 2000-meter front.

$$\text{PIOSO} = ((120 \text{M16} \times 100 + 36 \text{M249} \times 150 + 18 \text{M60} \times 250 + 24 \text{P}_{\text{BMP}} \times 250) \times 0.9) / 2000 = 13 \text{ bullets per 1 meter of front}$$

6. Compare fire densities $13/5 = 2.6$ (enemy fire density is 2.6 times greater).

Successful achievement of a combat objective is possible with a ratio of 3:1 and lower. In this instance, the established density of 3 to 5 bullets per minute per 1 meter of front supports a 50 percent defeat rate of advancing enemy infantry forces, and upon taking decisive action, the platoon can create the fire density of up to 15 bullets per minute, which supports an 80 to 90 percent defeat rate of attacking enemy infantry troops.

Thus, a motorized rifle company in the defense, using standard weapons and BMPs, is able to create fire density of over 3 bullets per minute per 1 meter of front (considering 30 percent losses), which is necessary to guarantee 50 percent losses against an enemy with three times the infantry force and to successfully repel attacks along the 2000 meter front with fire support.

It is most appropriate to calculate combat capabilities with the following conditions: level of enemy losses in an attack—0.35 (enemy refuses to continue the attack) and level of friendly defensive force losses—0.5 (combat capability limited).

Example calculation of platoon fire capabilities in a fight with enemy armored vehicles.

Initial data is BMP—3, RPG-7—3, M1 "Abrams"—3, IFV M-2 "Bradley"—4, ATGM "Drakon"—3.

Composition of motorized infantry platoon—3 BMP.

Tank platoon—3 tanks.

Calculating the fire capabilities of a platoon in a fight with enemy armored vehicles:

$$K_{bmp} = 0.3(BP_{bmp} \times N_{bmp} + BPrpg \times Nrpg) \times K_e \times K_{pn} / (BP_{BMPpr} + BP_{PTRKpr})$$

$$K_{bmp} = 0.3(0.53 \times 3 + 0.07 \times 3) \times 3 \times 0.5(0.55 + 0.32) = 2.8 \text{ (three IFV)}$$

$$K_t = 0.7(\sum BP_{Ni}) \times K_e \times (K_{PN} / BP_{Tpr}) = 0.7(0.5 \times 3 + 0.7 \times 3) \times 2 \times 0.5 / 1.47 = 0.86 \text{ (up to 1 tank)}$$

Thus, the motorized rifle platoon in the defense is able to defeat 3 IFVs during defensive operations and 1 tank, while maintaining the platoon's combat capability (losses no more than 50 percent).

Example calculation of fire capabilities of a motorized rifle platoon in repelling the enemy using small arms fire.

Motorized rifle platoon has AK-74—22, RPK-74—3, PKM—1, SVD—4.

1. Calculate total combat platoon rate of fire ΣBS_{vz} :

$$\Sigma BS_{vz} = 22AK \times 100 \text{ per minute} + 3RPK \times 150 \text{ per minute} + 1PKM \times 250 \text{ per minute} + 4SVD \times 30 \text{ per minute} = 3020 \text{ per minute}$$

2. Determine total combat platoon rate of fire considering losses during period of enemy fire preparation (losses up to 20 percent):

$$\Sigma BS_{vz}P = \Sigma BS_{vz} \times 0.8 = 3020 \times 0.8 = 2416 \text{ per minute}$$

3. Determine width of the front of fire support of the platoon:

$$Sh_F = F + 0.5(P_1 + P_2) = 400m + 0.5(300m + 300m) = 700m$$

4. Determine small arms fire density per 1 meter of front in 1 minute considering losses:

$$PIOSO = \Sigma BS_{vz} / Sh_F = 2416 / 700 = 3.45 \text{ bullets per minute per 1 meter of front}$$

5. Calculate enemy fire density per 1 meter of front considering losses from friendly artillery fire (up to 10 percent).

Up to 2 motorized infantry platoons and 1 to 2 tank platoons, which are capable of producing fire density of 13 bullets per minute per 1 meter and more (excluding tank machine guns) can attack along a front of 700 meters.

$$PIOSO_{pr} = ((44M16 \times 100 + 12M249 \times 150 + 6M60 \times 250 + 8P_{BMP} \times 250) \times 0.9) / 700 = 12 \text{ bullets per minute per 1 meter of front}$$

6. Compare fire densities $12/3 = 4:1$.

Using Table 4, we find the correlation of 4:1 and determine that the platoon, in the defense and under given conditions, can damage the enemy by 30 percent, while sustaining 84 percent losses of friendly personnel. Successful achievement of combat objectives is possible with this ratio and less. In this case, the established density of 3 to 5 bullets per minute per 1 meter of front supports a 50 percent defeat rate of advancing enemy infantry forces, and upon taking decisive action, the platoon can create the fire density of up to 15 bullets per minute, which supports an 80 to 90 percent defeat rate of attacking enemy infantry forces.


This way, the BMP motorized rifle platoon in the defense, using regular weapons and BMPs, is capable of producing fire density of 3 bullets per minute per 1 meter of front (considering 20 percent losses). This is necessary to guarantee 50 percent losses in an enemy with three times the infantry force and to repel attacks successfully along a 700m fire support front, while defending the stronghold along a front of up to 400 meters. 

Table 4. Losses of Offensive and Defensive Sides Depending on the Correlation of Forces and Means

TIME OF DAY	SPEED OF OFFENSIVE KM/H	SIDES	LOSSES BASED ON GIVEN FORCE AND MEANS CORRELATIONS BY PERCENTAGE					
			1:1	2:1	3:1	4:1	5:1	6:1
DAY	5	Offense	100	88	49	30	18	10
		Defense	20	28	56	84	100	100
	10	Offense	100	41	30	20	15	11
		Defense	60	20	33	46	60	73
NIGHT	5	Offense	100	62	37	26	18	13
		Defense	30	24	42	60	77	85
	10	Offense	70	33	21	15	11	9
		Defense	60	15	14	32	41	49

Endnotes

1. Russian Ministry of Defense, "Соотношение Сил и Средств" [Correlation of Forces and Means], *Военная Энциклопедия* [Military Encyclopedia], Volume 7 (Moscow: Voenizdat, 2003), 583.
2. Michael Chichenski, "Soviet Correlation of Forces and Means" (class lecture, U.S. Army Russian Institute, Garmisch, Germany 1982).
3. Photo by Vyacheslav Argenberg / <http://www.vascoplanet.com/>, edited by MIPB Staff.
4. Russian Ministry of Defense, *Учебно-методические Материалы по предмету Тактическая Подготовка* [Teaching and Methodological Materials for the Subject of Tactical Preparation] (Barnaul: Altai State Technical University by I. I. Polzuno, 2017), 24; Russian Ministry of Defense, *Боевые Уставы* [Combat Regulations] (Moscow, 2014), 7; and I. N. Vorobyev, *Тактика- искусство боя* [Tactics: The Art of Combat] (Moscow: Combined Arms Academy of the Russian Federation, 2002), 70, 117, 199, 212, 228, 232, 233, 279, 289, 357, 359, 616, 634.
5. Qualimetry assesses the quality of a commodity, service, or system. Quality is defined as the "aggregate of properties...associated with the result of consuming the object." Clint Reach, Vikram Kilambi, and Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means* (Santa Monica, CA: RAND Corporation, 2020), 71.
6. Ibid., 72–73.
7. V. N. Dorokhov and V. A. Ischuk, "Combat Potentials of Subunits [Battalion-Level] as an Integral Criterion for Assessing Combat Capabilities of Combat Formations and Combat Effectiveness of Arms and Military Equipment," trans. Clint Reach, *News of the Russian Academy of Missile, Rocket, and Artillery Sciences* [RARAN] 4, no. 99 (2017): 27–36.
8. Ibid.
9. Ibid.
10. Ibid.
11. V.A. Valezhanin and A.A. Tarchishnikov, *Боевые возможности мотострелкового (танкового) взвода, отделения (танка) и их расчет* [Combat Capabilities of the Motorized Rifle (Tank) Platoon, Subunits (Tank), and Their Calculation] (Minsk: Belarus National Technical University, 2011).
12. Ibid., 4.
13. Ibid., 4–5.
14. Chichenski, "Soviet Correlation of Forces and Means."
15. Reach, Kilambi, and Cozad, *Russian Assessments and Applications*, 94.
16. Vorobyev, *Tactics: The Art of Combat*, 633–634.
17. Lester W. Grau and Charles K. Bartles, *The Russian Way of War: Force Structure, Tactics and Modernization of the Russian Ground Forces* (Fort Leavenworth, KS: Foreign Military Studies Office, 2018), 58, <https://community.apan.org/wg/tradoc-g2/fmso/p/fmso-bookshelf>.
18. William Shakespeare, *The Tempest*, act 2, sc.1.
19. Valezhanin and Tarchishnikov, *Combat Capabilities*.
20. Comments in bold italics in Annex A are the authors' explanatory notes.

Dr. Lester Grau is a Vietnam veteran, Soviet foreign area officer, retired U.S. Army lieutenant colonel, and currently the research coordinator for the Foreign Military Studies Office, Fort Leavenworth, KS. He holds a bachelor's degree and master's degree in international relations and has a doctorate in military history. He is also a graduate of the U.S. Army Defense Language Institute (Russian) and the U.S. Army's Institute for Advanced Russian and Eastern European Studies. He is the author of 13 books and more than 250 published articles.

Mr. Clint Reach is a policy analyst at the RAND Corporation. He holds a bachelor's degree in management information systems and a master's degree in political science from Kansas State University. He also holds a master's degree in Russian and Eurasian studies from Johns Hopkins University School of Advanced International Studies. Mr. Reach served for 9 years in the U.S. Navy as a Russian linguist. Before joining RAND in 2015, Mr. Reach worked for a short time at the Office of the Secretary of Defense for Policy–Russia, Ukraine, and Eurasia.

Explosive Ordnance Disposal & Intelligence: Exploring Gaps between Mutually Supporting Communities

BY Lieutenant Colonel Philip D. Cordaro

Introduction

A significant gap exists between the military intelligence and explosive ordnance disposal (EOD) communities that prevents the realization of each other's full potential. It lies in the area of science and technology under technical intelligence (TECHINT) where subject matter expertise and intelligence often overlap in a confusing gray area. The EOD community has information and expertise on foreign weapon systems that it does not know are valuable to military intelligence, and the military intelligence community has access to information on foreign weapon systems that it does not realize is vital to EOD. While the importance of the communities coordinating with one another has been recognized since EOD's establishment in the 1940s and has been captured in multiple versions of TECHINT field manuals, regulations, and publications over the years, a gap still exists.¹ It can only be closed through a concerted effort to update education, training, doctrine, and manning to reflect and codify this mutually beneficial relationship of increasing importance as we shift our focus to large-scale combat operations.

Operation-Dependent Integration

During the counterinsurgency operations in Iraq and Afghanistan, a link between the EOD and military intelligence communities emerged because the intelligence community required robust counter-improvised explosive device (C-IED) acumen to identify trends and assist with their predictive analysis. That expertise was only available through EOD preserving and exploiting components related to the manufacture and employment of improvised explosive devices. The concepts of "attack the network" and "counter threat network" were captured in multiple North Atlantic Treaty Organization (NATO), joint, and Service doctrinal publications, but they were still perceived to apply only to

C-IED. Because of the perception that EOD and exploitation are solely tied to C-IED, the military intelligence community still does not associate the EOD mission with traditional intelligence collection activities. As a result, EOD's level of integration with the intelligence community fluctuates greatly depending on the type of operation being conducted.

During EOD school, the EOD community does not teach its relationship with military intelligence. Additionally, it provides minimal follow-on training on intelligence, other than how to conduct a TECHINT report for first-seen ordnance, and it does not openly share its operational reporting. The *Generic Intelligence Requirements Handbook for Joint Service EOD*, which the Naval EOD Technology Division published in January 2004, contains best practices for recording first-seen materiel but only for the purposes of developing EOD render-safe procedures.² When deployed, EOD units are often approached by agencies from across the broader intelligence community that are looking for specific information on ordnance, weapon systems, and associated components. EOD units' support to those requests varies because the units often do not have visibility into what those agencies will do with the data, which results in the EOD units' lack of appreciation for the impact of their reporting.

Joint Exploitation

In the Universal Joint Task List, several tasks now link EOD to exploitation, battlefield foreign materiel acquisition, and scientific and technical intelligence.³ Additionally, JP 2-01, *Joint and National Intelligence Support to Military Operations*, Appendix F, describes supporting intelligence through joint multidiscipline exploitations.⁴ It underscores how critical information collected through EOD operations feeds the intelligence cycle.

Threats



**Defense
Intelligence
Agency**

Conventional

- Automated Systems
- Documents and Media
- C&E Equipment
- Medical Materiel
- Mobility Systems
- Munitions
- Weapons



**Defense
Threat Reduction
Agency**

Unconventional

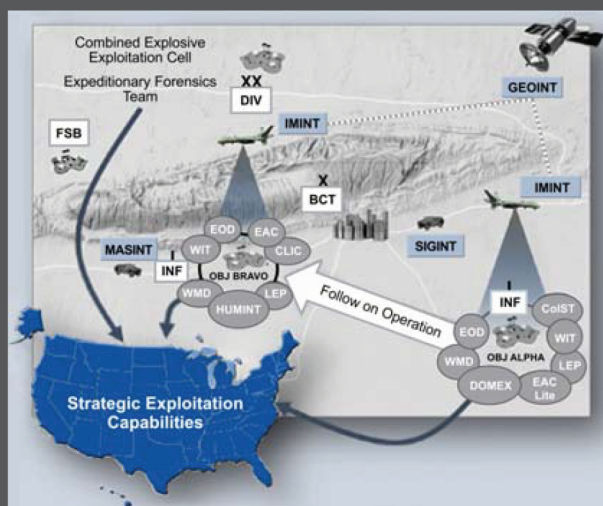
- Chemical
- Biological
- Radiological
- Nuclear
- IEDs
- Modified Munitions and Weapons

Expeditionary Exploitation



Collect, Exploit, Analyze

DoD Exploitation Capabilities



Organized under a Joint Task Force with Reachback

Outcomes

- Force Protection
- Targeting
- Signature Characterization
- Component and Material Sourcing
- Support to Prosecution
- Support to RDT&E
- Support to Special Activities

Joint exploitation may be conducted simultaneously at all three levels of warfare. While DIA primarily addresses conventional threats and DTRA primarily addresses unconventional threats, they and other CSAs may address threats in both areas.

Legend

BCT	brigade combat team	GEOINT	geospatial intelligence
C&E	collection and exploitation	HUMINT	human intelligence
CLIC	company level intelligence cell	IED	improvised explosive device
CoIST	company intelligence support team	IMINT	imagery intelligence
CSA	combat support agency	INF	infantry
DIA	Defense Intelligence Agency	LEP	law enforcement professional program
DIV	division	MASINT	measurement and signature intelligence
DoD	Department of Defense	OBJ	objective
DOMEX	document and media exploitation	RDT&E	research, development, test, and evaluation
DTRA	Defense Threat Reduction Agency	SIGINT	signals intelligence
EAC	echelons above corps (Army)	WIT	weapons intelligence team
EOD	explosive ordnance disposal	WMD	weapons of mass destruction
FSB	forward support battalion		

Over numerous deployments as part of EOD and C-IED task forces to Iraq and Afghanistan, I witnessed EOD teams identify a unique device or piece of ordnance that we thought would be of interest to someone in the intelligence community, but we did not know who. We had no familiarization training on intelligence requirements. The first time I detected a demand signal for EOD reporting was during a senior leader tour in Washington, DC, before an EOD battalion deployment to Afghanistan in 2013. Even then, the requirements were vague. No one provided a list of ordnance items that the intelligence community wanted to acquire, but we did at least come away with points of contact for when we had questions. Once deployed, our organic and contracted intelligence analysts at the battalion were extremely proficient at tracking trends but were disconnected from the larger intelligence collection apparatus. When we had questions about specific incidents, I would contact national-level intelligence agencies for answers because it seemed there was no intelligence organization at an echelon in between that understood the link between the communities. Since I arrived at the Defense Intelligence Agency's (DIA's) Joint Foreign Materiel Program Office (JFMPO) in 2017, intelligence community elements have started to leverage JFMPO as the primary link for tracking down EOD reports and points of contact. This was not by design but rather born out of necessity.

Congressional Support

Congressman Rick Crawford (who served as a U.S. Army EOD technician) included language in the FY20 National Defense Authorization Act requiring the Department of Defense (DoD) to conduct a study of the gap between the EOD and intelligence communities. He sent congressionally directed actions to the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), Foreign Materiel Program Director, requiring an analysis of the current EOD, Foreign Materiel Program, and intelligence relationship and the establishment of an explosive ordnance intelligence sub-discipline under TECHINT.⁶ He also sent action memorandums to the Army G-2 and OUSD(I&S) on specific aspects of the relationship between the communities.

These actions by Congress, OUSD(I&S), and the Joint Staff are driving a deeper study into the relationship gap that could result in a significant change in the way the two communities interact in the future. Although initial requests from Congressman Crawford focused on using EOD technicians as intelligence analysts, the recent FY20 National Defense Authorization Act language and congressionally directed actions to OUSD(I&S) centered on the establishment of explosive ordnance intelligence and increased coordination between the EOD and intelligence communities.

In March 2020, OUSD(I&S) directed the U.S. Navy to conduct a study on the current relationship between the two communities and to propose recommendations on how to improve collaboration.⁷ Following the 3-month study that canvassed combatant command (COCOM), combat support agency, and Service EOD and intelligence staffs, the U.S. Navy-led group sent OUSD(I&S) multiple recommendations to facilitate greater coordination between the communities. OUSD(I&S) recently forwarded the recommendations to Congressmen Crawford.

Role of the Joint Foreign Materiel Program Office

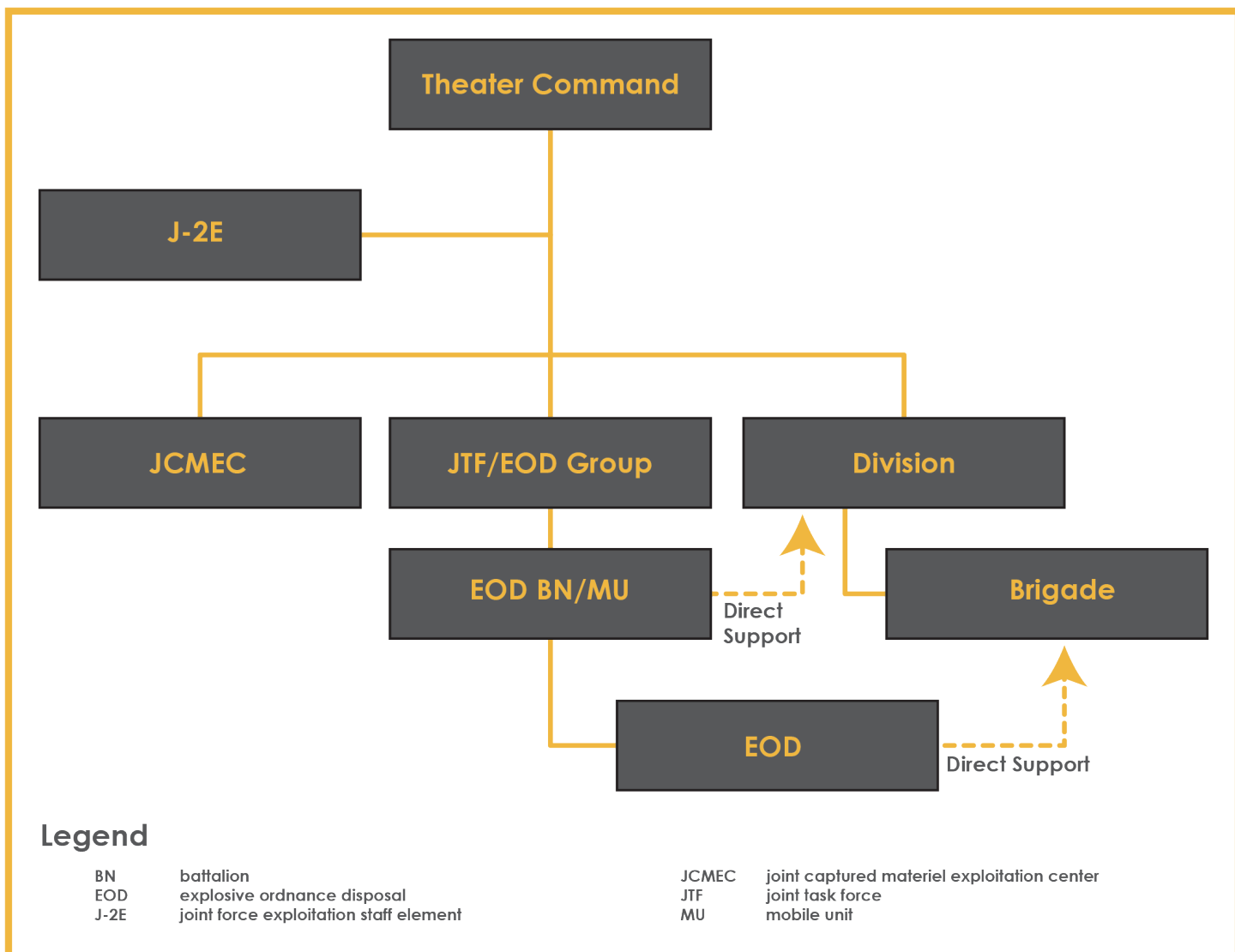
DIA's JFMPO is responsible for managing the DoD's foreign materiel enterprise. This responsibility includes—

- ◆ Validating all foreign materiel requirements.
- ◆ Deconflicting acquisitions.
- ◆ Coordinating exploitations.
- ◆ Maintaining visibility of all subsequent countermeasures developed by the test and evaluation community.

JFMPO's Expeditionary Operations section contains a joint captured materiel exploitation center (JCMEC), which stands up at the behest of a COCOM commander during named operations for the exploitation of materiel recovered or captured on the battlefield and the coordination to transport it back to national-level exploitation laboratories. If a COCOM commander requires an in-theater foreign materiel exploitation capability, JFMPO deploys the JCMEC under the J-2X, J-2E, or J-23. A deployed JCMEC includes experts from across the intelligence community and a company from the 203rd Military Intelligence Battalion (TECHINT) to collect foreign materiel from across the battlefield. JP 3-42, *Joint Explosive Ordnance Disposal*, explains the relationship between a JCMEC and an EOD headquarters. Every JCMEC level-one collection team requires EOD support to conduct its mission.

JFMPO is also responsible for establishing and deploying expeditionary exploitation teams in as little as 24 hours to support requirements from the defense attaché office and COCOM commander. JFMPO tailors the teams based on the target and location. It can leverage subject matter experts from more than 25 organizations and agencies to support those requests. Regardless of the target, the team will always incorporate EOD support and capture reporting in DIA-published intelligence information reports.

When not deployed, JFMPO's expeditionary operations team coordinates with either the J-2X or the J-23 section in each COCOM to disseminate requirements to the operational forces. In 2018, JFMPO recognized the classification of the list was limiting its dissemination to the EOD teams and worked with the Service intelligence centers to develop an unclassified list of requirements that EOD teams could



Explosive Ordnance Disposal and Captured Materiel Relationships⁸

carry with them on missions. The list also includes contacts for JFMPO and experts at the Service intelligence centers. Initially titled the “do not destroy” list, it is now referred to as the “most wanted ordnance” list. Administrators for the EOD Information Management System (EODIMS), which is the joint system of record for all EOD reporting, also plan to add it as a reference.

In support of its wider Foreign Materiel Program governance role, JFMPO also canvasses more than 20 Service, COCOM, and combat support agency-level organizations for each one’s top 50 foreign materiel acquisition priorities. Although JFMPO primarily collects that data to aggregate into the DoD’s top 50 foreign materiel acquisition priority list, each submission can also be used by military intelligence personnel preparing EOD units to deploy in support of a specific command or to a particular region. JFMPO is also coordinating foreign materiel acquisition requirements and opportunities with the COCOMs to integrate them further into the Foreign Materiel Program activities that directly align with their priorities. Because of the way most

COCOMs develop their priorities in the J-3, J-5, and J-58 sections, it is critical for the J-2X or J-23 section to synchronize Foreign Materiel Program activities across the COCOM. Although foreign materiel acquisition activities are an intelligence function, the priorities, funding, and resulting exploitation are relevant and of significant interest to many other offices.

EOD Reporting

In early 2020, EODIMS administrators coordinated with JFMPO to reclassify the database from a Defense Warfighting Mission Area to a Defense Intelligence Mission Area.⁹ This change took effect in June 2020 and will lead to changes that will allow intelligence analyst search engine tools on Secret and Top Secret networks to query EODIMS data and reporting. EOD TECHINT reports provide actualities on foreign materiel that can be used to positively confirm or deny assessments. The analysts will not have access to render-safe procedures or disposal details but will be able to find EOD reports to use as sources and provide more depth to their analysis. This is a crucial step toward getting the wider

intelligence community to recognize the unique value EOD reporting provides to satisfy the intelligence community's collection requirements.

JFMPO engages in more direct messaging efforts to the joint Service EOD community during technical conferences, predeployment training, professional military education courses, leader development opportunities, and deployments. These efforts have expanded the EOD community's understanding of its symbiotic relationship with the intelligence community. To capitalize fully on the relationship, military intelligence officers who are integrated with these units still need a better understanding of how EOD exploitations are useful to the intelligence community as raw reporting. If the national-level intelligence community understands and values EOD's access and reporting, but the military intelligence units on the battlefield with EOD do not understand its value, the communities will continue to have a significant gap. JFMPO's current engagement strategy focuses on reaching the intelligence professionals assigned to joint Service EOD units. These personnel are the true lynchpins who, with greater understanding, can best champion the relationship between the military intelligence and EOD communities.

Unified Exploitation Community of Interest

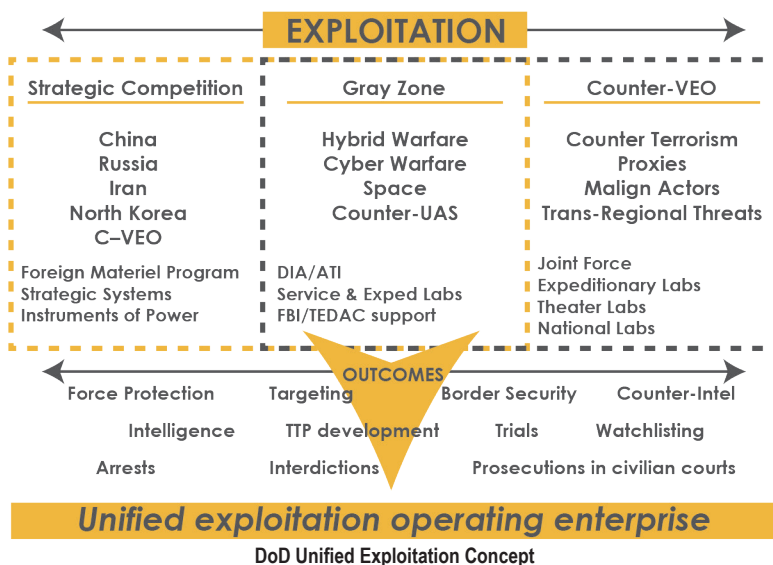
Unified exploitation is a concept that has existed at least since the 2012 West Point study on Combined Joint Task Force Paladin's Exploitation Systems,¹⁰ but it did not gain traction until DoD senior leaders attending a U.S. Special Operations Command (SOCOM) seminar in 2018 recognized the gap and recommended combining the various DoD exploitation efforts into one cohesive community. Since then, OUSD(I&S) and the Joint Staff J-5 have led an effort to establish the DoD unified exploitation community of interest. With an understanding of all the desired outcomes of exploitation, the community of interest developed the term "collected exploitable material" (CEM) to encompass: *all material and/or materiel in the possession of the Department of Defense (DoD), regardless of its classification or how it was obtained, that could be exploited in support of Department and national interests.*¹¹

The community of interest is coordinated around five lines of effort (LOEs):¹²

- ◆ LOE 1: Policy and Doctrine.
- ◆ LOE 2: Processes.
- ◆ LOE 3: Technology and Architecture.
- ◆ LOE 4: Capabilities and Resources.
- ◆ LOE 5: Information Sharing.

The unified exploitation community of interest's two desired end states are¹³—

- ◆ Under the umbrella of a unified exploitation architecture, all collected exploitable material is fully exploited in a timely and accurate manner to be discoverable by, and shareable with, all authorized customers.
- ◆ The processes for unified exploitation of collected exploitable material are transparent and collaborative, resulting in efficient, effective, and sustainable mission activities regardless of their location in the unified exploitation enterprise.



In the last 15 years, Services and combatant commands have stood up their own exploitation laboratories to meet their various mission requirements. There are currently separate U.S. Army, U.S. Navy, U.S. Marine Corps, SOCOM, and DIA exploitation laboratories; however, there are no exploitation or reporting standards across the laboratories, and they do not use a common database. This approach does not allow for a DoD common operational picture of all exploitable material collected by DoD elements. Additionally, problems often arise between exploitation entities because of the classification of collected material and some organizations' inability to share data because of the classification associated with how they collected it.

The Secretary of Defense signed a memorandum in January 2020 to eliminate issues with the over-classification of collected exploitable material. According to the memorandum, all newly acquired raw and unexploited collected exploitable material that the U.S. Armed Forces capture, collect, or handle during military operations is to be unclassified unless sensitive sources, methods, or activities were used to acquire the collected exploitable material.¹⁴ The DoD unified exploitation community of interest is also embedded within the larger U.S. Government battlefield evidence community of interest, the NATO Technical Exploitation Group, and the NATO Battlefield Evidence Working Group.

Conclusion

The fact that we are having the conversation and looking for ways to better integrate the EOD and military intelligence communities is a step in the right direction. The issue is starting to receive the level of visibility required to drive the necessary institutional changes. As integration efforts continue to move forward, it will be crucial for the EOD and military intelligence communities to establish regular opportunities for greater communication. Large-scale combat operations are the driver to better coordinate our efforts. EOD should start training Soldiers on their roles within intelligence earlier in their careers, and the intelligence community should recognize the value EOD Soldiers can provide to intelligence collection and analysis efforts. Only when the communities start to gain a better appreciation for their mutually supporting capabilities will we be able to build a bridge over the gap to tighten our collaborative efforts. ✨


Endnotes

1. Department of the Army, Field Manual 30-16, *Technical Intelligence* (Washington, DC: U.S. Government Publishing Office, 31 August 1972 [obsolete]).
2. Department of the Navy, *Generic Intelligence Requirements Handbook for Joint Service EOD* (16 January 2004).
3. Office of the Chairman of the Joint Chiefs of Staff, Universal Joint Task List, accessed 19 August 2021, <https://www.jcs.mil/Doctrine/Joint-Training/UJTL/>.

4. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 5 July 2017).
5. Ibid., F-2, adaptation of original figure.
6. Representative Rick Crawford letters to Office of the Under Secretary of Defense for Intelligence and Security, Foreign Materiel Program Director, 3 February 2020.
7. Office of the Under Secretary of Defense for Intelligence and Security memorandum for the Director of Navy Staff, Subject: Explosive Ordnance Disposal Intelligence Gaps, 25 March 2020.
8. Office of the Chairman of the Joint Chiefs of Staff, JP 3-42, *Joint Explosive Ordnance Disposal* (Washington, DC: The Joint Staff, 9 September 2016), II-18, adaptation of original figure.
9. The Explosive Ordnance Device Information Management System requested a mission area change from the Warfighter Mission Area to the Department of Defense (DoD) portion of the Defense Intelligence Mission Area supporting the following domains: exploitation, mission management, dissemination, collection, analysis, and production. The change, in accordance with DoD Information Technology Portfolio Repository Guidance and Secretary of the Air Force, was approved and is effective as of 24 June 2020.
10. Department of the Army, *CJTF Paladin Exploitation Systems: The Evolving Role in Unified Exploitation* (Annapolis, MD: West Point, 19 October 2012).
11. Department of Defense, *Implementation Plan to the Department of Defense Strategy for Unified Exploitation* (August 2020).
12. Ibid.
13. Ibid.
14. Ibid.

LTC Philip Cordaro is the Commander, 303rd Explosive Ordnance Disposal Battalion, at Schofield Barracks, HI. Before taking command, he was assigned to the Defense Intelligence Agency's Joint Foreign Materiel Program Office where he was the Deputy Director for Enterprise Operations and the U.S. Foreign Materiel Program Head of Delegation.


CW2 CHRISTOPHER G. NASON




MILITARY INTELLIGENCE LIBRARY


Options Available

LIBRARY CATALOG




DATABASES






USAICoE WRITING PROGRAM

EBOOKS



RESEARCH GUIDES



The MI Library website is located at:
<https://auls.insignalls.com/Library/Home?LibraryID=0010&Language=English>



700-Series Battalion Conducts External Evaluation to Improve Mission Essential Task Proficiency

by Major George Gurrola, Captain Mason Lockey,
and Chief Warrant Officer 3 Katy Tomlinson

Editor's Note: Some figures in this article were abbreviated because of their size. The complete figures can be found with the web version of the article at <https://mipb.army.mil>.

Introduction

As the U.S. Army continues to emphasize lethality and readiness, military intelligence (MI) units must focus on sustaining technically and tactically proficient teams and Soldiers. An important aspect of preparing for current and future operations is to achieve and sustain a high degree of training proficiency in the operational domain. From 24 to 28 August 2020, the 717th MI Battalion (BN), 470th MI Brigade-Theater (MIB-T), conducted an external evaluation (EXEVAL) to validate both the battalion's and the companies' mission essential task (MET) proficiency. The battalion's EXEVAL is challenging because of its operational control (OPCON) and administrative control (ADCON) relationships (Figure 1). The battalion planned and simultaneously executed several training and battle rhythm events, each geared toward gaining an honest MET proficiency assessment. Using the training and evaluation outlines (T&EO), the 717th MI BN conducted the first cited 700-series battalion assessment of the METs to thoroughly evaluate its daily contribution to mission.

This article starts with an overview of doctrine as it pertains to EXEVALs. It also provides "a way," or framework, to conduct a 700-series battalion EXEVAL. The EXEVAL trained, certified, and validated the battalion's and companies' MET proficiencies. The training event also facilitated the collaboration between the brigade and battalion at a critical transition period and amid the coronavirus disease 2019 (COVID-19) pandemic. More importantly, the EXEVAL produced significant outputs, such as the fiscal year 2021 (FY21) unit training plan (UTP) and the training methodology necessary to sustain a T-level proficiency across all METs.

External Evaluation Design, A Way

The EXEVAL design sought to incorporate both objective and subjective criteria. FM 7-0, *Training*, specifies that EXEVALs "are scenario-driven evaluations of a unit's training proficiency conducted by leaders from outside the evaluated unit's chain of command. The commander two levels above the evaluated unit directs and resources the external evaluation."¹ In this case, the 470th MIB-T was the higher headquarters that trained and certified external observer

coach/trainers (OC/Ts) to execute the EXEVAL and provide objective and subjective feedback. The objective criteria used for the EXEVAL were primarily the battalion's mission essential task list (METL) tasks and its T&EOs. Evaluators also used the individual critical task lists to observe and evaluate individual tasks as either GO or NO-GO. The evaluators assessed the battalion's METL, which consisted of—

- ◆ MET 1: Conduct Mission Command.
- ◆ MET 2: Direct Operation Intelligence Activities.
- ◆ MET 3: The Sustainment Warfighting Function.

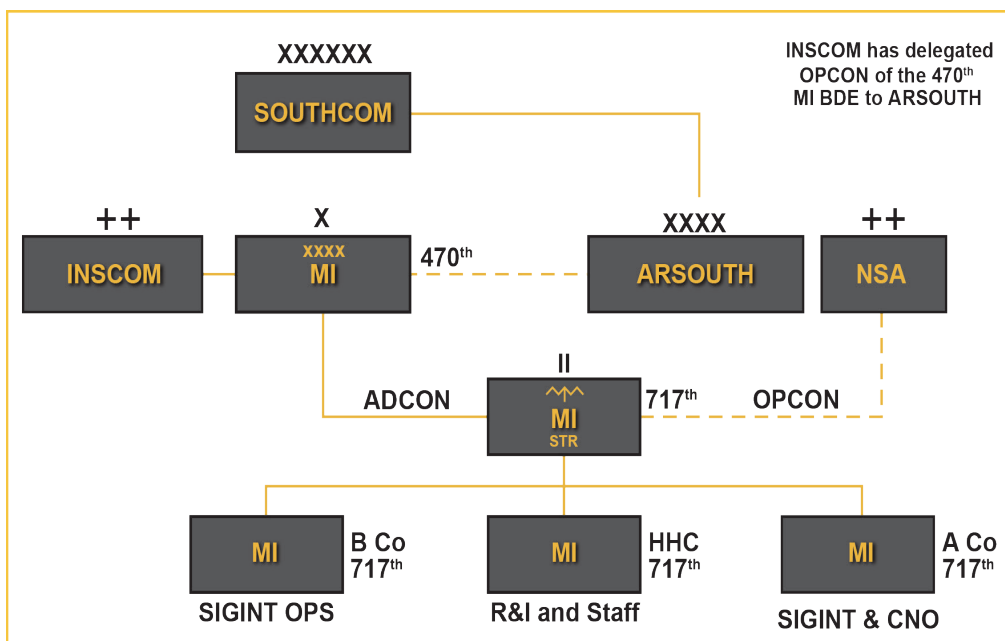


Figure 1. 717th MI BN, 470th MI Brigade Task Organization

To test MET 1, the event focused on the evaluation of the battalion's execution of the military decision-making process (MDMP) on the FY21 UTP. To test MET 2 and the execution of global cryptologic operations, the battalion was evaluated on 26 separate mission briefs, its Joint Qualification System progression, and other routine site events. To evaluate MET 3, the battalion planned and executed the Junior Leader Development Course (JLDC) and conducted sustainment support operations. Evaluators used task proficiency criteria and standards to measure proficiency.

While the EXEVAL used objective criteria to evaluate task proficiency, it also allowed brigade leaders to provide subjective feedback. The evaluators provided input based on their personal experiences and observation, allowing leaders across the brigade to add value to the exercise.

The EXEVAL schedule design was to validate both the battalion's and the companies' MET proficiency by using the

daily battle rhythm events. In this case, the EXEVAL leveraged routine training events that were originally scheduled across 2 weeks. However, the lack of evaluators and their availability narrowed the schedule to 1 week. Figure 2 shows the first 2 days of the schedule of events across time and space. The schedule is color-coded by MET and provides predictability for both the OC/T and those being evaluated. Overall, the condensed schedule stressed the battalion's systems and processes while gaining an honest objective assessment from the brigade evaluators.

Military Decision-Making Process on the FY21 Unit Training Plan

As part of exercising the battalion's MET 1, the 717th MI BN deliberately developed and implemented the battalion's FY21 UTP and long-range calendar during the EXEVAL. The battalion staff used the MDMP to develop the UTP and provide maximum predictability to the formation. It is

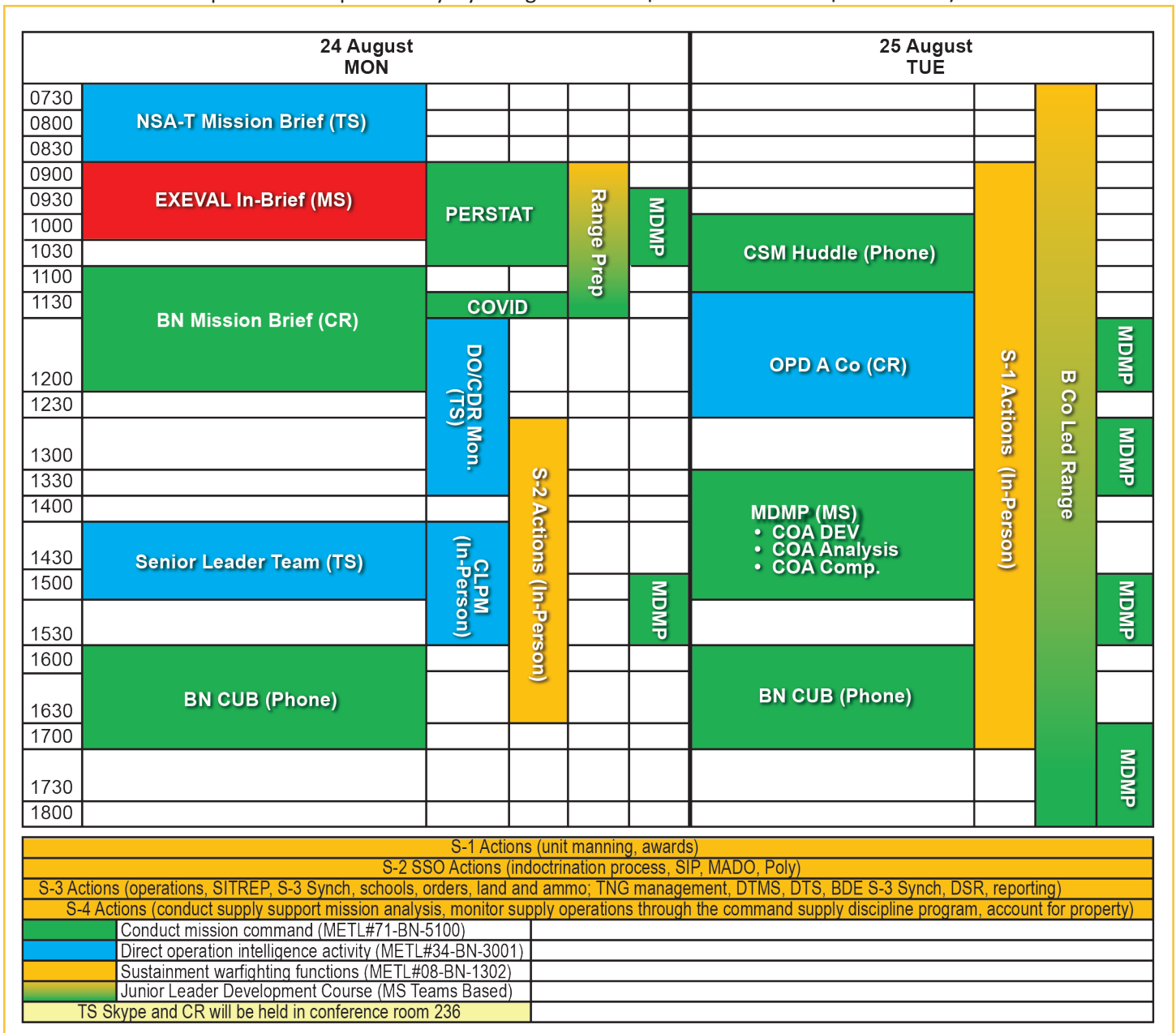


Figure 2. External Evaluation Schedule

important to note that many individuals on the staff had not formally participated in an MDMP or had limited experience. In preparation for the week of execution, the battalion's executive officer led the staff through an MDMP education session. The staff discussed the seven steps of MDMP, including key inputs and outputs. ADP 5-0, *The Operations Process*, states, "successful planning requires the integration of both conceptual and detailed thinking."² Because of the timeline, the staff placed an emphasis on mission analysis, course of action (COA) development, COA analysis, and rehearsals. As the chief of staff, the executive officer managed and coordinated the staff's work while also providing quality control.

Critical to the execution of the MDMP on the UTP was the background knowledge taught in the U.S. Army Command and General Staff College's "M100: Training and Deployment Operations" module. The module requires students to conduct a training requirements analysis while applying doctrine. The MDMP on the UTP was essential in understanding how to integrate doctrinal concepts into the battalion's collective and individual training strategy.³

The following week, the process began with the receipt of the mission and the battalion commander's guidance, which called for the battalion to focus on the core METs. The commander's guidance was for the staff to focus on developing a UTP by "doing less, better." As part of the MDMP, the commander asked the staff to develop two COAs. The first COA was to develop a focus on "evolution," that is, the evolution of the previous year's UTP, and to consider the limitations and impacts of the COVID-19 environment, whereas the second COA, "COA Revolution," would allow the staff to develop a new plan by adjusting the battle rhythm and training requirements and methodologies as they saw fit.

The battalion ensured the incorporation of bottom-up feedback and staff analysis. The company commanders

provided their input to the UTP COA and identified numerous limitations and constraints. The staff identified specified and implied tasks. This would create the opportunity to discuss and develop solutions and to better prioritize training. The executive officer continued to lead the process, covering the fiscal year calendar quarter-by-quarter and facilitating the staff to identify and recommend training. As a result, the battalion's collective and individual training events were removed, added, or shifted from the calendar; this created more white space, flexibility, and ultimately predictability for the companies.

In Figure 3, the FY21 717th MI BN line of effort training strategy displays the UTP over time. For purposes of the EXEVAL, the MDMP concluded with COA approval. Through the process, the following areas were addressed:

- ◆ The development of new battalion METs would be in line with higher headquarters and company-level missions.

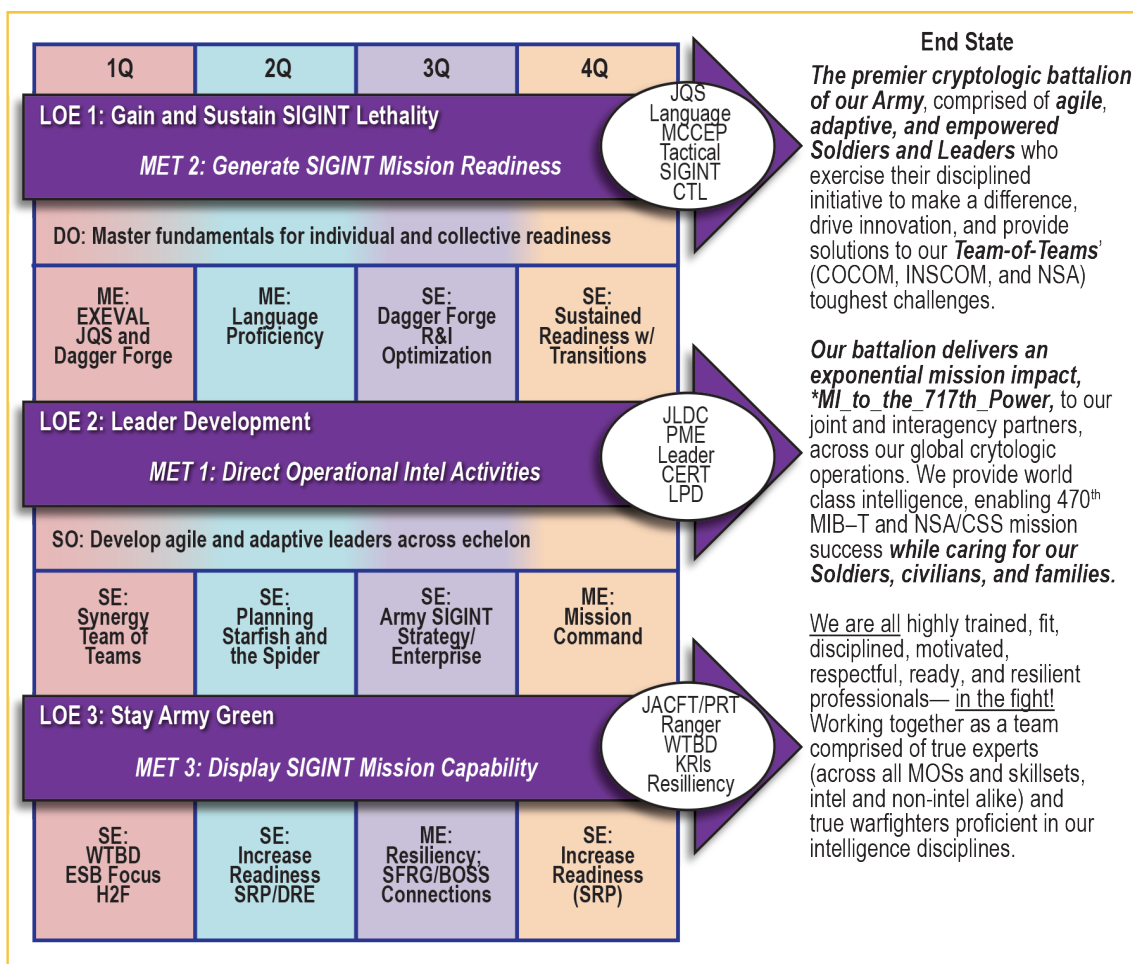


Figure 3. FY21 717th MI BN Line of Effort Training Strategy

- ◆ Companies providing support to the National Security Agency (NSA)-Texas would be re-task-organized, adding a platoon to each company.
- ◆ The reception and integration process would be improved to decrease a Soldier's NSA out-of-access time.

- ◆ Sergeant's Time Training and Warrior Task and Battle Drills would focus on Expert Soldier Badge tasks.
- ◆ Company missions/training would be protected.
- ◆ Language training would become a priority following the NSA's reconstitution after COVID-19 restrictions.
- ◆ Tactical driver training would be eliminated.
- ◆ Range requirements would be reduced for Soldiers in line with the tables of distribution and allowances.

Battalion Junior Leader Development Course

The battalion also executed its JLDC to train and prepare junior leaders to assume duties and responsibilities of a noncommissioned officer (NCO) in the U.S. Army. The battalion's most experienced NCOs run the 1-week course, focusing on mentorship and increasing enlisted leadership proficiency. This opportunity provided every Soldier the chance to test their mettle and leadership skills and to better understand the decision-making processes. Figure 4 displays 2 days of the JLDC execution timeline.

The battalion leveraged this event during the EXEVAL and gained helpful outside viewpoints on how to improve future iterations of JLDC. For one, external evaluators praised the hands-on approach by the trainers on topics such as time management and delegation. They also identified best practices such as exposing junior enlisted to using the five-paragraph operation order for all events as well as providing small group sessions with the brigade command sergeant major. As a result, the battalion intends to incorporate these lessons learned in future JLDC iterations.

Monday	Tuesday
MS Teams Familiarization 0730-0800	Stress Fire Range 0600-0900
Introductions, Admin 0800-0900	Diet/Nutrition 0930-1030
PT Discussion (Overview) 0900-0930	Time Management and Delegation 1030-1130
After Action Reviews 0930-0950	Sponsorship 1130-1200
Unit History 0950-1000	Lunch/Personal Hygiene 1200-1300
Resources (APD, IKN, ATN, CALL) 1000-1100	Taking Charge of Events/NCOIC 1300-1430
Base Resources (BH, MRT) 1100-1130	Developing Short Training Classes 1430-1530
Lunch 1130-1230	PSG Roundtable Discussion 1530-UTC
Role of the NCO (Junior Leadership) 1230-1400	
Role of the NCO (Senior Leadership) 1230-1400	
1SG Roundtable Discussion 1530-UTC	

Figure 4. FY21 Junior Leader Development Course Schedule


Lessons Learned

While the EXEVAL was conducted to standard, it was not perfect, and it is therefore important to capture lessons learned to share across the U.S. Army Intelligence and Security Command enterprise. The EXEVAL includes the following lessons learned:

- ◆ Train and certify external evaluators early. The EXEVAL requires knowledgeable evaluators or OC/Ts who understand the unit's METs and respective T&EOs. Developing evaluators who can balance their own requirements while learning the intricacies of a 700-series battalion takes time and coordination. It is recommended that evaluators be trained weeks in advance to allow for coordination before the event.
- ◆ External evaluators are key to improving major training events and internal systems and processes.
- ◆ Clearly define structure and outputs before starting the MDMP.
- ◆ Create a collaborative environment in which the staff members know their input is respected and valued. Understand the value of straightforward input across all warfighting functions.
- ◆ Maximize opportunities to have staff members create, manage, and present their content, thus allowing the executive officer/chief of staff to oversee and manage the MDMP process as a whole.
- ◆ Frequent cross-echelon touchpoints provided a clear, shared understanding.
- ◆ An understanding of the OPCON/ADCON relationships was instrumental in the facilitation of the EXEVAL. The higher headquarters must understand command and support relationships and perform the inherent responsibilities.
- ◆ Having a knowledge base of our mission access requirements is imperative. Many of our Soldiers are unable to "come inside the wire" because of the stringent security restrictions that our OPCON element places on us.

Conclusion

The EXEVAL had tangible benefits that promoted collaboration and communication across the entire MIB-T. The event facilitated "eyeball-to-eyeball" interaction between the brigade and battalion elements. This face-to-face, albeit socially distanced because of COVID-19, was essential to gain a shared understanding of the battalion's individual and collective training proficiencies. Given the turnover of personnel and the geographic separation between brigade and battalion elements, the EXEVAL provided a unique opportunity for face-to-face interaction.

In line with the Army Signals Intelligence Strategy, the battalion's enduring goal is to produce and sustain cryptologic-lethal Soldiers to the force while simultaneously developing tactically proficient Soldiers. The EXEVAL helped provide an honest assessment of the daily operations executed by the battalion. As a result of the EXEVAL, the battalion helped provide predictability and prioritization for FY21 while enabling key leaders to capitalize on the lessons learned to refine cryptologic, tactical training, and operational support to deliver an exponential mission impact. 

Endnotes

1. Department of the Army, Field Manual 7-0, *Training* (Washington, DC: U.S. Government Publishing Office [GPO], 14 June 2021), F-2.
2. Department of the Army, Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. GPO, 31 July 2019), 2-16.
3. Department of the Army, *CGSC Circular 350-1 U.S. Army Command and General Staff College Catalog* (Fort Leavenworth, KS: Command and General Staff College, 2020), 7-10.

MAJ George Gurrola serves as the battalion S-3 for the 717th Military Intelligence (MI) Battalion, 470th MI Brigade-Theater (MIB-T), at Joint Base San Antonio, TX. He holds a master's degree from Georgetown University's School of Foreign Service and a bachelor of arts from Texas A&M University. His previous assignments include serving as an assistant professor at the U.S. Military Academy, the 205th MI Battalion, and 3rd Battalion, 75th Ranger Regiment.

CPT Mason Lockey is an MI officer and currently serves as the battalion assistant S-3 in the 717th MI Battalion, 470th MIB-T, at Joint Base San Antonio, TX. He previously served as the S-2/assistant S-2 for the 12th Combat Aviation Brigade and 1st Battalion, 3rd Aviation Regiment (Attack Reconnaissance) in Katterbach, Germany. He holds a master of science in strategic leadership from Black Hills State University, SD. He is also a recent graduate of the Signals Intelligence/Electronic Warfare course.

CW3 Katy Tomlinson is a cryptologic technician and serves in the 717th MI Battalion, 470th MIB-T, at Joint Base San Antonio, TX. She previously served as the emerging threats mission manager and senior cryptologic reporter at the 312th MI Battalion at Fort Sam Houston, TX. Prior to that she was the brigade collection manager and cryptologic officer in charge for the 3rd Armored Brigade, 1st Armored Division, at Fort Bliss, TX. She holds a bachelor of science in criminology from Florida State University.



What is Foundry

The Foundry Intelligence Training Program is a critical enabler to Army global readiness. It provides commanders the necessary resources (funding, facilities and subject matter experts) to prepare military intelligence Soldiers, Civilians, and units to conduct intelligence operations and activities at the tactical, operational, and strategic levels.

Foundry Training Types

Foundry enhances individual and collective intelligence training for the Active and Reserve Components through –

- a. Resident (TDY) or at a Foundry Site
- b. Live Environment Training
- c. Mobile Training Teams



Funding

Headquarters, Department of the Army, Office of the Deputy Chief of Staff for Intelligence, may allocate Foundry resources that support unit METL, Army Service component command's intelligence warfighter function training requirements and advanced intelligence training provided by the intelligence community.

Schedules

Foundry courses can be scheduled through the Army Training Requirements and Resources System (ATRRS). ATRRS allows units to submit training requests online and view calendars of all available, requested, and scheduled intelligence training. ATRRS also displays training objectives, prerequisites, class size, and course administrative requirements. ATRRS URL: <https://www.atrrs.army.mil>.

Points of Contact

DA G-2 TRAINING POINT OF CONTACT
Foundry Program Manager: 703-695-1268
INSCOM FOUNDRY POINT OF CONTACT
Foundry Program Administrator: 703-706-1890
INSCOM ATRRS: 703-706-2227

Using Your Experiences to

Develop Leaders



Drive Beneficial Change

Inform the Force

Soldiers Do Well That Which the Commander Checks

by Mr. Chet Brown, Chief, Lessons Learned Branch

An organization does well only those things the boss checks.

—GEN Bruce C. Clarke, Former Commander, U.S. Army Europe

Introduction

A hypothesis emerged from the preceding epigraph addressing a common question posed in a recent lessons learned discussion with a group of military intelligence (MI) unit leaders: “Why do we continue to see the same performance challenges and issues at the [combat training centers] CTCs?” To answer this question, we first need to look at factors leading to the problem.

U.S. Army Combat Training Centers

- ◆ Joint Multinational Readiness Training Center, Hohenfels, Germany.
- ◆ Joint Maneuver Training Center, Camp Atterbury, Indiana.
- ◆ Joint Readiness Training Center, Fort Polk, Louisiana.
- ◆ Mission Command Training Program, Fort Leavenworth, Kansas.
- ◆ National Training Center, Fort Irwin, California.

Enduring Challenges at the CTCs

There are many reasons why some people mistakenly think the enduring challenges that units and personnel experience at the CTCs are the result of repeating avoidable mistakes. It is also an inaccurate generalization that we learn the same lessons over and over again. CTC rotations are training exercises, not experiments. Training exercises seek to develop or assess performance, adjusting activities or events to achieve the commander’s objectives, whereas an experiment is “an attempt to try out a new procedure, idea, or activity.”¹ I offer an opinion, in three parts, as to why CTC rotations experience enduring challenges, shortfalls, or deficiencies.

Part 1—Maximize Sweat for Good Purpose. The CTCs introduce heuristic stressors to maximize rotational training unit (RTU) sweat in training; the objective is to reduce RTU bleeding on the battlefield. The CTC’s impact on each mission variable (METT–TC) is difficult, if not impossible, for an RTU to replicate at home station.² No matter how well trained an RTU may be at home station, a CTC rotation will provide opportunities for discovery learning. The RTU commander or the senior CTC observer coach/trainer can apply a rheostat effect to increase or reduce operations tempo, activities, or challenges to maximize the training effect or benefit.



GEN Dwight D. Eisenhower speaking with paratroopers about to embark on the World War II D-Day invasion. Photo taken on 5 June 1944. (U.S. Army photo)

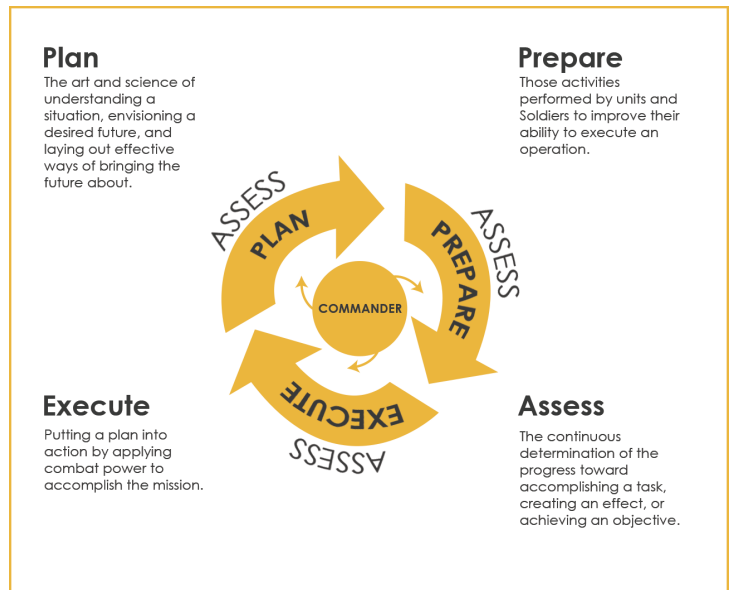
Part 2—Know that “Stuff Happens.” “Murphy” (Murphy’s Law, aka anything that can go wrong will go wrong) and the enemy (opposing force) affect the RTU operation. This is also known as “the enemy gets a vote” as to the outcome. CTC events will continue to reveal challenges in the most highly trained units and personnel. Unanticipated conditions or events will arise and affect the mission variables. In other words, “stuff happens.” These are the ubiquitous opportunities for personnel to excel, engage in discovery learning, or anticipate the constructive guidance, counseling, and mentoring in various forms from one’s higher headquarters. These unforeseen situations are routinely resolved by learning what one can from the event while carrying on with the mission. Much learning occurs in the process of recovering from a mistake.

Part 3—Prepare. The third part of the answer to “Why do we continue to see the same performance challenges and issues at the CTCs?” brings us to what I think the question was attempting to illustrate. We know we will face certain challenges at a CTC. The information to help us succeed is readily available. Some suggest too much information is available—an overwhelming amount that prevents us from performing a triage of the most pertinent. Each CTC attempts, during its respective leader training program engagements, to assist the RTU in understanding what information is most useful to prepare for a CTC rotation. The key to operational and mission success from a lessons learned perspective might lie in one word—*prepare*—perhaps an underemphasized phase in the operations process.

Point of Origin?

No one plans to fail at a CTC rotation. Units we observed exhibited an unwavering commitment to planning and orders production before and during the rotation. The U.S. Army plans very well. Countless operations plans and various orders documents (WARNO, OPORD, and FRAGO) provide supporting evidence.³ Sometimes, headquarters engage in

so much planning that they forget the one-third/two-thirds rule, stealing time from their subordinates to conduct their own planning or preparation. The simple act of reviewing during the three sequential activities (plan, prepare, and execute) and the one continuous activity (assess) in the operations process helps form a hypothesis that, if confirmed, will provide commanders and leaders with information to address some of the enduring challenges experienced at the CTCs.



The Operations Process⁴

The prepare phase of the operations process offers the last opportunity for commanders to mentor, or influence the behavior of, their subordinates before they begin a mission. **Soldiers do well that which the commander checks.** The saying remains true even when substituting *leader* for *commander*. Observations by the U.S. Army Intelligence Center of Excellence Lessons Learned Team support the naturally resulting hypothesis from this truism: **Performance challenges indicate the absence of leader influence or involvement.** Leader involvement at the lowest tactical levels is a key component of effective troop leading procedures. **Your personal involvement during the preparation phase can reverse negative MI performance training and operations trends observed at the CTCs.**

**Plans are nothing. Planning is everything.
—GEN Dwight D. Eisenhower**

Plans are nothing, but planning is everything. Several variations of this quote are attributed to lessons learned by GEN Dwight D. Eisenhower when serving as Supreme Commander of the Allied Expeditionary Force in Europe during World War II. One must avoid the temptation to associate this lesson with the earlier description of “stuff happens” and instead dig a little deeper to discover a more practical lessons value.

The significance of GEN Eisenhower's quote is not about planning; rather, it is about how planning helps us to prepare for most if not every contingency. If we are fully prepared, we can overcome planning failures. Ironically, over the decades, more than a few CTC observer coach/trainers have commented on how U.S. units execute an operation as planned even when realizing the plan is not working. The units fight according to the plan, not the enemy. Rarely does the RTU revise the plan to account for unanticipated mission variables. Conversely, multiple anecdotes describe the opposing force's focus on revising their plan to achieve their objectives or defeat the enemy (the RTU) in adherence to the opposing force's doctrinal tenets or principles.

The Army's definition of prepare activities, from ADP 5-0, *The Operations Process*, lends additional emphasis to the prepare phase's crucial role in enabling superior performance: "*Preparation consists of those activities performed by units and Soldiers to improve their ability to execute an operation.*"⁷⁵ I'll add some words to this quote to illustrate my point: to improve their ability to execute an operation, *despite deficiencies in the plan.*

By failing to prepare, you are preparing to fail.
—Benjamin Franklin

Maximize Your (Leader) Presence

It is easy for anyone to criticize a leader—whether in politics, government, sports, media, social organizations, or the military. Commanders are responsible for everything the unit does or fails to do. It is neither difficult nor useful for me to provide examples that link a unit's or a Soldier's performance struggles to a leader's action or inaction. What follows are tips on how leaders, particularly at the tactical level, can avoid some of the challenges observed during CTC rotations and home-station training. Your actions may be the key in preventing other leaders asking, "Why do we keep making the same mistakes?"

Inspect Training. Show up unannounced at differing and various training events where you are not expected. A more effective method is to inspect training with a noncommissioned officer (first sergeant or platoon sergeant) or a warrant officer. You need not interject or disrupt training. Quietly observing, while maybe conferring with your subject matter experts in the background, will convey the seriousness of your interest. Your physical (or online) presence also provides an opportunity to praise in public, correct in private, without interfering.

Pre-Combat Checks (PCC)/Pre-Combat Inspection (PCI). Hold subordinates and yourself accountable for conducting PCC/PCI. Packing lists exist for practical reasons, one of which is to ensure Soldiers have the items they need to

accomplish the mission. Conducting a PCC/PCI is a simple method to ensure standards are met, although there were few things I disliked more than having to dump my A and B bags in the company area prior to moving out on a training exercise. All the careful rolling, packing, weatherproofing, and double-checking the night before an exercise were undone each time there was a 100 percent PCI. Unfortunately, the need to conduct a 100 percent inspection was validated multiple times, based on the number of attempts a few Soldiers made to replace items on the packing list with personal demand items or contraband. Here are some things to consider:

- ◆ A less intrusive variation of the 100 percent layout is to empower subordinate leaders with conducting the PCC/PCI and to empower more senior leaders with spot-checking.
- ◆ PCC/PCI failures must be addressed. Every time a leader fails to enforce a standard, they establish a lower standard. I remember my first field training exercise in an MI unit 35 years ago. 1SG Adams asked an enlisted MI Soldier (not me) whose fingers were turning blue, "Where are your gloves?" The Soldier's reply of "I didn't bring any" resulted in 1SG Adams directing the squad leader to provide his gloves to the Soldier and then for the platoon sergeant to give up his gloves to the squad leader. I was waiting for the exchange to reach higher up the chain of command, but that is where the lesson stopped.
- ◆ An additional benefit of PCC/PCI is the opportunity to institute or enforce standardized vehicle load plans, organizational clothing, and individual equipment. Load plans (textual and graphic) are a validated best practice. Having your vehicles, Soldiers' rucksacks, and common table of allowance items (aka TA-50 gear) packed according to a standardized scheme facilitates rapid action in a crisis or access in low-visibility conditions.

Motor Pool Monday. It is amazing how much stuff breaks in the motor pool between Friday night when vehicles are securely parked and Monday morning at the start of motor stables' preventive maintenance checks and services (PMCS). Motor stables is only the beginning. Effective leaders understand that completing prime mover PMCS is only one part in determining the operational readiness rate of MI systems.

Systems Test Tuesday? Successful leaders not only ensure that prime mover PMCS are completed, but they also stick around to confirm that their MI systems are fully operational. If not personally aware of all the required function checks and tests needed to confirm an MI system is full mission capable (FMC), insightful leaders will seek the

assistance of a knowledgeable noncommissioned officer or chief warrant officer. Some systems rely on esoteric steps or connections to determine FMC. Sometimes, leaders assume that providing power to a system is good enough to prove the system is FMC.

Validation Exercise. Multiple CTC rotations and home-station training observations identify the successful completion of a validation exercise as a best practice. Validation exercises confirm an element's ability to execute all components of a communications primary, alternate, contingency, and emergency (PACE) plan. The validation exercise converts the PACE concept from a plan to a preparation. The physical expanse of an RTU area of operations at the National Training Center is unmatched at home stations. Some units have emplaced elements and communications nodes at distant locations in collaboration with civilian authorities. One light brigade at Fort Drum, New York, deployed elements along the northern reaches and western tier of New York State to validate command post communications.

Epigraph

GEN Bruce C. Clarke, *General Bruce C. Clarke's Thoughts on Leadership* (Fort Belvoir, VA: U.S. Army Engineer School, 1986), 1. GEN Clarke was a U.S. Army officer who served in World War I, World War II, and the Korean War. He held numerous commands, including U.S. Army Pacific and U.S. Army Europe.

Endnotes

1. *Merriam-Webster's Collegiate Dictionary*, 10th ed. (Springfield, MA: Merriam-Webster Incorporated, 1999), s.v. "experiment (n.)," (1999).
2. METT-TC is mission, enemy, terrain and weather, troops and support available-time available and civil considerations.

Leader Involvement Improves Performance

Don't mistake "Leader Involvement Improves Performance" as a call to micromanage or complete the tasks that subordinates should perform. Look at it as a call to push away from the keyboard, or to put down the smartphone, and to engage in leadership by walking around to ensure effective preparations. Soldiers will appreciate your presence—a judicious presence—and will take pride in demonstrating their level of preparedness. ✨

There are no secrets to success. It is the result of preparation, hard work, and learning from failure.⁶

—GEN Colin Powell

3. WARNO: warning order; OPORD: operation order; and FRAGO: fragmentary order.

4. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 2-25. Change 1 was issued on 6 December 2017.

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

6. GEN Colin Powell, quoted in Oren Harari, *The Leadership Secrets of Colin Powell* (New York: McGraw Hill, 2002), 164.

GREAT SKILL Program

Military Intelligence Excepted Career Program

Our Mission

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

Who are we looking for?

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

Basic Prerequisites

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

For a full list of prerequisites, please visit our website (SIPRNET <http://gsd.daiis.mi.army.smil.mil>) or contact an Accessions Manager at gs.recruiting@us.army.mil or call (301) 833-9561/9562/9563/9564.



FUTURES FORUM

Global Multi-Domain Operations Competitors in 2035: Implications of the Space Domain Race

Illustration by MIPB Staff

Mr. Kevin B. Gorski

Introduction

The Earth's Moon offers many possibilities for the advancement of humanity, including the mining of essential minerals and the potential of unknown materials. In addition to the United States, other nations and numerous commercial organizations are engaged in the exploration of the Moon and beyond:

- ✦ China is currently conducting two robotic lunar missions, with three robots exploring and gathering mineral samples for return to Earth.
- ✦ Russia has successfully launched and recovered spacecraft, and has set human space-orbiting endurance records.
- ✦ Other nations are capable of launching and placing satellites into orbit.
- ✦ Commercial space ventures are on the rise and will eclipse formal government space and planetary exploration.

For the United States and the Department of Defense, the space domain will increase in complexity on Earth and in space. This is not about searching for the presence of other life forms; rather, it is about ensuring that the United States has access to, and maintains maneuvering capability within, the Earth's orbit and beyond. Accomplishing this goal requires navigating international treaties that govern space and lunar exploration, and developing policies and standards in conjunction with other nations and commercial enterprises.

Why an Interest in Lunar Activities?

The United States and Russia started their space programs in the 1940s and 1950s. Since then, the Chinese established an ambitious program of their own. By 1970, China had launched its first satellite; in 2003, it sent its first astronaut into space; and now it is building a space station. Most recently, the Chinese collected lunar soil and rocks and returned them to Earth.

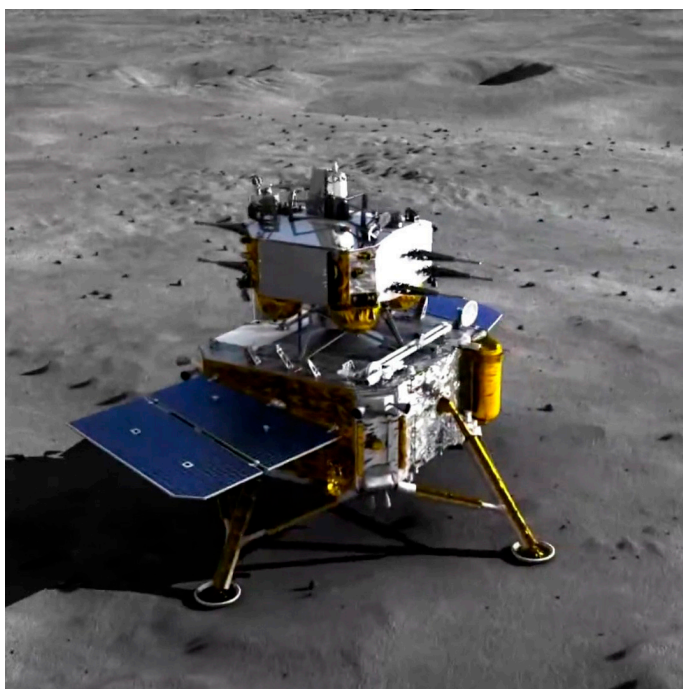
From a military intelligence perspective, there are three primary areas of interest as China and other countries explore the lunar surface. First, although several of these Moon minerals are available on Earth, scientists believe that the different properties could potentially enhance the application of common construction, communications, energy transference and storage, and weapon lethality and protection measures. Table 1, on the next page, lists the minerals and elements known to exist on the lunar surface and their associated application. Second, China's current exploration of the lunar surface is a robotic mission. Similar efforts by any country or private company may accelerate human inhabitation of the lunar surface. Third, many of these exploration goals include going farther into space and to Mars. In addition to government space missions, many private organizations are conducting lunar research, some for exploration, and others for potential mining opportunities.

MINERAL OR ELEMENT	AVAILABILITY	APPLICATION
Al ALUMINUM	Present with other minerals. Requires extraction.	Excellent electrical conductor, and when atomized, aluminum powder is a good solid rocket fuel when burned with oxygen.
Fe IRON	Abundant. Requires additional exploration for deposit validity.	Additive manufacturing, 3D printing, selective laser sintering, selective laser melting, and electron beam melting.
Ti TITANIUM	Present. Surface and subsurface extraction required.	Framing of future spacecraft.
Ca CALCIUM	Abundant.	Ceramic/silicon-based solar cells, along with creating flexible metals, electrical conductors in zero atmospheres.
Mg MAGNESIUM	Likely abundant for lunar mining at low depths.	Various alloys for aerospace, automotive, and electronics applications.
Si SILICON	Abundant as metalloid on lunar surface.	Supports solar panel arrays along with glass, fiberglass, and ceramics. High purity supports semiconductor applications.
³He HELIUM-3	Present and challenging to gather. Could be exhausted if over-mined.	Application with nuclear fusion, yet questionable results. Overall, this rare earth element is more valued than gold.
C CARBON	Present.	Potential for production of lunar steel.
N NITROGEN	Present.	Mining would be difficult because of trace amounts.

Table 1. Lunar Mineral Availability and Application

China's Chang'e Project

The Chinese Lunar Exploration Program launched its first spacecraft, Chang'e-1, in 2007. More recently, the Chinese launched Chang'e-4, arriving on the Moon's far side in January 2019. It included the Yutu-2, a robotic lunar rover equipped with the lunar penetrating radar, a ground-penetrating radar that uses pulses to image the subsurface of the Moon. In 1972, the U.S. Apollo 17 mission deployed the Apollo lunar sounder experiment while in orbit, which penetrated approximately 1.3 kilometers into the Moon's surface. Although the Chinese lunar penetrating radar data is not available, considering the technological improvements since the 1970s, it is likely the recordings are better and may have detected water and other deposits.

The Ascender (or Descender) and Lander assembly of Chang'e-5 on the moon surface³

In December 2020, the Chang'e-5 lunar exploration vehicle landed on the Moon. The vehicle collected samples and launched an ascender to bring the lunar material back to Earth later that month.¹ It was the first time that moon rocks and soil have been brought back to Earth since the former Soviet Union's Luna 24 mission in 1976.²

Who Owns the Moon?

With increased space activity in the 1950s and 1960s, many nations recognized the need to establish an international legal framework, under the auspices of the United Nations, to protect space. The 1967 Outer Space Treaty, which still exists, details numerous rules governing the peaceful exploration and use of space.⁴ Although more than 100 countries have signed and ratified the treaty, it is virtually impossible to enforce.⁵ The 1979 Moon Treaty reiterates most provisions of the Outer Space Treaty and adds two new concepts that address the exploitation of natural resources in outer space. However, most countries have not ratified the Moon Treaty, including the United States, Russia, and China.⁶ A recent article on space law, states—

Seeking clearer regulatory guidelines, private companies in the US prompted the US government, and legalized space mining in 2015 by introducing the US Commercial Space Launch Competitiveness Act of 2015. Similar national legislations legalizing extra-terrestrial appropriation of resources are now being replicated by other nations, including Luxembourg, Japan, China, India and Russia. This has created an international legal controversy on mining rights for profit....A legal expert stated in 2011 that the international issues "would probably be settled during the normal course of space exploration."

The U.S. Commercial Space Launch Competitiveness Act of 2015 was created to “facilitate a pro-growth environment for the developing commercial space industry,” making it legal for U.S. companies and citizens to own and sell resources that they extract from the Moon, Mars, and beyond. Additionally, in April 2020, former President Donald Trump signed an executive order establishing that “Americans should have the right to engage in commercial exploration, recovery, and use of resources in outer space, consistent with applicable law,” and that the United States does not view space as a “global commons.”⁸ This opens up the potential for the U.S. Government, private ventures, and other nations to consider their options in outer space. As for China, the Chinese Lunar Exploration Program is actively pursuing its goals, with its space station and series of Chang’e missions.

An important consideration for Army intelligence is how a country or an alliance of nations, including private entities, would employ capabilities on the lunar surface. Table 2 outlines potential conceptual ideas for military applications.

Conclusion

As a domain, space includes the immediate orbiting activities around the Earth, space basing (to include the inhabitation and mining of the Moon), and further exploration into outer space. While for many nations much of space exploration is currently conceptual, countries such as China are developing and conducting ambitious space operations. Therefore, the U.S. Army, Department of Defense, and various intelligence agencies have an obligation to be involved in space exploration discussions here on Earth and in actual space ventures—government or civilian.



MISSION	PLAUSIBILITY	APPLICATION
LUNAR BASE	Likely first activity before any other concept—use of lunar materials will enable construction once a similar orbiting station module has established initial basing operations.	<ul style="list-style-type: none"> Lunar surface base—Modular base station elements—access to water and power source. Sub-lunar surface base—Use of known lunar lava tubes once surface base is complete. Lunar artificial intelligence-enabled robotic bases are more likely in advance of human occupation/habitation.
LUNAR LAUNCHING SITE	Conceptual based on success of orbiting space stations and creation of materials to form the habitat structures.	Opportunities for both Earth-to-Earth and Moon-to-other planets, or asteroid exploration and mining.
LUNAR COLLECTION ARRAY	Likely—conceptual designs.	Precision cosmological measurements via telescope observations looking at Earth for geological activities but as a stable optical surveillance collection means.
LUNAR NAVIGATION ARRAY	Most likely—concepts exist.	Lunar navigation arrays could replace or enhance existing orbiting navigational satellites.
LAUNCH MISSILES FROM MOON TO EARTH	Conceptual — challenge lies in getting missiles safely to the lunar surface. An alternative is kinetic rods launched from an orbiting satellite or lunar space station.	Nuclear weapons directed falling rod or meteorite at enemy targets.

Table 2. Lunar Application

Endnotes

1. “解放军报, 嫦娥五号探测器实施动力下降并成功着陆” [People’s Liberation Army Daily, the Chang’e-5 probe carried out a power descent and successfully landed], China Military Network, Ministry of National Defense Network, December 2, 2020, http://www.81.cn/jfjbmap/content/2020-12/02/content_277167.htm.
2. Neel V. Patel, “China just brought moon rocks back to Earth for the first time in its history,” *MIT Technology Review* online, December 16, 2020, <https://www.technologyreview.com/2020/12/16/1014773/china-moon-rocks-back-earth-chang-e-5/>.
3. The photograph of the Ascender (or Descender) and lander assembly of Chang’e-5 on the moon surface is licensed under a Creative Commons Attribution 3.0 Unported license by the China News Service, <https://www.youtube.com/watch?v=b-HMhWenTM0&t=7s>.
4. “The Outer Space Treaty at a glance,” Arms Control Association, last reviewed October 2020, <https://www.armscontrol.org/factsheets/outerspace>.
5. “The Outer Space Treaty has been remarkably successful – but is it fit for the modern age?” *The Conversation*, January 27, 2017, <https://theconversation.com/the-outer-space-treaty-has-been-remarkably-successful-but-is-it-fit-for-the-modern-age-71381>.
6. Matt Williams, “Trump signs an executive order allowing mining the moon and asteroids,” *Phys.org*, April 13, 2020, <https://phys.org/news/2020-04-trump-moon-asteroids.html>.
7. Charlie Bowles, “Space Law: The Commercial Space Race Begins,” *EM Law*, March 8, 2021, <https://www.emlaw.co.uk/international/space-law-the-commercial-space-race-begins/>.
8. Williams, “Trump signs executive order.”



MILITARY INTELLIGENCE CORPS HALL OF FAME INDUCTEES – 2021



Brigadier General Brian A. Keller, U.S. Army, Retired


Brian Keller entered the U.S. Army as a Reserve Officer Training Corps cadet at the University of Connecticut. After graduating as a distinguished military graduate in 1980, his first four successive assignments—platoon leader, S-2, executive officer, and company commander—were in the 522nd Military Intelligence (MI) Battalion and 2nd Squadron, 1st Cavalry Regiment, 2nd Armored Division, at Fort Hood, Texas.

After graduating from the Defense Intelligence College's Postgraduate Intelligence Program, BG Keller volunteered as the S-2, 1st Ranger Battalion, 75th Ranger Regiment, where he participated in Operation Just Cause in Panama. After completing Command and General Staff College and the School of Advanced Military Studies, he was assigned to the 25th Infantry Division (Light) at Schofield Barracks, Hawaii. He served first as the Division's Assistant Chief of Staff, G-2 (Plans and Operations), and then as the 125th MI Battalion S-3 and executive officer. In 1995, he moved to Fort Drum, New York, where he served first as the 10th Mountain Division (Light Infantry) G-2, and later commander of the division's 110th MI Battalion where he helped prepare an MI company team to deploy in support of Operation Joint Guard in Bosnia.



After assignment as a Deputy Chief of Staff, G-2 Intel XXI Study action officer, and attendance at the Army War College, BG Keller took command of the 513th MI Brigade at Fort Gordon, Georgia, in 2000. Following the 9/11 terrorist attacks, he deployed his brigade's tactical command post to Kuwait to oversee intelligence operations conducted by four of the brigade's battalions in support of U.S. Central Command and Joint Special Mission Units operating in Afghanistan, and a fifth battalion simultaneously conducting counternarcotics and counterterrorism intelligence operations for U.S. Southern Command. In 2002, BG Keller volunteered to serve as the Director of Intelligence, J-2, for Joint Special Operations Command, deploying multiple times to both Afghanistan and Iraq. After 24 years in the operational force, BG Keller was assigned to Fort Huachuca, Arizona, in 2004, as the deputy commander/assistant commandant of the U.S. Army Intelligence Center. He subsequently served as the Director of Intelligence, J-2, at U.S. European Command in Germany from 2005 to 2007.

In 2007, BG Keller was named deputy chief of staff for intelligence, C-2, of Multi-National Force-Iraq for his last deployment in support of Operation Iraqi Freedom. His final assignment was as the Military Executive at the National Geospatial-Intelligence Agency in Bethesda, Maryland, focusing the agency's support to warfighters in Afghanistan and Iraq.

BG Keller retired from active duty on 28 February 2010. His awards and decorations include the Distinguished Service Medal, Defense Superior Service Medal (one Oak Leaf Cluster), Legion of Merit, Bronze Star Medal (two Oak Leaf Clusters), Meritorious Service Medal (five Oak Leaf Clusters), Army Commendation Medal, and Army Achievement Medal (two Oak Leaf Clusters), as well as numerous campaign and service ribbons, the Ranger Tab, the Army Staff Badge, the Master Parachutist Badge with Combat Star, and German Airborne and Jordanian Airborne badges. BG Keller was also awarded the MI Corps Association's Knowlton Award. 

2021



MILITARY INTELLIGENCE CORPS HALL OF FAME INDUCTEES



2021

Colonel Marc B. Powe, U.S. Army, Retired (Deceased)

Marc Powe entered the U.S. Army in the early 1960s and completed two tours in Vietnam, first as a province intelligence advisor in the Mekong Delta and then as a military intelligence company commander supporting the 4th Infantry Division. After serving as an instructor at the U.S. Army Intelligence Center and School at Fort Huachuca, Arizona, he graduated from the Command and General Staff College and then spent 2 years at the Army's Military Personnel Center.

Proficient in several foreign languages, including Russian, German, Vietnamese, Arabic, and French, COL Powe's skills were put to the test in several attaché and other human intelligence (HUMINT) positions. In 1977, he was assigned to Moscow as the first operations officer for the largest U.S. Defense Attaché Office in the world. Shortly after his arrival, the U.S. Embassy suffered a major fire, and COL Powe earned a Soldier's Medal for his heroic actions during the event. Two years later, he was asked by the Army's Deputy Chief of Staff, G-2, to undertake a study on improving Army HUMINT. In 1980, COL Powe was assigned to the Defense Intelligence Agency to expand this study throughout the Department of Defense and begin implementing its recommendations. He was then given Army staff responsibility for establishing a new special operations intelligence unit that became operational in 1982.

In 1985, he was assigned to Baghdad, Iraq, as the first defense attaché in the United States Embassy since its previous closure in 1967. His office collected and reported high-value intelligence, mainly focused on the Iraq-Iran War. In 1987, COL Powe undertook a specially assigned task to recover Soviet materiel that Libyans had abandoned in the Republic of Chad. He was able to acquire and transfer to American custody an intact MI-24 Hind helicopter gunship and anti-aircraft systems.

In 1988, COL Powe was assigned to his third attaché position, in Tunis, with his specific target being Libyan efforts to create weapons of mass destruction. Finally, COL Powe served as the chief of staff of the Directorate of Attachés and Operations at the Defense Intelligence Agency from 1991 until his retirement in 1992. In addition to managing a large headquarters in Arlington, Virginia, he oversaw more than 1,000 HUMINT collectors abroad, focused particularly on the Middle East and South Asia.

COL Powe retired from active duty on 31 March 1992 and went on to have a successful 22-year civilian career. He passed away on 2 August 2020. His awards and decorations include the Defense Superior Service Medal (one Oak Leaf Cluster), Legion of Merit, Soldier's Medal, Bronze Star Medal (two Oak Leaf Clusters), Purple Heart, Defense Meritorious Service Medal (two Oak Leaf Clusters), Meritorious Service Medal (two Oak Leaf Clusters), Air Medal (four awards), Air Medal with V Device, Army Commendation Medal, and Army Achievement Medal, as well as numerous campaign and service ribbons, and the Army Staff Identification Badge. He received the Director of Central Intelligence Exceptional Collector Award in 1987 and 1991 and was inducted into the Defense Attaché Service Hall of Fame in 1999.



2021



MILITARY INTELLIGENCE CORPS HALL OF FAME INDUCTEES




2021

Chief Warrant Officer 5 Matthew R. Martin, U.S. Army, Retired

Matt Martin enlisted in the U.S. Army in 1993 as an intelligence analyst. He attended Ranger School as a private first class and then spent 4 years as an intelligence analyst at the regimental and battalion level within the 75th Ranger Regiment. In 1999, after just 5 years in service, he was appointed a Military Intelligence (MI) Corps warrant officer. After graduating from the Warrant Officer Basic Course, Martin served as an all-source intelligence technician with D Company, 313th MI Battalion, 82nd Airborne Corps, from 1999 to 2003. During this assignment, he was attached to the 3rd Infantry Division for a tour in Bosnia, and then he deployed to Kandahar, Afghanistan, with the 3rd Brigade, 82nd Airborne Corps. While there, he led the division's intelligence support element, analyzing and targeting the movements of the Taliban and al-Qaeda along almost the entire 1,500-mile Afghanistan-Pakistan border.

In 2003, CW5 Martin went to Hawaii as the joint intelligence support element chief in the Special Operations Command Pacific J-2. For the next 3 years, his team focused on the counterterrorist threat throughout Southeast Asia. After graduating from the Warrant Officer Advanced Course in 2006, CW5 Martin became the all-source production chief for the 1st Special Forces Group at Joint Base Lewis-McChord, Washington, for 2 years. He then was recruited into a Special Mission Unit where he led a team of targeting officers from 2008 to 2011. During this assignment, he deployed to numerous locations in a variety of roles, including the J-2 of a forward-deployed task force on a counterterrorism mission in North Africa.

In 2011, CW5 Martin spent a few months at the U.S. Army Intelligence Center of Excellence at Fort Huachuca, Arizona, developing a new analytic tradecraft course, before volunteering for a tour in Afghanistan as the deputy analysis and control element chief with the 1st Cavalry Division at Regional Command East in support of Operation Enduring Freedom. He then returned to Fort Huachuca as the chief of the Warrant Officer Training Branch from 2012 to 2015, during which time he completely revamped all MI warrant officer training. He then applied for and was chosen as the sixth Chief Warrant Officer of the MI Corps. During his 3 years in the position, he was the driving force behind advancing MI capabilities, creating the CW5 Rex Williams Award, and improving talent management of warrant officers throughout the MI Corps.

CW5 Martin retired from active duty on 31 October 2018. His awards and decorations include the Legion of Merit, Bronze Star Medal (two Oak Leaf Clusters), Defense Meritorious Service Medal (one Oak Leaf Cluster), Meritorious Service Medal (two Oak Leaf Clusters), Joint Service Commendation Medal, Army Commendation Medal (four Oak Leaf Clusters), Joint Service Achievement Medal, and Army Achievement Medal (one Oak Leaf Cluster), as well as the Master Parachutist Badge and Ranger Tab. CW5 Martin was also awarded the MI Corps Association's Knowlton Award. 




**Ms. Harriet Ross Tubman (Deceased)**

Harriet Tubman was born a slave known as Araminta Ross in 1822 on Anthony Thompson's plantation in Dorchester County, Maryland. In 1849, she escaped to freedom in Pennsylvania and, thereafter, led a number of trips to free approximately 80 fellow slaves. She is undoubtedly most famous for her Underground Railroad activities. However, from 1862 to 1865, she also acted as a spy and scout for the Union Army, operating against Confederate forces and their civilian supporters in South Carolina, Florida, and Georgia.

In early 1862, Governor John Andrews of Massachusetts, a staunch abolitionist and friend of Tubman's, asked her to travel to South Carolina as a spy and scout. She was also to conduct other missions as required, including nursing, making medicines from roots and herbs, and training the newly freed in applying skills learned on the plantation to their new lives. Governor Andrews provided her with a pass that allowed her to travel throughout the Union-controlled areas as she desired. Upon arriving in Beaufort, South Carolina, in the spring of 1863, she recruited at least nine former slaves, who could easily maneuver around and mingle with Confederate troops and sympathizers. These spies collected intelligence concerning enemy positions and strengths, movements, and fortifications in Confederate-controlled areas. Tubman also collected information through systematic questioning of escaping slaves, analyzed all collected information, and conducted strategic planning.

One of her most daring and important missions took place in June 1863, when Tubman and her spies collected vital intelligence about Confederate reinforcements and heavily mined waters along the Combahee River north of Beaufort. Colonel James Montgomery, commander of the Second South Carolina Volunteers of African Descent, not only used the intelligence that Tubman's network of spies had collected but also chose her to lead a raid of six Southern plantations on the river. The raid liberated an estimated 750 men, women, and children held in bondage, seized or destroyed millions of dollars of Confederate staples, and opened the river for Union boats. It is estimated that at least 100 men freed in this raid later joined the Union Army as soldiers. Reporting on the raid to Secretary of War Edwin Stanton, Brigadier General Rufus Saxton, the military governor of Beaufort, said, "This is the only military command in American history wherein a woman, black or white, led the raid, and under whose inspiration it was originated and conducted."

After the Combahee River Raid, Tubman returned to Beaufort and continued to collect information as available until the end of the war. At that time, she worked in the Home for Destitute Colored Women and Children in Washington, DC, and provided nursing care at Fort Monroe in Hampton, Virginia. She then returned to Auburn, New York, where she set up one of her homes for the homeless and another as a nursing home and care facility for the elderly. Harriet Tubman died of pneumonia on 10 March 1913 and was buried with military honors at Fort Hill Cemetery in Auburn. 



Awards

For Excellence in Military Intelligence

Captain Meghan S. Oroho **2021 Recipient of the** **Lieutenant General Sidney T. Weinstein Award** **for Excellence in Military Intelligence**

The MI Corps created the LTG Sidney T. Weinstein Award in 2007 to honor the accomplishments of the "Father of Modern Military Intelligence." LTG Weinstein was not only a fine officer; he was a mentor, a role model, a friend to many, and a dedicated family man. This award is given annually to one MI captain who, through his or her actions, demonstrates the values and ideals for which LTG Weinstein stood: Duty, Honor, and Country.




CPT Meghan Oroho, a native of Clearwater, Florida, was commissioned through the U.S. Military Academy in 2014. She graduated both the Military Intelligence (MI) Officer Basic and Captains Career courses, as well as Airborne School, Air Assault School, Army Combatives Level I, and the Information Collection Planners Course. Her civilian education includes a bachelor of science in international law. Accepted to Duke's Fuqua School of Business, CPT Oroho will pursue her master of business administration beginning in July 2021 and thereafter will become an instructor in West Point's Department of Behavioral Sciences and Leadership.

Between October 2019 and June 2021, CPT Oroho served as the company commander of the single-source intelligence company, Alpha Company, 205th MI Battalion. Prior to that role, she served as the assistant brigade operations officer, Headquarters and Headquarters Detachment, 500th MI Brigade. In 2017, she deployed with the 2nd Infantry Brigade Combat Team, 82nd Airborne Division, in support of Operation Inherent Resolve. During that time, she served as the brigade collection manager, as well as the brigade intelligence support element officer in charge. Prior assignments include information collection platoon leader, 1st Squadron, 73rd Cavalry Regiment, and assistant S-2, 2nd Battalion, 508th Parachute Infantry Regiment.

As part of Alpha Company, 205th MI Battalion, CPT Oroho pioneered the Advanced Miniaturized Data Acquisition System Dissemination Vehicle (ADV) and ADV modernization efforts with three of her Soldiers forward positioned in Camp Hansen, Japan. Under her leadership, the team shaped future intelligence systems and drove Army Tactical Exploitation of National Capabilities. CPT Oroho also planned, resourced, and equipped the newly activated Pacific processing, exploitation, and dissemination (PED) center with more than \$5 million in newly fielded equipment and a contracted work force of more than 100 intelligence professionals. Her hard work and dedication to this crucial effort resulted in an exponential increase in intelligence PED across the Indo-Pacific region.

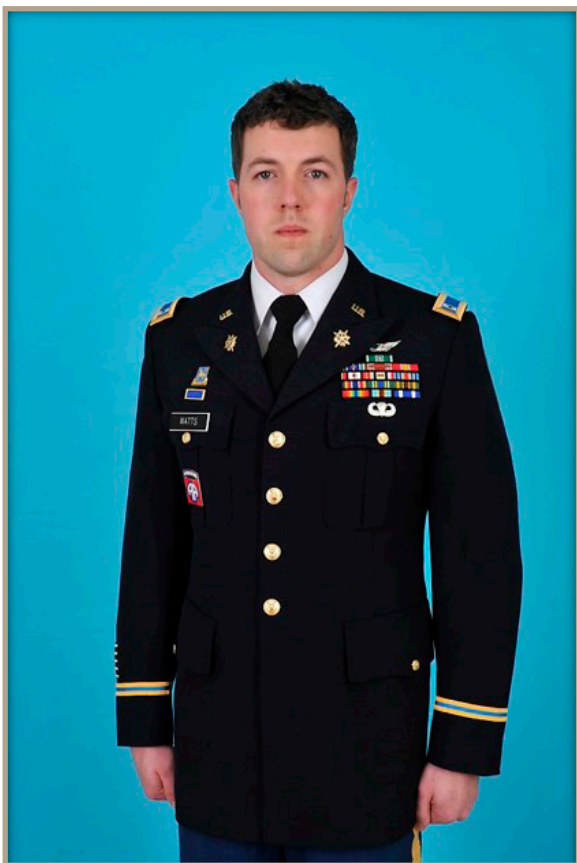
CPT Oroho also demonstrated her compassion as a leader who genuinely cares about Soldiers and their families. She built the most robust Soldier Family Readiness Group (SFRG) at the 205th MI Battalion and created innovative and inclusive SFRG events, resulting in high participation and the building of strong bonds within her team.

Her awards and decorations include the Bronze Star Medal, Meritorious Service Medal, Army Commendation Medal, Army Achievement Medal (1 Oak Leaf Cluster), Parachutist Badge, Air Assault Badge, and German Armed Forces Proficiency Badge (Gold). 

Awards For Excellence in Military Intelligence

Chief Warrant Officer 2 R. Ian Watts 2021 Recipient of the Chief Warrant Officer 5 Rex Williams Award for Excellence in Military Intelligence

The MI Corps established the CW5 Rex Williams Award in 2016 to recognize the outstanding achievements of a company grade warrant officer (WO1-CW2) within the MI community. This award is named in honor of an icon in MI, who spent his 31-year military career improving training, mentoring countless Soldiers, and helping define the foundations of intelligence analysis. CW5 Williams also served as the first Chief Warrant Officer of the MI Corps.




CW2 R. Ian Watts was born in Atlanta, Georgia, in 1982 and was raised in Washington, North Carolina. In September 2000, he enlisted in the U.S. Army as a 96D, Imagery Analyst (now 35G, Geospatial Intelligence [GEOINT] Imagery Analyst). In 2015, CW2 Watts was appointed a warrant officer and awarded military occupational specialty 350G, GEOINT Imagery Technician. He has served in various enlisted, noncommissioned officer, and warrant officer assignments, with multiple deployments in support of Operations Iraqi Freedom, New Dawn, Enduring Freedom, and Inherent Resolve.

Early in his warrant officer career, CW2 Watts implemented new intelligence architectures to integrate aerial reconnaissance tactical collection data for joint all-domain operations in Korea. Later, his employment of the Tactical Ground Station in Iraq was credited for successful targeting efforts against more than 800 high-value ISIS targets. Since 2018, as the officer in charge (OIC) for the Advanced Operations Course-GEOINT (AOC-G) and deputy OIC for the Digital Intelligence Systems Master Gunner (DISMG) Course, he has focused on building the comprehensive operational training to support the Military Intelligence Training Strategy and the establishment of the Army Foundry Platform.

When the coronavirus disease 2019 pandemic abruptly halted most Army training, CW2 Watts quickly pivoted his in-classroom training to a world-class virtual instruction platform. Collaborating with the most active DISMGs throughout the community, he operationalized the Gunner

Entry Program, which teaches the foundational concepts for understanding and implementing functional topologies to support tactical formations and missions. More than 400 intelligence professionals and leaders graduated the course between 30 March and 18 December 2020. Additionally, architecture and topology training was established within other important training programs, such as the 353T Military Intelligence (MI) Systems Maintenance/Integrator Warrant Officer Basic Course, the Warrant Officer Advanced Course, and most recently as required training for the 35F committee instructors. CW2 Watts also led training for nine DISMG classes with 98 graduates, and three AOC-G classes with 31 graduates.

CW2 Watts's awards include the Meritorious Service Medal, Army Commendation Medal (6 Oak Leaf Clusters), Army Achievement Medal (2 Oak Leaf Clusters), Presidential Unit Citation, Joint Meritorious Unit Award, Basic Aviation Badge, Basic Parachutist Badge, Drivers Badge, and numerous other service-related awards and decorations. He is also a recipient of the MI Corps Association's Knowlton Award. 

Awards For Excellence in Military Intelligence

Staff Sergeant Marcus L. Simpson 2021 Recipient of the Command Sergeant Major Doug Russell Award for Excellence in Military Intelligence

The CSM Doug Russell Award was created in 2001 in honor of an esteemed noncommissioned officer who personified the integrity, moral courage, and loyalty espoused in the NCO Creed. Russell served in uniform for 32 years, followed by 14 years as the Director of NCO and Enlisted Affairs, Director of Retiree Activities in the Association of the U.S. Army, and President of the American Military Society. The award is presented annually to an outstanding Soldier in the rank of sergeant or below, who has made a significant contribution to the MI Corps.



Born and raised at Eglin Air Force Base, Florida, SSG Marcus Simpson enlisted in the U.S. Army as a 35F, Intelligence Analyst, after graduating from high school. Upon completion of Advanced Individual Training at Fort Huachuca, Arizona, he volunteered to become Airborne and was assigned to the 307th Airborne Engineer Battalion (AEB), 3rd Brigade Combat Team, 82nd Airborne Division.


At the 307th AEB, SSG Simpson was assigned to the company intelligence support team (CoIST), providing intelligence support to the brigade's five battalions. In addition to serving in the CoIST, he served as the primary U.S. Central Command analyst for the brigade S-2, conducting morning briefings for the brigade staff and supporting more than 20 battalion-level and higher exercises. He also served as the primary company communications security custodian and was responsible for the unmanned aircraft system platoon's RQ-7 Shadow cryptologic fills, enabling more than 2,000 flight hours.

From 2019 to 2020, during a deployment with 3rd Brigade to Afghanistan in support of Operation Freedom's Sentinel, SSG Simpson served as the nightshift noncommissioned officer in charge at the Kandahar Intelligence Fusion Center. In this capacity, he reviewed more than 250 graphical intelligence summaries that were distributed throughout the Combined Joint Operations Area-Afghanistan and supported more than 75 United States

and coalition operations. During a period of base attacks, he maintained an indirect fire running estimate that local commanders used to assess and respond to enemy threat capabilities. SSG Simpson also maintained a running estimate of tensions with Iran following the death of Iranian commander Qasem Soleimani.

In January 2020, SSG Simpson was selected to travel to Jalalabad to establish the Regional Targeting Team-East (RTT-E) intelligence cell with 12 Afghan partners and members of the 7th Special Forces Group. As the senior intelligence analyst, he ensured the daily integration and synchronization of intelligence efforts with multiple units and the Combined Joint Intelligence and Operations Center. He also created a robust named area of interest overlay encompassing 88 districts in RTT-E that enhanced the region's direct action and targeting capabilities.

Redeploying on 1 May 2020, SSG Simpson served as the CoIST squad leader until mid-August. He was then selected to become the senior intelligence sergeant, Headquarters and Headquarters Company, 307th AEB, 3rd Brigade Combat Team, 82nd Airborne Division.

SSG Simpson's awards and decorations include the Army Commendation Medal with "C" device, Army Achievement Medal, Army Good Conduct Medal, National Defense Service Medal, Afghanistan Campaign Medal, Global War on Terrorism Service Medal, Noncommissioned Officer Professional Development Ribbon, Army Service Ribbon, Overseas Service Ribbon, NATO Medal, and Parachutist Badge. 

Awards For Excellence in Military Intelligence

Mrs. Andrea L. Rodman **2021 Recipient of the** **Ms. Dorothe K. Matlack Award** **for Excellence in Military Intelligence**

In 2018, the MI Corps established the Ms. Dorothe K. Matlack Award to honor a Department of the Army Civilian (GG-9-GG-12) who has made a significant contribution to MI within the previous three years. The Matlack Award is named for one of MI's early pioneers and champions of Army human intelligence efforts. Dorothe Matlack started her career in 1948 as a GS-2 File Clerk and retired in 1975 after serving 27 years in the Office of the Assistant Chief of Staff for Intelligence.



Mrs. Andrea Rodman's career began as an all-source intelligence analyst serving with the 101st Military Intelligence Battalion, 1st Infantry Division, in Wurzburg, Germany. She deployed from 2004 to 2005 with the division analysis and control element in support of Operation Iraqi Freedom, serving as a designated briefer to the division commander. Following her active duty career, she joined the Counter-Improvised Explosive Device Operations Integration Center, Joint Improvised Explosive Device Defeat Organization, where she led the Network Nodal Division. In 2006, Mrs. Rodman joined the 1st Information Operations (IO) Command where she served as an analyst focused on Iraq and Syria.

In 2012, Mrs. Rodman became the Intelligence Team Chief for the U.S. Central Command (CENTCOM) Regional Support Team, 1st IO Command G-2, a position she continues to hold. She leads analysts in the production and dissemination of intelligence support to information operations. Mrs. Rodman's technical skills and ability to understand the cognitive dimension of Middle Eastern populations and adversaries have been critical for IO planning. She provided an assessment of ISIS communications and vulnerabilities that identified exploitable weaknesses. These were then used to help bring down the group in Iraq and Syria. She was also instrumental in providing intelligence to CENTCOM J-39, Army Cyber Command, and multiple task forces that used existing strategic perceptions of ISIS

to identify specific tactical objectives. This allowed operators to foster division between groups, disrupt ISIS communications, and prevent the group's expansion. Mrs. Rodman and her team of analysts created assessments for each faction within ISIS that augmented planning by United States, coalition, and Iraqi forces to methodically drive ISIS from its strongholds in Iraq and eventually Syria.

Mrs. Rodman also proved instrumental in the success of cross-functional teams focused on Iran and Afghanistan. Following the January 2020 airstrike that killed Islamic Revolutionary Guard Corps Commander Qasem Soleimani, she was tasked with providing daily briefings to the Army Cyber Command commander and staff as well as weekly operations and intelligence briefings. Her efforts and dedication increased situational awareness and communications between various IO units, contributing to more synchronized planning support in the wake of this potentially dangerous international event.

Mrs. Rodman holds an associate degree in weapons of mass destruction and a bachelor's degree in international relations. She has completed the Army Management Staff College Basic Leadership Course and the Information Environment Advanced Analysis Course, and holds a Certificate in Women's Leadership from Cornell University.





Moments in MI History

How Did We Get Here?

The U.S. Army Intelligence School Moves to Fort Huachuca (Part 3 of 4)

by Lori Stewart, USAICoE Command Historian

This year is the 50th anniversary of Fort Huachuca as the Home of Military Intelligence. In recognition of this significant milestone, *Military Intelligence Professional Bulletin* (MIPB) is publishing a history of how Army intelligence training transitioned from being scattered across the United States after World War II to its current location at Fort Huachuca, Arizona, in 1971. MIPB will publish this story in four parts.

January–March 2021 issue

- ◆ The Story Begins at Fort Holabird.
- ◆ What's Wrong with Fort Holabird?
- ◆ MG Joseph McChristian and the Intelligence Center Concept.

April–June 2021 issue

- ◆ Blakefield Report Recommends Fort Huachuca.
- ◆ Could Fort Lewis Be a Better Answer?

July–September 2021 issue

- ◆ The Smith Study.
- ◆ Readyng the New Home.

July–September 2021 issue–Bonus Column

- ◆ Congressional Blowback.
- ◆ The Realization of a Dream.

Author's Note: All primary documents used in the writing of this article are in the historical documents collection at the U.S. Army Intelligence Center of Excellence. This includes correspondence related to the various studies, study reports, newspaper articles, testimony and statements given during the congressional hearings, the Army's information papers in preparation for the congressional hearings, the General Accounting Office's report, and the final report of the congressional subcommittee. Also used were the annual historical reports of the U.S. Army Intelligence School for 1966 to 1970 and the U.S. Army Intelligence Center and School for 1971 and 1972.

Introduction

On 4 May 1971, the U.S. Army Intelligence Center and School (USAICS) Commandant COL Charles W. Allen and CSM Clyde Fields unfurled the school colors at Fort Huachuca, Arizona, and proclaimed USAICS open for business. This action concluded an almost 5-year effort to find the ideal “home” for military intelligence (MI). The story involves multiple staff studies and cost analyses, congressional investigations and hearings, careful movement planning, and critical liaison between the staff at Fort Holabird, Maryland, and Fort Huachuca. Ultimately, it was the first step to the consolidation of several disparate Army intelligence training efforts into one entity now known as the U.S. Army Intelligence Center of Excellence.

The Smith Study

The Army was seriously considering Fort Huachuca as the site for its Intelligence Center, but political opposition put

the plan on hold. At the same time, MG Joseph McChristian, Department of the Army Assistant Chief of Staff for Intelligence, received data that made him doubt whether Fort Huachuca could support such a large center. He thought that Fort Lewis, Washington, would be suitable for a variety of reasons and made a pitch for Fort Lewis to GEN Bruce Palmer Jr., Vice Chief of Staff of the Army. GEN Palmer disagreed, saying that the center should go to Fort Huachuca, but to placate MG McChristian, he briefed Army Chief of Staff GEN William C. Westmoreland who deferred the decision in favor of yet another study.

So, on 24 September 1970, an independent study kicked off under the chairmanship of MG E.P. Smith, the Assistant Chief of Staff for Force Development. The Smith Board was directed to examine the feasibility of establishing an intelligence center and to recommend what activities it should include and where it should be located.

Unlike MG William H. Blakefield, commander of the Army Intelligence Center, MG Smith was not limited to any particular locations, so the size of his proposed center was not influenced by the limitations of any particular post. MG Smith's conclusion was that an intelligence center based on the 1968 U.S. Army Continental Army Command Center Team Concept, which collocated a branch school with its combat developments agency, was most desirable and feasible. He also reached the same conclusion as MG Blakefield and recommended that the intelligence center be located at Fort Huachuca.

MG Smith estimated that initially the intelligence center would be comprised of 912 permanent party military and civilian personnel (not including dependents) and a daily load of 2,000 students. An additional 723 personnel spaces were set aside for the future addition of the 184th MI Company and 14th MI Battalion if and when resources (primarily water and housing) permitted. His study, then, called for a total long-range population of 3,635. As for the cost, he estimated \$65.3 million, which included \$4.7 million for the initial move and immediate renovations at Fort Huachuca plus \$45.7 million for long-range construction of housing and academic facilities. The remaining \$14.9 million would cover the move of the 184th and 14th, if deemed possible at a later date.

When briefed on the Smith Board's recommendations, GEN Westmoreland reaffirmed his approval of the transfer of the U.S. Army Intelligence School (USAINTS) to Fort Huachuca, declaring, according to one attendee at the meeting, "Let's do it!"¹ Approval by the Secretary of the Army followed 2 days later, and MG McChristian backed the decision in mid-November. The public announcement was delayed until the appropriate congressional committees were briefed in mid-December.

Reading the New Home

On 5 January 1971, less than 3 weeks after the approval was granted, the USAINTS Commandant, COL Allen, sent a letter to the Deputy Chief of Staff for Military Operations, Department of Army, requesting a movement directive be published authorizing relocation commencement on 15 January. Some effort had been made as early as March the previous year before the relocation had been temporarily suspended. A team from Fort Huachuca and Sierra Vista, including the superintendent of Sierra Vista schools, visited

Fort Holabird to brief the staff and faculty on conditions at Fort Huachuca and the civilian community, and in early May, USAINTS personnel had visited Fort Huachuca to survey the available space. With all the approvals in place, the relocation effort kicked into high gear with the activation of a Movement Control Office at Fort Holabird to coordinate the transfer and liaise with personnel at Fort Huachuca. At this time, USAINTS civilian personnel were notified and advised of their options for relocation.

Members of the advance party arrived at Fort Huachuca on 28 January and established USAINTS Forward in one of the buildings in the old World War II cantonment area, which would serve as the school's academic campus until new facilities could be constructed.



The World War II cantonment area that served as the U.S. Army Intelligence Center and School's first academic complex.

U.S. Army photo

They began setting up preliminary operations for the move: coordinating classroom areas, barracks, equipment and supplies, and off-post housing. The serious housing issue became immediately clear. Relocating personnel were told it was best to leave their families in Maryland until they could locate adequate housing at Fort Huachuca or in the surrounding communities. When COL Donald M. Phillips, the Director of Instruction, arrived and took command of USAINTS Forward on 17 February, he directed that several barracks be set aside to house incoming personnel until other housing could be arranged.

By the end of the first week of February, a contract had been let for the refurbishment and renovation of the classroom and barracks buildings, including rewiring and installing air conditioning. Labor and material costs had skyrocketed 54 percent since the cost estimates had been made the previous year. Consequently, USAINTS personnel



Headquarters of the School Brigade in Building 67116.

tackled some of the smaller renovations themselves, such as painting, cleaning, carpentry, and grounds work, with materials provided by the post. According to one local news article, “As a measure of their desire to make Ft. Huachuca a permanent home, the men and women of the organization worked almost 11 man-years in a self-help program, refurbishing academic facilities, barracks, and mess halls.”² Because the school was to be located in an area previously planned for demolition, structures and roads had not been maintained, leading the post commander to request additional funds to cover road repairs and the replacement of

plumbing fixtures, heating equipment, doors, and doorjamb. By mid-April, 33 of 170 buildings had been renovated and work on another 46 begun.

Because academic operations continued at Fort Holabird while Fort Huachuca was being readied, the movement of the main body was conducted in phases beginning on 1 March. As a course graduated at Fort Holabird, the instructors and support staff closed down their operations and turned their facilities in; they then traveled to Fort Huachuca and prepared for the start of their next class at the new location. An advanced party of the School Brigade,

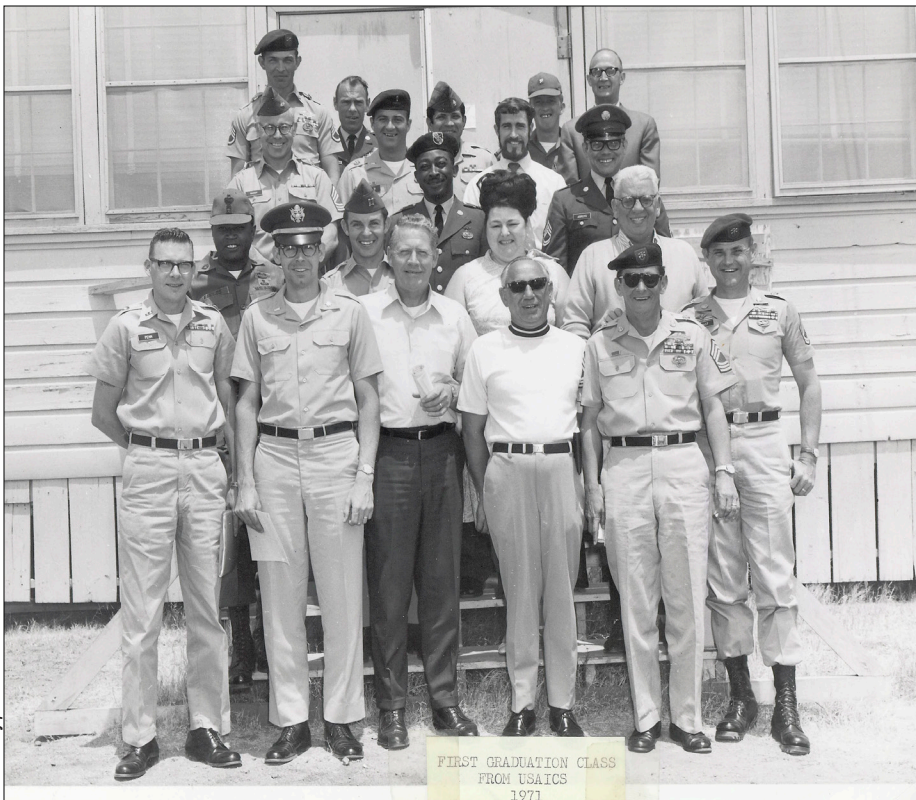
under the command of Deputy Brigade Commander LTC T.C. Gettings, and the First Student Battalion, commanded by CPT T.W. Flinchum, began operations at Fort Huachuca on 1 March.³ On 23 March 1971, USAINTS was redesignated USAICS.

Six weeks later, on 3 May, COL Allen officially relocated to Fort Huachuca and published General Order 1, attaching USAICS to Sixth Army for administrative and logistical support. In a ceremony the following day attended by 300 staff, faculty, and students, COL Allen officially unfurled USAICS’ colors. MG W.B. Latta, Post Commander and Commanding General of the U.S. Strategic Communications Command, welcomed the new organization, declaring: “You are the beginning of something. The beginning of permanent roots for the intelligence school.”⁴ COL Allen hosted a second ceremony later in the afternoon for USAICS personnel only, at which he officially closed USAINTS Forward and opened Headquarters, USAICS.

As the first six classes began on 4 May, 71 percent of USAINTS personnel had completed the relocation, and USAICS was prepared to conduct 32 different courses to a daily student load of 1,200 to 1,300.



Sign at the Main Gate of Fort Huachuca in 1971, listing the U.S. Army Intelligence Center and School as a tenant.



The first class to graduate from the U.S. Army Intelligence Center and School in 1971.

Over the next several months, additional personnel made the move, including 46 of 146 civilian personnel previously employed at Fort Holabird. In the months following, USAICS hosted the Commanding General of U.S. Army Continental Army Command, GEN Ralph Haines, as well as Secretary of the Army Stanley R. Resor and Sergeant Major of the Army Silas Copeland. On 2 September 1971, COL Elvin Dalton assumed command of USAICS, replacing COL Allen.

That same day, the last class in session at Fort Holabird, an MI Officer Advanced Course, graduated, thus terminating intelligence training at the Maryland post. The move was officially complete and the Army had its new Intelligence Center. 🇺🇸

Endnotes

1. COL Ben Anderson, handwritten note, n.d.
2. "Intelligence School Celebrates 1 Year at Fort Huachuca," *Huachuca Scout*, 31 August 1972.
3. The brigade commander COL R.W. Bertholf remained at Fort Holabird with the brigade until mid-May. The Second Student Battalion also remained at Fort Holabird but deployed its companies in phases. Company D was the last major subordinate element to deploy to Fort Huachuca on 30 September 1971.
4. "I-School Standard Planted; 'Permanent Roots' Take Hold," *Huachuca Scout*, n.d.



COL Elvin Dalton, Commandant, U.S. Army Intelligence Center and School, September 1971 to May 1973.

Next time in this series:

- ◆ Congressional Blowback.
- ◆ The Realization of a Dream.



Moments in MI History

How Did We Get Here?

The U.S. Army Intelligence School Moves to Fort Huachuca (Part 4 of 4)

by Lori Stewart, USAICoE Command Historian

This year is the 50th anniversary of Fort Huachuca as the Home of Military Intelligence. In recognition of this significant milestone, *Military Intelligence Professional Bulletin* (MIPB) is publishing a history of how Army intelligence training transitioned from being scattered across the United States after World War II to its current location at Fort Huachuca, Arizona, in 1971. MIPB will publish this story in four parts.

January–March 2021 issue

- ◆ The Story Begins at Fort Holabird.
- ◆ What's Wrong with Fort Holabird?
- ◆ MG Joseph McChristian and the Intelligence Center Concept.

April–June 2021 issue

- ◆ Blakefield Report Recommends Fort Huachuca.
- ◆ Could Fort Lewis Be a Better Answer?

July–September 2021 issue

- ◆ The Smith Study.
- ◆ Readyng the New Home.

July–September 2021 issue–Bonus Column

- ◆ Congressional Blowback.
- ◆ The Realization of a Dream.

Author's Note: All primary documents used in the writing of this article are in the historical documents collection at the U.S. Army Intelligence Center of Excellence. This includes correspondence related to the various studies, study reports, newspaper articles, testimony and statements given during the congressional hearings, the Army's information papers in preparation for the congressional hearings, the General Accounting Office's report, and the final report of the congressional subcommittee. Also used were the annual historical reports of the U.S. Army Intelligence School for 1966 to 1970 and the U.S. Army Intelligence Center and School for 1971 and 1972.

Introduction

On 4 May 1971, the U.S. Army Intelligence Center and School (USAICS) Commandant COL Charles W. Allen and CSM Clyde Fields unfurled the school colors at Fort Huachuca, Arizona, and proclaimed USAICS open for business. This action concluded an almost 5-year effort to find the ideal “home” for military intelligence (MI). The story involves multiple staff studies and cost analyses, congressional investigations and hearings, careful movement planning, and critical liaison between the staff at Fort Holabird, Maryland, and Fort Huachuca. Ultimately, it was the first step to the consolidation of several disparate Army intelligence training efforts into one entity now known as the U.S. Army Intelligence Center of Excellence.

Congressional Blowback

While personnel at USAICS were gearing up to train the Army's intelligence personnel, members of Congress were

preparing to reopen the case on the school's relocation. On 21 April 1971, New York Congressman Otis Pike, a member of the House Armed Services Committee, requested MG Joseph McChristian, Department of the Army Assistant Chief of Staff for Intelligence, visit his office to discuss Fort Lewis, Washington, as an option for the intelligence center, rather than Fort Huachuca. In response, the Army sent a fact sheet contrasting the advantages and disadvantages of Fort Huachuca and Fort Lewis. A month later, Maryland Congressman Clarence Long, who had been against the closure of Fort Holabird since the beginning, wrote a letter to Secretary of the Army Stanley R. Resor requesting that the Army reverse the decision to move the school to Fort Huachuca. Members of the Military Construction Subcommittee of the House Appropriations Committee, responding to constituents' complaints about the housing situation at Fort Huachuca, called a June hearing at which

they reprimanded the Army for providing Congress with inadequate data. Finally, not happy with what he called the Army's "evasions and mush," Congressman Pike requested the General Accounting Office (GAO) conduct an audit of the move.¹

GAO began its investigation on 26 July 1971 and published its final report on 15 March 1972 amid accusations by Congressmen Long and Pike that the Army had intentionally delayed its publication until the Intelligence Center reached full operations at Fort Huachuca.² While the Army's counsel deemed the report impartial, Congressman Long used the report as evidence that the Army had "deliberately deceived" Congress and the public by withholding information about the water and housing problems at Fort Huachuca. He charged that "the Army did not tell Congress that its move to Fort Huachuca was a mere ploy in its real ambition to set up a 10,000-man Intelligence Center in the Arizona desert."³ The Army responded to Congressman Long's accusations admitting its error in estimating the housing situation but defending its efforts to ensure the Intelligence Center established at Fort Huachuca would not exacerbate the water problems.⁴

Congressman Pike used the GAO report to call for official hearings before a Special Subcommittee of the Armed Forces Investigation Subcommittee, which took place on 10 May 1972. In his opening statement, Congressman Pike argued that the Army had not been fully supportive of the subcommittee's investigation or the GAO study. This had hindered the subcommittee's ability to "develop all of the basic facts necessary for a valid judgement" about whether the Army had made the best decision to move the Intelligence Center to Fort Huachuca.⁵ Congressman Long then testified at length about the housing situation and concluded that the move from Fort Holabird was an "expensive transfer for which there was no real military justification."⁶ The Director of the GAO's Logistics and Communications Division, J. Kenneth Fasick, called the Army's planning "inadequate" and agreed with Congressman Long that "this was not a good example of a case study for relocation of military bases."⁷

Congressman Pike's star witness seemed to be MG McChristian, now retired, who recounted his efforts to achieve a large, integrated intelligence center and his preference for Fort Lewis. While he believed that Army Chief of Staff GEN William C. Westmoreland favored his more extensive concept of an intelligence center, he understood the myriad considerations that had to go into the final decision and the reasons why the Army Chief of Staff approved Fort Huachuca. He testified that "I believed in this center very

strongly" and while "it is better at [Fort] Huachuca today than it was at [Fort] Holabird," he lamented, his recommendations were overruled. Congressman Pike concluded, "You have been on the side of angels through this."⁸

BG Oliver Dillard, the Director of Intelligence Support in the Office of the Assistant Chief of Staff for Intelligence, read a prepared statement that was cut short because of time.



BG Oliver Dillard was chosen to represent the U.S. Army at the congressional hearings in 1972.

BG Dillard stressed that much of the confusion was due to a misunderstanding of the myriad studies conducted for two interrelated but separate subjects—the move of U.S. Army Intelligence School (USAINTS) from Fort Holabird to Fort Huachuca and the Intelligence Center Concept. He stated, "Somehow the early conceptual studies and documents, which were part of the decision making process, but which did not represent formal decisions, were mistakenly credited by some people as being the final Army decision. Thus, the issues involving the move of the school and the plans for an Intelligence Center became distorted."⁹ MG Linton S. Boatwright, Deputy Chief of Staff for Personnel's Director of Individual Training and chairman of a Long-Range Stationing Study Group (LRSSG), also testified, stressing that in making the recommendation to move USAINTS to Fort Huachuca, his LRSSG took into account the availability of housing, requirements for long-range construction, and water limitations. For all the advantages that Fort Huachuca had over other installations, "I strongly felt, and I still strongly feel, that from an operational point of view Fort Huachuca is the place for the Intelligence Center."¹⁰

The subcommittee report was published on 12 July 1972. In summarizing its findings, the report accused the Army of pre-choosing Fort Huachuca as the location of the intelligence center before conducting adequate studies, then "painting over the shortcomings...to justify its selection"

and tailoring its Intelligence Center Concept to fit existing conditions. It further stated, "If a qualitative improvement in intelligence was required, and if the Center was to satisfy that requirement, the Army has chosen to dispense with that improvement by its acceptance of the abbreviated Center/Team. It appears that is a high price to pay for the luxury of not admitting a mistake in the selection of Fort Huachuca." In addition to suggesting that the Secretary of Defense establish a standard format for future relocation and closure studies and cost analyses, the subcommittee recommended that the Army relook at its Intelligence Center Concept and determine, "from the standpoint of economy and efficiency," if it would be better located at Fort Lewis or some other "suitable" location.¹¹

Regardless of the subcommittee's findings, the Army maintained that selecting Fort Huachuca as the site of the Intelligence Center and School was not a mistake. No installation within the continental United States could have supported MG McChristian's full Intelligence Center Concept without additional relocations and transfers of other activities, which would have substantially added to the cost. Consequently, MG McChristian's Intelligence Center Concept was never approved. Instead, the Smith Board reconfirmed the more immediate and practical need to find a location where the Army could better train its intelligence personnel and collocate them with their counterparts in the Combat Developments Command Intelligence Agency in accordance with the original U.S. Army Continental Army Command Center Concept. The various studies conducted in late 1969 and early 1970 clearly showed that Fort Huachuca was ideal for training, as well as developing and testing sensitive intelligence equipment. The post's superior advantages—good classrooms, plenty of airspace and training space, and an uncluttered electromagnetic spectrum—also checked off many of MG McChristian's requirements for an adequate intelligence center. Responding to the subcommittee's report, Secretary of the Army Robert Froehlke, who had been appointed to the position in July 1971 upon the resignation of Secretary Resor, expressed concern over accusations that the Army had "deliberately engaged in a scheme to deceive Congress and the American public."

He further stressed that "the operational reasons for selecting Fort Huachuca are sound and, when other Army stationing considerations have been taken into account, Fort Huachuca is the most appropriate location for the center. Therefore, I consider a further study—raising the specter of again moving the school and those personnel who moved to Fort Huachuca—to be unnecessary."¹²

The Realization of a Dream

By the time the congressional hearings had come to a close, the USAICS had been operating at Fort Huachuca for more than a year. Instructors and staff, as well as the Army's senior intelligence leaders were generally positive about the new location, stating, "The advantages of the move have generally been realized. In addition, there has been a significant heightening of the morale of both students and instructors brought about by the move from the crowded, grimy [Fort] Holabird to the clean desert air of [Fort] Huachuca."¹³

Within the first year of operations at Huachuca, USAICS staff and faculty had developed new Noncommissioned Officer Basic and Advanced courses, stood up a task force to develop the program of instruction for the new MI Officer Basic Course, added field training exercises to courses that had never had them, and submitted for approval plans for the construction of a new academic complex to replace the World War II buildings the center and school were currently using. In 1973, the Combat Developments Command Intelligence Agency made its move to Fort Huachuca, and USAICS absorbed the Combat Surveillance and Electronic Warfare School. The first MI Officer Basic Course started on 29 March, the realization of a long-desired goal. In addition to being authorized its own shoulder sleeve insignia, USAICS was also authorized a general officer as commander. On 7 May 1973, BG Harry Hiestand took command of USAICS replacing COL Elvin Dalton, who had shepherded the center through its first 2 years at the Arizona location.

In the coming years, USAICS continued to grow. In October 1976, responsibility for the Army Security Agency Training Center and School and the Army Security Agency Combat Development Activity at Fort Devens, Massachusetts, transferred to the U.S. Army Training and Doctrine Command (TRADOC), which in turn placed those organizations under the command of USAICS. In the process, the Army Security Agency school was redesignated the U.S. Army Intelligence School Devens (USAISD).




Robert Froehlke, Secretary of the Army, July 1971 to May 1973.



Headquarters of the U.S. Army Intelligence School at Fort Devens.

Responsibility for all MI training was now consolidated at USAICS, but training was still being conducted at four locations: USAICS at Fort Huachuca; USAISD at Fort Devens; the USAISD Detachment at Goodfellow Air Force Base, Texas; and the USAISD Detachment at Corry Station, Florida.¹⁴

The final step in the consolidation occurred on 1 October 1990, when TRADOC assumed command of Fort Huachuca as part of the 1988 Base Realignment and Closure (BRAC) initiative. The U.S. Army Information Systems Command (formerly the Strategic Communications Command and known today as NETCOM) became a tenant activity on post, while the U.S. Army Intelligence Center became the post's senior mission. BRAC 1988 also resulted in the transfer of all the training elements of USAISD to Fort Huachuca.

This move was completed in 1994. After more than a quarter of a century of effort, Fort Huachuca had finally become the "Home of Military Intelligence" in an all-embracing sense. 



Aerial view of the U.S. Army Intelligence Center complex in the mid-1990s.

Endnotes

1. *Testimony before the Armed Services Subcomm. of the Comm. on Armed Services, House of Representatives, on Relocation of the U.S. Army Intelligence School from Fort Holabird to Fort Huachuca*, 92nd Cong., 2nd Sess. (10 May 1972) (statement of Congressman Otis Pike), 1.
2. In fact, the report had not been ready for security review until 11 February 1972, and the Department of the Army completed its review on 18 February, stating while the report was not classified, it did have stationing information that had not yet been approved. The Army asked that the report not be publicly released.
3. "Long Charges Army Deceit in Holabird Move," *Baltimore News-American*, 25 March 1972.
4. In January 1972, the Army had requested \$2.6 million to construct an additional 100-family housing units. They now identified a deficit of 974 units.
5. *Testimony before Armed Services Subcomm.* (statement of Congressman Pike), 2.
6. *Testimony before Armed Services Subcomm.* (statement of Congressman Clarence D. Long), 6.
7. *Testimony before Armed Services Subcomm.* (statement of J. Kenneth Fasick, Director, Logistics and Communications Division, General Accounting Office), 12; and *Testimony before Armed Services Subcomm.* (statement of Congressman Long), 7.
8. *Testimony before Armed Services Subcomm.* (statement of MG Joseph McChristian), 17, 24.
9. *Testimony before the Armed Forces Investigating Subcomm.* (10 May 1972) (statement of BG Oliver Dillard, Director, Intelligence Support, Office of the Assistant Chief of Staff for Intelligence), 12; and *Testimony before Armed Services Subcomm.* (statement of BG Dillard), 40–41.
10. *Testimony before Armed Services Subcomm.* (statement of MG Linton S. Boatwright), 52.
11. *Report of the Armed Services Investigating Subcomm. of the Comm. on Armed Services, House of Representatives, Relocation of the US Army Intelligence School from Fort Holabird to Fort Huachuca*, 92nd Cong., 2nd Sess. (12 July 1972), 2, 3, 5, 13.
12. Secretary of the Army Robert Froehle to Honorable F. Edward Hebert, Chairman, Committee on Armed Services, House of Representatives, letter, 22 September 1972.
13. MAJ Kilday, *Information Brief: Advantages of Locating the Intelligence Center at Fort Huachuca*, n.d.
14. Because the U.S. Air Force was executive agent for cryptologic analysis and reporting and the U.S. Navy was executive agent for non-communications signals analysis, Army students trained at Goodfellow Air Force Base and Corry Station, respectively, for those missions.



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

What we need from you:

- ◆ Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.

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

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

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

MIPB (ATZS-DST-B)

Dir. of Doctrine and Intel Sys Trng

USAICoE

550 Cibique St.

Fort Huachuca, AZ 85613-7017



Headquarters, Department of the Army.

This publication is approved for public release.

Distribution unlimited.

PIN: 211409-000