MI Professional Bulletin
January–March 2021
PB 34-21-1

U.S. Army Reserve and Army National Guard Intelligence Operations

Twice the Citizen

Always Ready, Always There

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

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

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

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

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

By Order of the Secretary of the Army:

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

Official:

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

2118101

From the Editor

The following themes and deadlines are established:

October–December 2021, *Intelligence Disciplines.* This issue will focus on new, critical, and refocused aspects of the intelligence disciplines and complementary intelligence capabilities. Deadline for article submission is 26 August 2021. **This is a change from the previously published submission deadline.**

January–March 2022, *Targeting and Intelligence.* This issue will focus on how intelligence operations are evolving to support the delivery of lethal and nonlethal effects against intended targets. Deadline for article submission is 21 September 2021.

April–June 2022, *Army Intelligence and Modernization.* This issue will focus on how Army intelligence will transform to support a multi-domain capable force by 2035. Deadline for article submission is 17 December 2021.

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

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

Tracey A. Remus
Editor

MI Professional Bulletin

January–March 2021
PB 34-21-1
Volume 47 Number 1

We would like to thank SGM Stacey Gant, U.S. Army Reserve Intelligence Sergeant Major, U.S. Army Intelligence Center of Excellence Reserve Forces Office; and CW4 James Graham, Senior Warrant Officer Advisor and Digital Intelligence Systems Master Gunner, Army National Guard G-2, for their assistance as the "stakeholders" for this issue. Their ability to connect with authors within their respective components was key to bringing the issue together.

Features

DEPARTMENTS

Always Out Front

by Major General Anthony R. Hale
Commanding General
U.S. Army Intelligence Center of Excellence

This edition of the *Military Intelligence Professional Bulletin* (MIPB) spotlights our brothers and sisters serving in components (COMPOs) 2 and 3 who remain an integral part of our military intelligence (MI) Corps and our Army. During my 32 years of service, I have observed a common thread, which shouldn't be lost on us as a profession—the important contributions that the U.S. Army Reserve and Army National Guard make to our national security. I experienced this firsthand as a deployed battalion commander and as the Resolute Support J-2 while integrating U.S. Army Reserve enablers, and during my tenure as the U.S. Army Forces Command G-2 working with both COMPOs. To compete and potentially engage in conflict with a peer or near-peer competitor in a multi-domain operations environment, we need a Total Force that is "organized, trained, sustained, equipped and employed to support combatant commander requirements… to achieve anticipated objectives."[1]

This quarter's MIPB not only highlights new ways to train COMPOs 2 and 3 but also offers innovative takes on existing capabilities and training opportunities. My three objectives to *Build Leaders, Drive Change,* and *Inform,* along with my number one priority—*People*—are important to all COMPOs. The only way we will achieve a multi-domain capable force by 2028 and a multi-domain ready force by 2035 is to focus our efforts on the right things at the right time.

Build Leaders

One way to build leaders is to optimize the use of existing training and available infrastructure. A prime example includes incorporating several Army resources into unit training, such as the Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) and Foundry sites, supplemental training from organizations outside the Department of Defense, and the use of mission training complexes and Army Reserve Intelligence Support Centers. COL Rose Keravuori's article has a key point that I don't want you to miss—leaders at brigade and echelons below must ensure training is planned correctly to meet the identified training goals. Her article goes into detail about best practices when preparing to use existing training resources and emphasizes proactive engagement for leaders at all levels.

Drive Change

It is crucial that we adapt training across the U.S. Army Reserve when movement or access to Army Reserve Intelligence Support Centers is difficult. Decentralization through virtual resources is one of the keys to achieving this objective. The Intelligence and Electronic Warfare Smartbook, highlighted in SFC Hurst's article, is a centralized repository of documentation and training resources for MI Systems Maintainers/Integrators. This resource is one of several initiatives our Reserve forces are undertaking to create products accessible by Soldiers from remote locations.

A recent example of driving change is the work initiated by two 111th MI Brigade Soldiers, SPC Kendall Lydon and SFC Saquawia Pennington, who are changing the way we approach the Army Chief of Staff's top three issues: suicide, sexual harassment and sexual assault, and racism and extremism. SPC Lydon and SFC Pennington combined a bottom-up analysis with top-down understanding of the Army to develop an innovative, grassroots program designed to tackle sexual harassment and improve our SHARP program. From that program's success, they began developing a broader program (RAPID: Resiliency, Awareness, Prevention, Inclusion, and Diversity) to achieve effects across all three of the issues and briefed both programs to the Chief of Staff and Sergeant Major of the Army. Their success is now driving change across the Army, as other installations examine how to implement these programs. As leaders in the Intelligence Corps, we intuitively understand how and why we train the way we

do, but in order to foster innovation, we must empower our youngest and brightest to solve problems we may not know exist.

Inform

This quarter's Training Readiness column gives you a good understanding of the One Army School System (OASS). It describes how OASS operates and how it supports the development of the Total Force. It also highlights some of the unique training challenges facing COMPOs 2 and 3.

The article by Mr. David Summers introduces a new distance learning opportunity available through the Human Intelligence Training–Joint Center of Excellence. The J2X Staff Officer Course Distance Learning replaces the former resident J2X Course. The pilot course graduated on 2 March 2021. The new course is more rigorous in its design and uses problem solving in its instruction methodology.

People

One of the ways we take care of people is to ensure that every member of our team is ready to contribute. We will continue to build and maintain all COMPOs with talented, capable, and competent MI professionals. These professionals must be ready to support our Army in multi-domain operations within large-scale ground combat operations and be able to contribute with the level of expertise the Army has come to expect from our Intelligence Corps. –Desert-6

Endnote

1. Secretary of the Army, Army Directive 2012-08, *Army Total Force Policy* (Washington, DC, 4 September 2012), 1.

Always Out Front!

Doctrine Bonanza

As of this writing, 17 May 2021, ATP 2-19.4, *Brigade Combat Team Intelligence Techniques,* and ATP 2-22.4, *Technical Intelligence,* have been approved and are undergoing the process for official Army publishing on the Army Publishing Directorate's website, https://armypubs.army.mil/.

While waiting for official publication, the U.S. Army Intelligence Center of Excellence Doctrine Division has posted the publications as Final Approved Drafts (FADs) to the Intelligence Knowledge Network (IKN) at https://ikn.army.mil/apps/IKNHostedWebsites/MIDoctrine (common access card login required). A FAD is an unofficial copy of an approved doctrinal publication that can be disseminated for interim use by Army forces prior to official publication. Once the official Army techniques publications are published on the Army Publishing Directorate's website, they will be removed from IKN.

ATP 2-19.4 is the Army's doctrinal publication describing brigade combat team (BCT) intelligence techniques. The techniques in this publication apply across the entire range of military operations with an emphasis on large-scale combat operations at echelons brigade and below within the infantry, armored, and Stryker BCTs. ATP 2-19.4 discusses the doctrinal duties and responsibilities of the BCT intelligence warfighting function and describes the intelligence process within the context of the operations process.

ATP 2-22.4 provides doctrinal guidance and techniques on how theater to battalion intelligence staffs assist commanders in leveraging national technical intelligence (TECHINT) organizations to provide the exploitation necessary to support intelligence analysis. It focuses on the collection, processing, analysis, and exploitation of foreign materiel found within the area of operations. TECHINT's systematic approach integrates multiple organizations, disciplines, functions, and processes to produce technical analysis for applications across national to tactical intelligence objectives.

CSM Forum

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

Time—There is no doubt about the importance of people, money, equipment, and any number of resources with regard to training, but none of these matter without time. Time is one of those components that many people assume leaders understand how to manage, and it should be an implied task. It is not that time management is difficult, but it can be complex when associated with a never-ending list of priorities. Truly understanding the importance of time and its proper use directly relates to readiness. Our Army is in the midst of modernizing in preparation for the challenges posed by emerging threats in today's world, which comes with a number of considerations that require us to put a lot of value on time.

Although our Army has progressed in many ways, in the past we managed some actions with regard to time that we may want to reconsider. The Army used training, support, and mission cycles from the old 2002 version of FM 7-0, *Training the Force,* that dictated how commanders could prioritize time and resources while ensuring the accomplishment of specific missions. This may not work for all military intelligence units, but we could potentially use portions of these concepts today. Another important aspect of time management was the commander's enforcement of locking in training calendars. Companies, and sometimes higher echelons, will always play catch-up as priorities and requirements shift, forcing commanders to alter their schedules. If commanders and their first sergeants and command sergeants major do not guard time like any other resource and learn to manage it, we will not be able to prepare for the next mission.

We were fighting a counterinsurgency war long before many of our current Soldiers joined the Army, including many of our senior leaders. Preparing to conduct multi-domain operations within large-scale ground combat operations requires updates to equipment and training. Different units will have different capabilities, meaning there will be multiple training requirements. This will drive us to develop new and creative ways to mesh all the equipment to accomplish the mission, which will require a great deal of planning. The Army's iterative plan to equip units will not be completed quickly, further exacerbating the need to ensure time is managed properly at each echelon. After new equipment arrives, noncommissioned officers need to be certified so that they can ensure Soldiers are properly trained on the equipment and the mission. All of this takes time.

Admittedly, the need to synchronize training for components (COMPOs) 1, 2, and 3 is rather rhetorical. Realizing the importance of time in this area is unbelievably important. As previously stated, the equipment may not be the same in each unit, and the training needs are somewhat different as we move from counterinsurgency to multi-domain operations. What makes this so crucial for COMPOs 2 and 3 is again time. When Soldiers train only 2 days a month and 2 weeks a year, in comparison to a COMPO 1 unit, time management takes on an even more important meaning. Defining mission requirements in detail will provide focus for all the issues previously mentioned in a finite amount of time for the U.S. Army Reserve and National Guard.

Our Army is adapting and preparing for the future threats, and it is clear there are many requirements to securing our readiness. Additionally, we spend a great deal of time taking care of our people and ensuring leaders at every echelon are creating an environment that builds trust and provides positive leadership. All of these requirements cause a definitive strain on time. Obviously, taking care of people is the priority, because if that does not happen, there is no mission. MG Anthony Hale, U.S. Army Intelligence Center of Excellence Commanding General, repeatedly tells leaders to look at what they have to do, want to do, and will not do, and then assign time and resources to the first two areas. We will meet our requirements, but we will need to prioritize requirements and prepare leaders to manage time as one of our most important resource.

Always Out Front!

Technical Perspective

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

As our Army continues its transition from counterinsurgency operations to multi-domain operations within large-scale ground combat operations, the capabilities that the U.S. Army Reserve and the Army National Guard intelligence personnel and formations bring to bear are more important than ever. The "Citizen-Soldier" nature of these intelligence professionals serving in Reserve and Guard units bring many unique and specialized skillsets to the fight. It is not uncommon for military intelligence (MI) professionals within our reserve forces to have advanced skillsets in national security related fields different from their military occupational specialties, making them combat multipliers within their formations.

Key to cross-component integration here at the U.S. Army Intelligence Center of Excellence is the One Army School System (OASS). OASS is designed to standardize education for Army schools, regardless of component, and is key to maintaining a trained and ready intelligence force. OASS is vital to MI training, ensuring that all courses and occupational specialties are held to the same high standard. It also offers training opportunities and delivery of instruction tailored to meet the needs of our professionals who do not wear the uniform every day. As we transition to large-scale ground combat operations, ensuring we have a trained and ready force across the intelligence enterprise will be paramount, and "OASS will ensure Soldiers, regardless of component, attend Professional Military Education (PME) or functional training courses on time and to standard."[1]

Executing relevant and realistic training is vital to preparing the total force to fight in the future operational environment. Both the U.S. Army Reserve and the Army National Guard are actively engaged in this effort. The Army Reserve Intelligence Support Centers (ARISCs) stand ready to provide intelligence training, even during these challenging times. CW4 Brian Harris, an ARISC all-source intelligence technician, has been critical in adapting training to the virtual environment and providing instruction via Microsoft Teams using the Commercial Virtual Remote initiative (also known as CVR). Through this alternative medium, the MI Readiness Command continues to train a variety of courses, including the Basic Open-Source Intelligence Course, Intelligence Documents and Drafting course, and several other critical curricula, ensuring MI Soldiers are well trained and ready to fight.

MI Soldiers in the Army National Guard are also actively training to support large-scale ground combat operations. Soldiers from the Minnesota Army National Guard's 1st Armored Brigade Combat Team, 34th Infantry Division, executed the first National Training Center (NTC) rotation in the era of the coronavirus disease 2019. Upon arrival at NTC, "intelligence sections and units began to work on MI systems set-up and integration, [reception, staging, onward movement, and integration] RSOI tasks and Intelligence Preparation of the Battlefield (IPB) in support of the Military Decision Making Process (MDMP). IPB and intelligence support to MDMP were conducted continuously throughout the entire rotation. . . .The rotation provided many MI Soldiers cross-training opportunities in Current Operations, Plans, [brigade intelligence support element] BISE and Fires/Targeting."[2]

As we look to create multiple dilemmas for our adversaries across all domains, it is critical that, as intelligence professionals, we think and train in terms of the "total force," not three separate components. As a former instructor for our Warrant Officer Intermediate Level Education and Warrant Officer Senior Service Education Phase III courses, I saw firsthand the great benefit and sense of teamwork that developed when students across all Army components were learning and sharing ideas together in class. It will undoubtedly take the total force to secure our vital national security interests in both competition and conflict.

As I close out this column, I would like to thank you and your families for your daily sacrifice, selfless service, and contributions to the Army in the defense of our Nation.

Endnotes

1. "The One Army School System," STAND-TO!, February 27, 2011, https://www.army.mil/article/52524/the_one_army_school_system.

2. Chloee Carlson, "1/34th ABCT First Unit to Conduct NTC Post-COVID," *ARNG Intelligence & Security Newsletter* 3 (30 October 2020): 11.

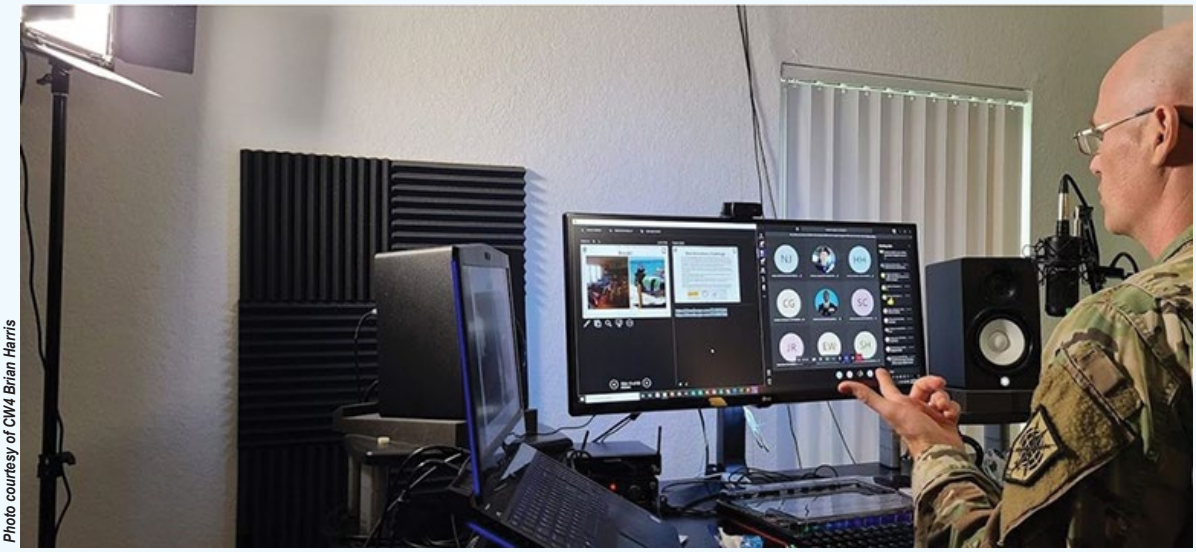


Photo courtesy of CW4 Brian Harris

CW4 Brian Harris, an all-source intelligence technician at the Army Reserve Intelligence Support Center in Orlando, FL, provides instruction using Microsoft Teams through the Commercial Virtual Remote initiative.

One Team, One Fight! Always Out Front! and Army Strong!

Not Your Grandma's Collection Management

As of this writing, 17 May 2021, ATP 2-01, *Collection Management,* has been approved and is undergoing the process for official Army publishing on the Army Publishing Directorate's website, https://armypubs.army.mil/.

While waiting for official publication, the U.S. Army Intelligence Center of Excellence Doctrine Division has posted the publication as a Final Approved Draft to the Intelligence Knowledge Network (IKN) at https://ikn.army.mil/apps/IKNHostedWebsites/MIDoctrine (common access card login required). Once the official Army techniques publication is published on the Army Publishing Directorate's website, https://armypubs.army.mil/, it will be removed from IKN.

ATP 2-01 establishes doctrine for the specific tasks of the collection management (CM) process. CM is a dynamic, continuous, and interactive process requiring constant cooperation between the commander, the CM team, and the rest of the staff. CM requires creativity and critical thinking to meet the level of detail necessary to satisfy the commander's requirements. Key changes during the revision of ATP 2-01 include—

- The CM logic chart, see page 8.
- Addition of joint CM discussions of essential element of information, collection operations management, and collection requirements management.
- Longer and better discussion of CM relative to the military decision-making process.
- Restructured chapters for a better flow of information.
- Significant addition/revision of supporting tables and graphics.
- Better discussion of requirements management and mission management as well as the addition of execution management.
- New construct added where intelligence requirements comprise priority intelligence requirements (mandatory), targeting intelligence requirements (optional), and other intelligence requirements (optional).

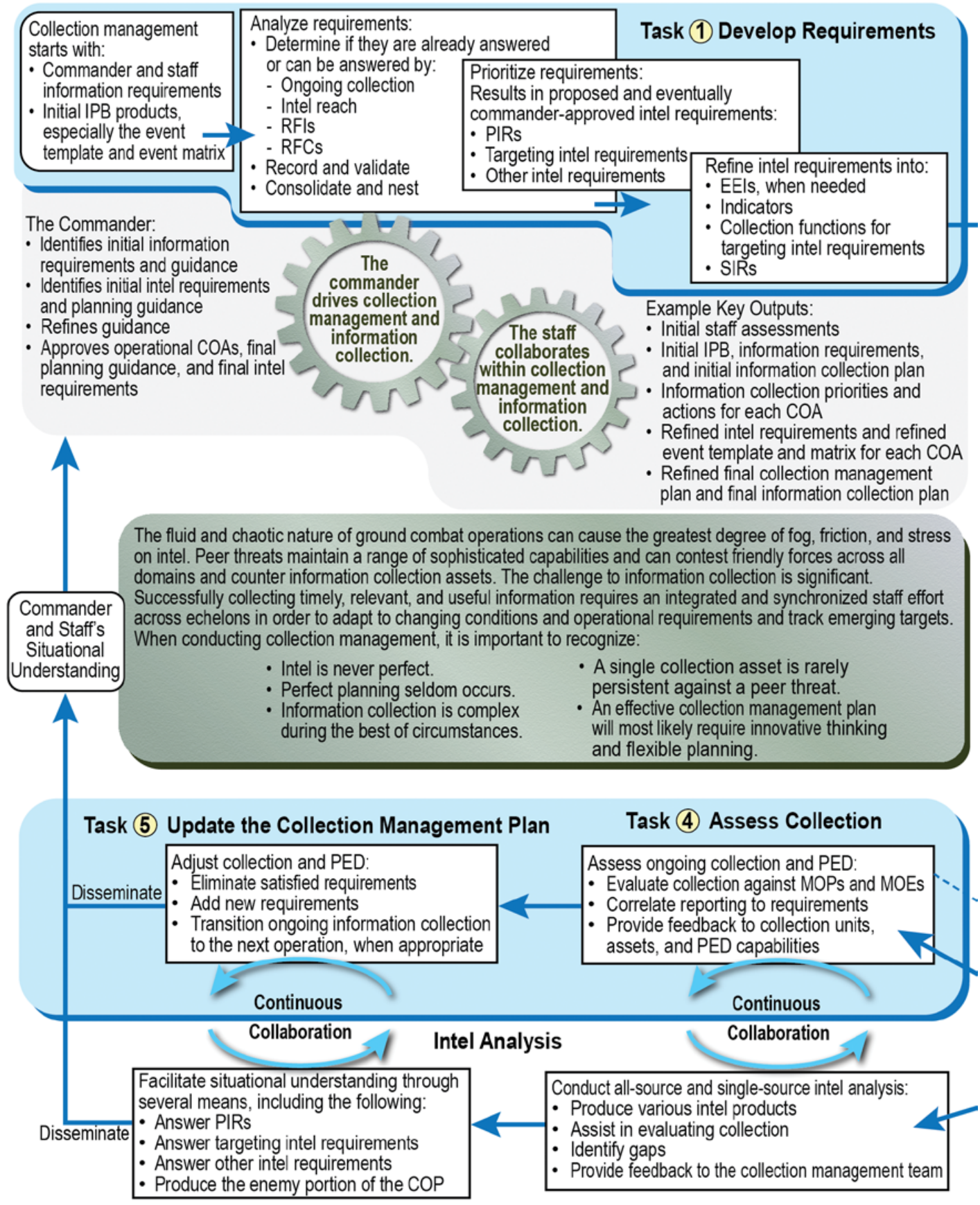
Military Intelligence Doctrine Library

Authenticated MI Doctrine can be found at:

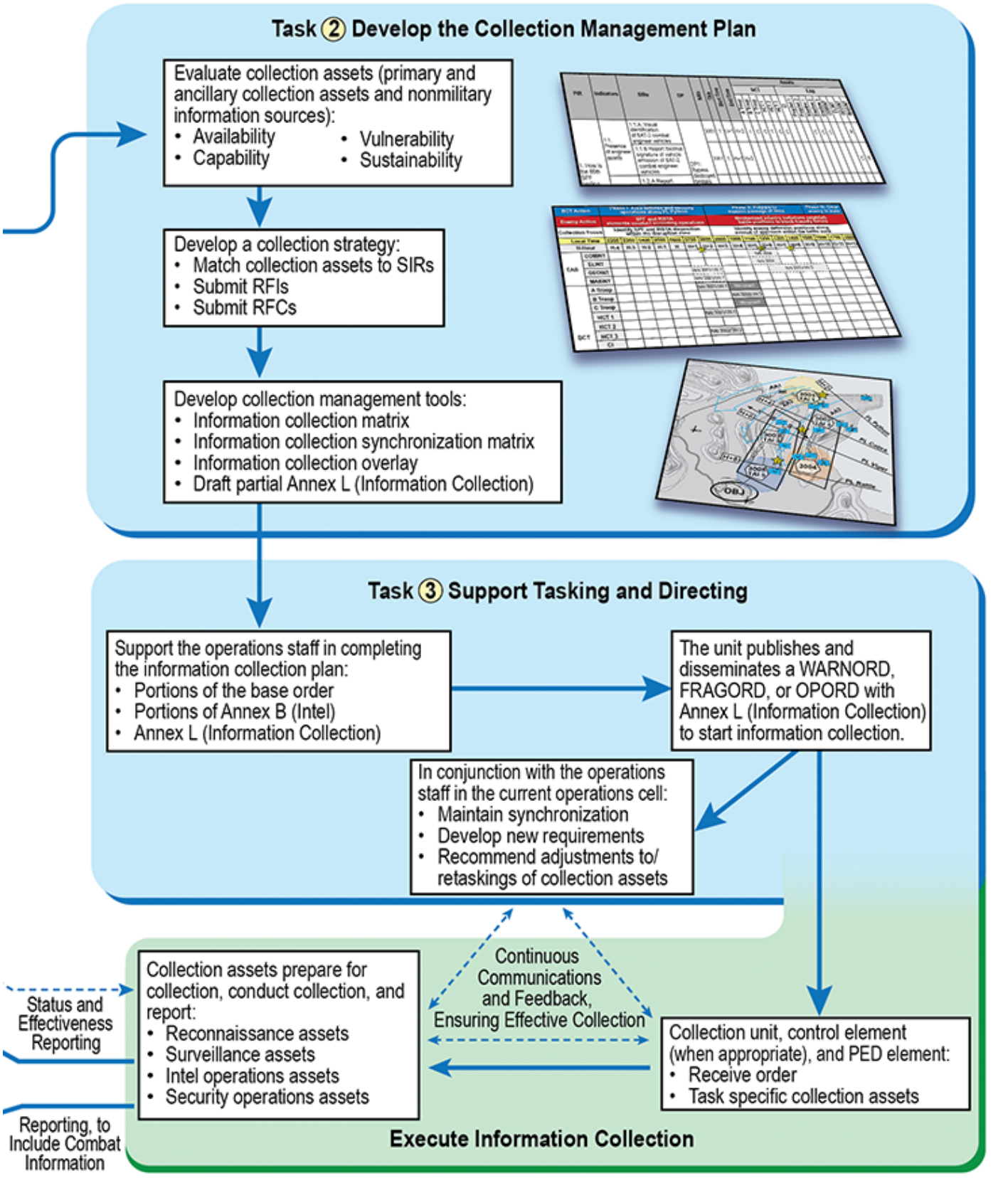
- https://armypubs.army.mil, then – Publications – Doctrine and Training. Select the type of publication ADP, ATP, or FM.
- https://ikn.army.smil.mil, then – Resources – MI Active Doctrine. Window opens in the IKN-S Doctrine Website. Select MI Active Doctrine from the left menu.
- https://www.ikn.army.mil, then select the MI Doctrine icon.

For questions concerning Army intelligence doctrine, please contact the USAICoE Doctrine Division via email at: usarmy.huachuca.icoe.mbx.doctrine@mail.mil

ATP 2-01, *Collection Management* Logic Chart



COA	course of action	EEI	essential element of information	intel	intelligence
COP	common operational picture	FRAGORD	fragmentary order	IPB	intelligence preparation of the battlefield



MOE	measure of effectiveness	PED	processing, exploitation, and dissemination	RFI	request for information
MOP	measure of performance	PIR	priority intelligence requirement	SIR	specific information requirement
OPORD	operation order	RFC	request for collection	WARNORD	warning order

U.S. Army photo by SSG Kenneth Burkhart

Building Indirect Lethality in Army Reserve Military Intelligence Tactical Teams

A U.S. Army Reserve Soldier with the 259th Military Intelligence Brigade walks to the brigade tactical operations center during exercise Always Engaged 18 at Joint Base Lewis-McChord (JBLM), WA, July 12, 2018. Exercise Always Engaged is a multicomponent military intelligence exercise conducted at JBLM.

by Colonel Rose Keravuori, Colonel Jackie East, Captain Matthew Thomas, and First Lieutenant Fernando Bendana

Introduction

U.S. Army Reserve military intelligence (MI) tactical teams enable indirect lethality through their support to lethal and nonlethal fires at echelons ranging from division to battalion task forces. In an expeditionary-military intelligence battalion (E–MIBn), MI tactical teams include human intelligence collection teams; counterintelligence teams; operational management teams; signals intelligence teams; cryptologic support teams; multifunctional teams; and processing, exploitation, and dissemination (PED) teams consisting of several intelligence disciplines. These teams focus on supporting lethality to enable maneuver commanders to dominate in their tactical tasks. The specific challenges that reserve MI tactical teams face are—

- Supporting the achievement of lethality in the available 38 training days (2 days of battle assemblies per month and 14 days of annual training allocated in one fiscal year).
- Obtaining results with geographically distributed and non-proximate resources.
- Increasing indirect lethality in the absence of organic subject matter expertise.

Solutions to some of these problems include focusing on team-level training, purposefully creating the right operational environment, making deliberate use of U.S. Army mission training complexes (MTCs), and using cadre from the Army Reserve Intelligence Support Centers (ARISC).

Focus on Team-Based Training

Team-based training, assessment, evaluation, and eventual certification are the goals for reserve component MI tactical teams. It is best to focus training at the team level, rather than at the company or battalion levels, because of the normal turnover of personnel, civilian job constraints, commitments to professional military education, and other factors Soldiers face in today's Army Reserve.

Measures of Collective Task Proficiency[1]

T : fully trained (complete task proficiency)
T- : trained (advanced task proficiency)
P : practiced (basic task proficiency)
P- : marginally practiced (limited task proficiency)
U : untrained (cannot perform the task)

Increasing indirect lethality to at least the practiced level (P level) of collective task proficiency,[2] based on ADP 7-0, *Training,* and the *Leader's Guide to Objective Assessment of Training Proficiency,*[3] requires a straightforward training management operation that is based on the intelligence team concept of the Military Intelligence Training Strategy. A unit's training management should include the following focus areas:

- Training, assessments, and evaluations conducted at night during battle assemblies, given the proper operational environment.
- Integrated training, assessments, and evaluations across intelligence disciplines for teams using a mix of live, virtual, or constructive domains.
- Team-level training and prevention of over-investment in individual military occupational specialty (MOS)-related training, especially training that simply re-creates institutional training.
- Use of available collective training resources during long battle assemblies and annual training.
- Aggregation of trained and ready teams at the section, platoon, and company level.
- Guidance from ADP 7-0 and the *Leader's Guide to Objective Assessment of Training Proficiency* to generate external evaluations by adjacent and echelons two levels higher.[4]

No field manual precisely defines the concept of intelligence teams; therefore, teams should be multifunctional and sized appropriately to execute a certain intelligence role and function. The mission essential tasks' and the supporting collective tasks' training and evaluation outlines (T&EOs) indicate the echelon required for the evaluation of performance steps and measures. Consideration must be given to discrete teams. For example, imagery teams consisting of one geospatial intelligence imagery analyst (MOS 35G) and one all-source intelligence analyst (MOS 35F) can be capable of PED for one full motion video line for one shift. Reviews of the T&EOs relevant to such a team revealed that an MOS 35F-qualified all-source intelligence analyst is not necessary for this team to achieve an outcome rating of "fully trained," indicated as T, or even a rating of "practiced," indicated as P. The role of the all-source intelligence analyst on this team is to generate a spot report; a size, activity, location, unit, time, and equipment (SALUTE) report; and other reports in coordination with the geospatial intelligence imagery analyst to enable rapid targeting and effects assessment. The person performing this function must maintain logs, write a post mission report, and be able to match identified items with high-payoff target lists. This person must also receive queuing information from other intelligence functions, be able to understand priority intelligence requirements (PIRs) well enough to identify information that may assist in answering commander's critical information requirements, and then bring that information to the attention of the officer in charge or the noncommissioned officer in charge. Although being a graduate of the initial entry MOS 35F granting course may make achieving a "GO" in these performance measures easier, most of these are common Soldier tasks that anyone can be trained to accomplish. A review of relevant T&EOs can identify performance steps and measures that non-MOS-qualified Soldiers are qualified to accomplish in their position.

Further, these discrete teams do not necessarily have to perform steps and measures with other intelligence functions assessed within the collective task or mission essential task. However, integrating their training does enhance the value and make assessment and evaluation simpler. AR 220-1, *Army Unit Status Reporting and Force Registration – Consolidated Policies,* and the *Leader's Guide to Objective Assessment of Training Proficiency* contain information that allows the aggregation of multiple teams of the same type into one higher echelon T-rating. Assessors and evaluators can also aggregate multiple types of team ratings to generate ratings for a mission essential task that have performance steps and measures for multiple types of teams.

The Right Operational Environment

Creating the proper operational environment helps achieve indirect lethality, given the limited training days available to reserve Soldiers. Innovating battle assemblies for better training, including night training, allows the highest possible assessment and evaluation outcomes at a low cost. The following analysis compares night operations battle assembly with day battle assembly (Figure 1, on the next page). This sample training schedule has sufficient night operations at low residual risk and enables the use of contract lodging in kind as well as sustenance in kind. Figure 2, also on the next page, shows a comparison of a night operations battle assembly versus a day battle assembly.

Night Operation Battle Assembly/Drills

SATURDAY						SUNDAY	
0930-1100 (1.5 hrs) APFT-Select-Pax	0930-1130 (2 hrs) Leader Workgroup	1130-1200 (.5 hrs) Soldiers Report Formation	1200-1800 (6 hrs) Operations	1800-1900 (1 hr) Dinner-SIK	1900-2359 (5 hrs) Operations	0000-0100 (1 hr) Operations	0100-0200 (1 hr) Leader Workgroup

SUNDAY								
0100-1000 (9 hrs) (7 hrs leaders) Warrior Rest Management	0900-1000 (1 hr) Leader Check-out LIK	1000-1100 (1 hr) Leader Workgroup	1000-1100 (1 hr) Soldiers Check-out LIK	1100-1130 (.5 hrs) Soldiers Report Formation	1200-1300 (1 hr) Lunch-SIK	1300-1600 (3 hrs) Operations	1600-1630 (.5 hrs) Soldier Release Formation	1630-1800 (1.5 hrs) DTMS

Day Operation Drills

SATURDAY							
0630-0800 (1.5 hrs) APFT-Select-Pax	0700-0800 (1 hr) Leader Workgroup	0800-0830 (.5 hrs) Soldiers Report Formation	0830-1130 (3 hrs) Operations	1130-1230 (1 hr) Lunch-SIK	1230-1700 (4.5 hrs) Operations	1730-1930 (2.5 hrs) Leader Workgroup	1700-2359 (7 hrs) (4.5 hrs leaders) Warrior Rest Management

SUNDAY								
0000-0700 (7 hrs) (6 hrs leaders) Warrior Rest Management	0600-0700 (1 hr) Leader Check-out LIK	0700-0800 (1 hr) Leader Workgroup	0800-0830 (.5 hrs) Soldiers Report Formation	0830-1130 (3 hrs) Operations	1130-1230 (1 hr) Lunch-SIK	1230-1600 (4.5 hrs) Operations	1600-1630 (.5 hrs) Soldier Release Formation	1630-1800 (1.5 hrs) DTMS

Figure by COL Keravuori

Figure 1. Sample Drill Weekend Training Schedules

Both approaches have 15 operational hours. Day operations allow a small addition to available leader training management hours and moderately more transition time for leaders and Soldiers. The day schedule generates much more transition time overnight between Saturday and Sunday operations.

An approach to providing balance among P-level and higher assessments and evaluations involves using a model of a one-night battle assembly at home station, one field training exercise battle assembly away from home station at a location with available supporting infrastructure, and one typical daytime battle assembly at home station. This revised time structure maximizes available time for operations, transition, and training management and best manages residual risk from reduced transition time during night battle assembly operations.

In addition to innovating battle assemblies, using an appropriate set of operational and mission variables will allow teams to meet the highest possible operational environment level that the T&EOs require for the mission essential task or supporting collective task. Operational variables such as time, infrastructure, information, and physical environments can be created, leveraged, and manipulated to achieve outcomes. Constructive, live, and virtual mission variables challenge and stress intelligence teams when conducting training, assessments, and evaluations.

NIGHT		DAY	
Night Leader Training Management	Night Soldier Training Management	Day Leader Training Management	Day Soldier Training Management
5.5 Hours	1.5 Hours	6 Hours	1.5 Hours
Leader Operations	Soldier Operations	Leader Operations	Soldier Operations
15 Hours	15 Hours	15 Hours	15 Hours
Leader Transition	Soldier Transition	Leader Transition	Soldier Transition
11.5 Hours	13.5 Hours	15 Hours	15 Hours
Leader Total Hours	Soldier Total Hours	Leader Total Hours	Soldier Total Hours
32 Hours + 1.5 for APFT Days at BA/Drill	30 Hours + 1.5 for APFT Days at BA/Drill	36 Hours + 1.5 for APFT Days at BA/Drill	31.5 Hours + 1.5 for APFT Days at BA/Drill

Figure by COL Keravuori

Figure 2. Night Battle Assembly versus Day Battle Assembly Comparison

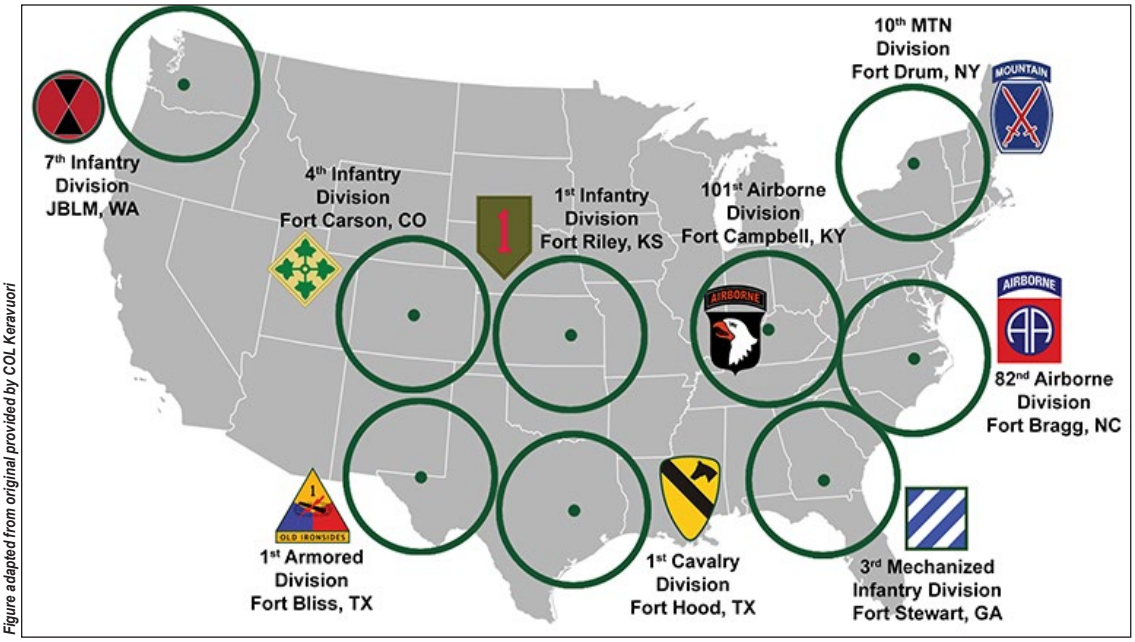


Figure adapted from original provided by COL Keravuori

Figure 3. Army Mission Training Complexes

Army Mission Training Complexes

With most Army Reserve centers geographically distributed and often in remote locations, leaders must make use of Army MTCs. MTCs are located at all military installations with a division or corps headquarters and are available for reserve unit use. The Army Reserve has five mission training complexes that also have an Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) capability. Figure 3 shows the Army MTC and IEWTPT locations in the center of the green circles. The circles represent approximately 8 to 10 hours of tactical vehicle driving from the center point to the circumference edge of the circle.

The MTCs possess many critical capabilities for tactical MI units to increase their support to lethality. These centers can establish command post-like organization and hardware that units can use. They can also simulate the mission command systems via the Warfighters Simulation (WARSIM) system. This is the same simulation system division and corps headquarters use to create virtual combat and sustainment operations for warfighter exercises. MTCs can replicate full motion video and produce automatically generated signals intelligence reporting for PED. These facilities can set up and network mission command systems such as Command Post of the Future (CPOF), Distributed Common Ground System-Army (DCGS–A), and Tactical Ground Intelligence Stations to enable integrated training outcomes. Finally, MTCs will allow MI systems maintainers/integrators (MOS 35T) to do their performance steps and measures.

As an example, at the MTC at Fort Stewart, Georgia, the 321st E–MIBn had access to a virtual battlefield and live equipment in a facility designed to resemble a division analysis and control element (ACE). The battalion's imagery intelligence analysts and signals intelligence analysts received full motion video, moving target indicator, and signals intelligence tactical reports to process, exploit, and disseminate in real time, while the battalion's intelligence operations and assessment team synchronized collection against division PIRs as provided by the exercise director. The E–MIBn was able to constructively feed reports and combat information to stimulate human intelligence and counterintelligence operational management teams. The MTC network had a voice and text chat capability that allowed the E–MIBn to provide targeting, battle damage assessment, queuing, fusion, and real-time modification of collection planning.

The costs for leveraging MTCs to increase support to lethality are minimal. Units must plan and prepare with the MTC to achieve better outcomes. This includes providing concept of exercise, staffing, digital account rosters, mission command system requirements, blue and white cell WARSIM operators, Multiple Unified Simulation Environment operators, and refresh training on DCGS–A and CPOF. This also allows time for the exercise white cell to prepare necessary division and ACE products to enable the MI unit being trained to execute its mission essential tasks.

In the Fort Stewart MTC example, the 321st E–MIBn invested 16 hours of coordination and planning time with the MTC and used 4 hours of digital training refresh. The 321st E–MIBn also provided a seven-person guard detail for 24-hour guard coverage over 10 days, 10 Soldiers for 4 days to train on WARSIM and the other enabling systems for fires and information collection at the MTC, and one Soldier for 4 days to prepare division and ACE CPOF products to enable the exercise. The military installation offered barracks and access to a dining facility during the event. The unit required 8 hours to conduct a tactical convoy operation over 230 miles to the MTC event and then another 8 hours back to home station. This investment enabled a 3-day training event that provided more than 24 hours of assessment and evaluation. The event replicated a U.S. division attacking

three enemy divisions in the defense, and it replicated full motion video, moving target indicator, and signals intelligence for PED. The event also allowed intelligence operations and assessment to execute their tasks, and stimulated operational management teams using a large-scale ground combat operation. The E–MIBn was able to generate P-ratings for each relevant mission essential task and supporting collective task evaluated.[5]

Army Reserve Intelligence Support Centers

The ARISCs give reserve units access to classified training spaces, intelligence architecture, and certified intelligence discipline observer coach/trainers (OC/Ts). The ARISCs have collectively more than 200,000 square feet of training and classified workspace provisioned with the Joint Worldwide Intelligence Communications System, SECRET Internet Protocol Router Network, Non-classified Internet Protocol Router Network, National Security Agency Network, and field support engineers provided by the Defense Intelligence Agency and the Military Intelligence Readiness Command. Five ARISCs are located across the United States (shown in Figure 4) with additional detachment locations, including Phoenix, Arizona; Orlando, Florida; Fort Devens, Massachusetts; and Dekalb, Maryland. Each ARISC has the mission to enable and facilitate MI reserve readiness. The ARISCs offer credentialed trainers, nationally aligned curricula, and access to Army program of record systems to enhance measured MI reserve team readiness in order to provide deployable, trained, equipped, and connected teams capable of meeting the mission requirements of combatant commanders and the national to tactical intelligence community.

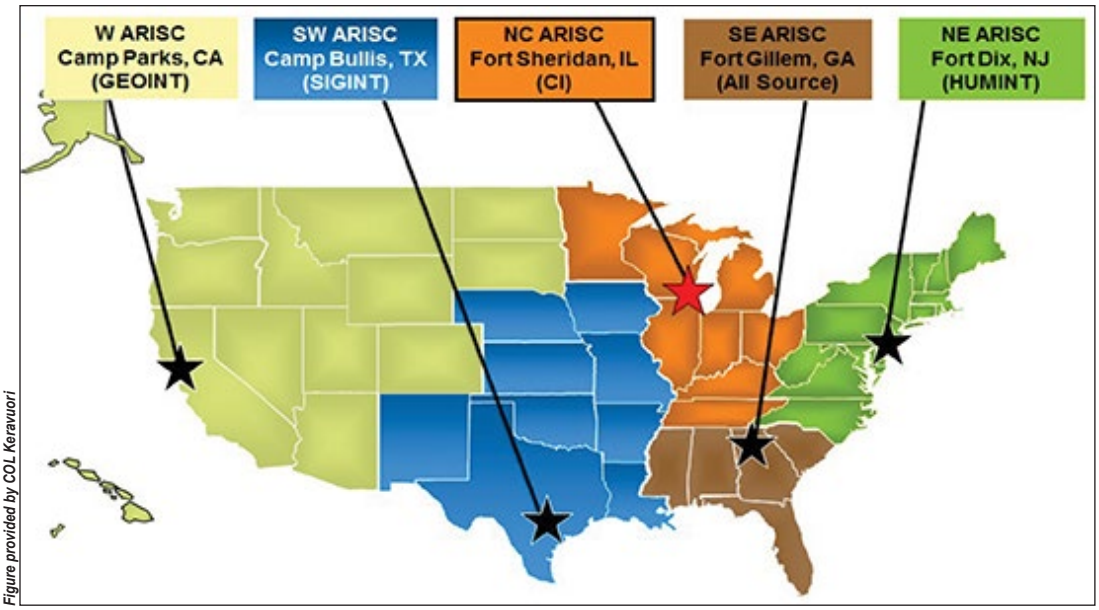


Figure provided by COL Keravuori

Figure 4. Army Reserve Intelligence Support Centers

The five main ARISCs are also Army Foundry sites. They can provide a certified intelligence discipline cadre across all intelligence disciplines. Each of the OC/Ts assigned to the ARISC has completed a certification program for their particular intelligence discipline. This seasoned cadre is available to train MI teams throughout the U.S. Army Reserve and is capable of supporting an external evaluation during scheduled unit training time, including battle assemblies and annual training exercises. First Army active duty Soldiers are also assigned to each ARISC and function as part of the cadre. MI company commanders consult the ARISC cadre to develop their company unit training plans and refine them regularly. As part of the planning process, MI company commanders take into consideration their mission essential task list, the mission they are training toward, a current assessment of their intelligence teams, the available time to train, and a desired end state. The ARISC cadre then helps the company command teams to develop tiered training strategies for all intelligence disciplines in alignment with the Military Intelligence Training Strategy and assists with the development of a realistic, executable training plan. ARISC personnel can also provide primary or assistant instructor support either at the ARISC site or with a mobile training team.

Conclusion

For reserve MI tactical formations, the focus continues to be on ready and deployable teams. As a reserve E–MIBn, the 321st has focused on conducting team-based training; innovating battle assemblies; and optimizing the use of MTCs, IEWTPTs, and ARISCs to increase team readiness, employability, and deployability. The future of MI teams will shift to better support the deep-sensing capability that division and corps commanders need in large-scale ground combat operations. Reserve MI tactical teams must innovate to continue to improve their teams' indirect lethality.

Endnotes

1. Department of the Army, Army Doctrine Publication (ADP) 7-0, *Training* (Washington, DC: U.S. Government Publishing Office, 31 July 2019), 4-2.

2. See ADP 7-0, *Training; Leader's Guide to Objective Assessment of*

Training Proficiency; and relevant training and evaluation outline report collective task forms.

3. The *Leader's Guide to Objective Assessment of Training Proficiency* is one of several tools for unit leaders to navigate through the instructions and procedures to plan, prepare, execute, and assess training. It is accessible to unit commanders and Soldiers through the Army Training Network at https://atn.army.mil/dsp_template.aspx?dpID-376 (common access card login required).

4. External evaluations can be achieved in one of three ways in accordance with ADP 7-0 and the *Leader's Guide to Objective Assessment of Training Proficiency*. First, two levels higher can evaluate mission essential tasks. For teams and platoons, this means the battalion commander and staff can evaluate; for companies, the brigade commander and staff can execute the evaluation. Second, these same documents also allow adjacent units to conduct external evaluations; for example, a sister platoon can observe, coach, and train a platoon and provide an external evaluation. Third, there are organizations and units outside the military intelligence (MI) tactical team's chain of command that could provide an external evaluation. These include other reserve component or active component MI units, the cadre of the Army Reserve Intelligence Support Centers, First Army observer coach/trainers, and the 84th training command observer coach/trainers. With only 38 days of available potential training and assessment time, leaders must leverage all available collective training resources and innovate to generate T ratings.

5. Of critical importance in building indirect lethality is the documentation of assessments and evaluations in the Digital Training Management System and the retention of sufficient documentation to give First Army and your higher headquarters confidence to execute post-mobilization validation/certification.

COL Rose Keravuori is a U.S. Army Reserve officer currently serving in the Office of the Chief of Army Reserve G-3/5/7. She previously commanded the 259th Expeditionary-Military Intelligence Brigade. She has deployed in an intelligence capacity to Kosovo, Iraq, and Afghanistan. COL Keravuori holds degrees from the U.S. Military Academy at West Point, University of Oxford, and Army War College.

COL Jackie East is a U.S. Army Reserve officer who serves as the Assistant Chief of Staff G-2, 84th Training Command, Fort Knox, KY. He previously commanded the 321st Expeditionary-Military Intelligence Battalion. He holds a master of arts in diplomacy and international commerce and a doctorate in public policy and research methods from the University of Kentucky, a master of arts in operational art and science from the School of Advanced Military Studies, and a master of arts in strategic studies from the U.S. Army War College.

CPT Matthew Thomas is a U.S. Army Reserve officer currently serving with the 321st Expeditionary-Military Intelligence Battalion in Orlando, FL. He is a counterintelligence and all-source intelligence officer with multiple deployments to the Middle East. In his civilian capacity, he works as an analyst for Army Futures Command. CPT Thomas holds a bachelor of science in international relations from the University of Central Florida.

1LT Fernando Bendana is a U.S. Army Reserve Officer who serves as platoon leader in Headquarters and Headquarters Detachment, 321st Expeditionary-Military Intelligence Battalion. He holds a bachelor of science in computer engineering.

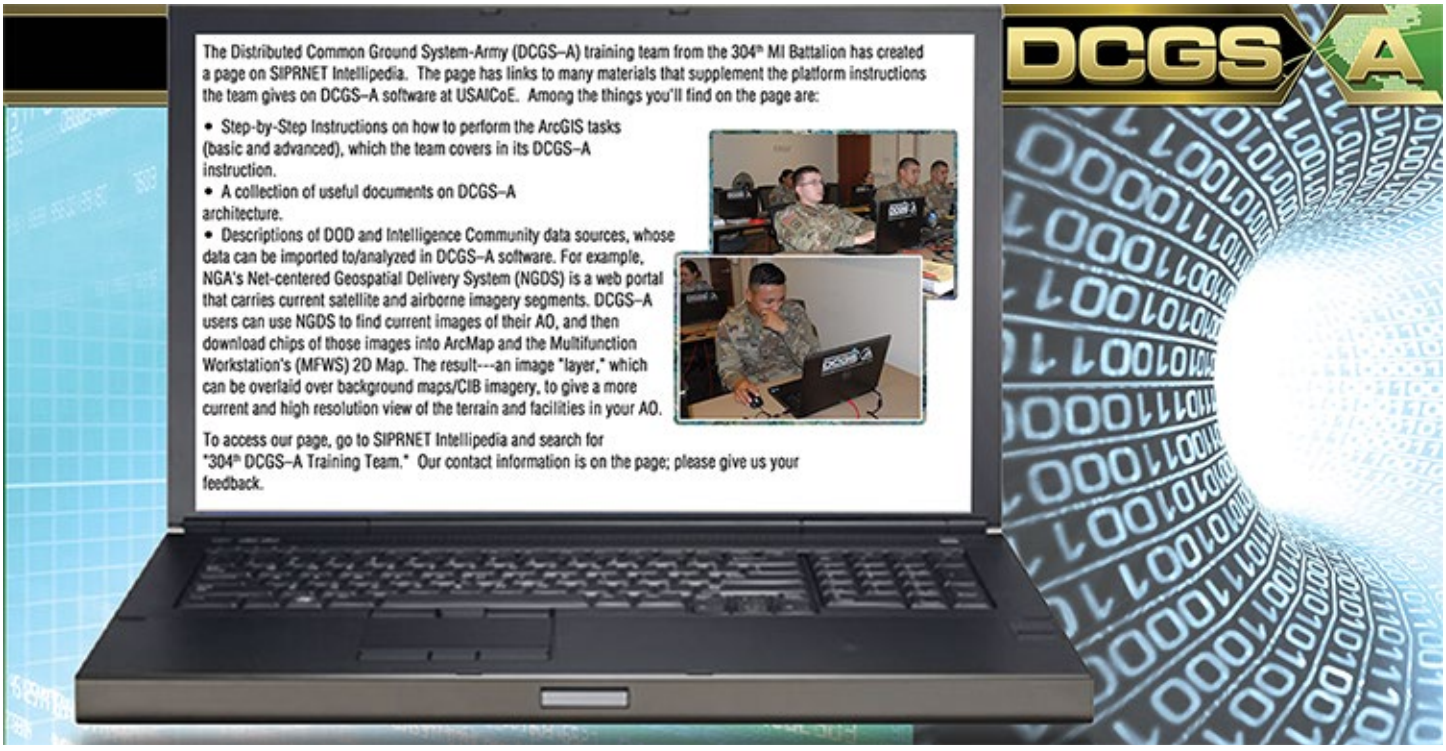


Photo by Joseph Siemandel, Joint Force HQ-Washington National Guard

Soldiers from Delta Company, 341st Military Intelligence Battalion, conduct low-level voice interception during the field training exercise Panther Strike Lite on February 8, 2020, at Joint Base Lewis-McChord, WA. Panther Strike Lite was a battalion-level exercise featuring human intelligence, signals intelligence, and counterintelligence in preparation for Panther Strike, a 300th Military Intelligence Brigade exercise at Camp Williams, UT.

Army National Guard Military Intelligence Training Exercises

by Major Christopher Mision

Introduction

Over the last decade, the Army National Guard (ARNG) military intelligence (MI) enterprise has developed a number of annual collective training exercises to support the evolving needs of the ARNG's intelligence warfighting function throughout the 5-year sustainable readiness cycle. These events have focused on three areas: the brigade combat team (BCT), the expeditionary-military intelligence brigade (E–MIB), and the 300th Military Intelligence Brigade (MIB) (linguist). This article describes exercises Cyclone Fury, Talon Strike, and Panther Strike, which support the three focus areas.

Cyclone Fury

Cyclone Fury is a tailorable collective training exercise designed to assist ARNG BCT commanders with the certification of the BCT's intelligence warfighting function in Prepare [year] 3. The exercise leverages live and constructive inputs, by way of role players and the Intelligence and Electronic Warfare Tactical Proficiency Trainer, to simulate and stimulate BCT intelligence systems and to facilitate the Military Intelligence Training Strategy (MITS) Tier 3 and Tier 2 certifications for crews and platforms, respectively. The Indiana Intelligence Center Foundry Platform staff designs, hosts, and facilitates the exercises, which

take place at the Muscatatuck Urban Training Center, located near Butlerville, Indiana. The training gives the training audiences the ability to leverage varying environments and domains to meet the units' training objectives. The initial iteration of Cyclone Fury was structured to prepare the 33rd Infantry Brigade Combat Team S-2 and Delta Company, 766th Brigade Engineer Battalion (MI company), to certify their intelligence warfighting function before participating in a Joint Readiness Training Center rotation. Another tailored Cyclone Fury exercise was conducted in November 2019 to allow the 75th Ranger MI Battalion to certify their intelligence warfighting function on Tier 3 tasks and the integration of electronic warfare (EW) and cyber capabilities.

The Army National Guard's 5-Year Sustainable Readiness Cycle[1]

- Prepare 1 ("year one"): Units focus on individual training such as duty military occupational specialty qualified training, weapons qualification, driver training, professional military education, Pre-Command Course, and attendance at other types of Army schools and institutions.
- Prepare 2 ("year two"): Units build upon training received in Prepare 1 by focusing on individual skill proficiency and certifications.
- Prepare 3 ("year three"): Units focus on sustaining individual skill proficiency and certifications.
- Prepare 4 ("year four"): Non-deploying select sustainment, maneuver support, and medical units will conduct a culminating exercise such as at a combat training center, a contractor technical evaluation, or a Joint Readiness Training Center training event. Apportioned units in Prepare 4 continue to train for unified land operations and would be the most likely units to be mobilized in a "surge" environment. Deploying units will prepare for a mission readiness exercise.
- Mission/Ready ("year five"): Units will maintain collective training proficiency at the level organized (e.g., detachment/company, battalion, and brigade or higher staffs).

Moving forward, the Indiana Intelligence Center will continue to hone Cyclone Fury's alignment with MITS certification and the soon-to-be-published Cyber and Electronic Warfare Training Strategy to support the future integration of cyber and EW in the BCT's MI company. Cyclone Fury's collective training team has worked in conjunction with the program management office for EW and cyber and the signals intelligence (SIGINT)/cyber/EW tabletop exercise to better align scenario development with upcoming BCT intelligence warfighting function force structure changes. Muscatatuck Urban Training Center, in its current form, stands ready to provide units with a complex and ready-to-use training range for SIGINT, EW, and cyber integration in a multi-domain operations space that is scalable to support MITS Tiers 3 through 1 certification when integrated with Camp Atterbury, Indiana. Ongoing work between the ARNG G-2 and ARNG G-3 to incorporate MITS Tier 3 and Tier 2 certifications into Exportable Combat Training Center exercises will ensure, along with Cyclone Fury, the ARNG BCTs are trained, certified, and ready before participating in a combat training center rotation or entering a ready year.

Talon Strike

Talon Strike is the 71st E–MIB's annual collective training exercise based in central Texas, supporting both the 636th and 250th MI Battalions and other National Guard MI units. Talon Strike targets an integrated collection-focused training scenario that feeds into analysis and exploitation elements, leading to subsequent refined or adjusted collection criteria that aim to exercise all steps of the intelligence process across all intelligence disciplines.

In 2019, Talon Strike executed single-source collection lanes at Camp Bullis near San Antonio, Texas. The exercise generated reports analyses and developed situational awareness for both the 71st E–MIB and the 58th E–MIB staffs to conduct military decision-making process training, enabling and improving readiness for the 58th E–MIB's Central Command mobilization. Additionally, geospatial intelligence (GEOINT) training executed from Camp Bullis focused on full motion video processing, exploitation, and dissemination.

U.S. Army National Guard photo by CPT Maria Mengrone

Guardsmen from the Texas Army National Guard (ARNG) and California ARNG brief the Commander, 58th Expeditionary-Military Intelligence Brigade, Maryland ARNG, during a combined arms rehearsal, May 19, 2019, in San Antonio in preparation for Talon Strike 2019, a 2-week training event at Camp Bullis, TX.

Based on lessons learned and best practices rehearsed from 2019, Talon Strike 2020 targeted the 36th Infantry Division G-2's analysis and control element as the primary training audience to prepare for the Operation Spartan

Shield mobilization. Initially planned for more than 400 personnel across four different states and locations, travel restrictions and training limitations decreased Talon Strike's audience to 52 personnel, largely populated from the 36th Infantry Division G-2. Exercise Comanche, a real-world scenario specifically tailored to the Central Command area of responsibility, brought an improved level of quality to training and directly led to increased readiness levels for analysts set for deployment to the Middle East.

In future years, the 71st E–MIB, 36th Infantry Division, and the Military Intelligence Training Center-Texas will partner to streamline MITS Tier 4 (individual certification) training and establish multiple iterations of MITS Tier 3 (crew certification) training exercises cut from the cloth of Talon Strike successes in previous years. Incorporating intelligence units, with priority based on the Sustainable Readiness Model cycle, and aligning them with specific scenarios for multidiscipline, high quality training will improve readiness, lethality, professional military education success, and ultimately retention, which are part of the Texas Adjutant General's and ARNG's training guidance goals.

Panther Strike

The 300th MIB (linguist), a unit within the Utah Army National Guard, hosted a virtual annual training event from 7 to 22 June 2020. Attendees included 182 intelligence, linguistic, and industry professionals. Constraints from the coronavirus disease 2019 (COVID-19) pandemic resulted in modifying the Panther Strike 2020 collective training exercise. Human intelligence (HUMINT), counterintelligence (CI), SIGINT, and all-source discipline Soldiers conducted training using resources from the Center for National Security Studies, the Center for Anticipatory Intelligence, the National Guard Bureau G-2 MI Gym, and the Panther Strike Planning Team. Despite the difficulties and restrictions in place because of COVID-19, the brigade was able to accomplish both collective and individual training.

The Center for National Security Studies instructed 110 Soldiers from HUMINT, CI, and all-source intelligence disciplines. The training incorporated formal briefings and lectures followed by the attendees conducting regular collective practical exercises. The trainers instructed on the following topics:

- Introduction to national security system and process.
- Intelligence analysis.
- Middle East history, politics, and culture.
- Radical fundamentalism and terrorist financing.
- Law of war.

Panther Strike[2]

"Panther Strike is important because it is one of the few exercises in the country where we have a very robust footprint of military intelligence Soldiers and support structure together at one place."

—LTC Kiley Laughlin, former commander of the 223rd MI Battalion, California Army National Guard

"We haven't captured a peer nation platoon on the battlefield in a conventional situation in a really long time. There have been new laws and regulations added to interrogations and screenings. We need to adapt to the modern world so we are teaching them the way to perform it effectively, correctly, and legally for tomorrow's war."

—SSG Dan Mealy, instructor with the HUMINT training team during Panther Strike 2019

U.S. Army photo by SGT Nathan Baker

Military intelligence Soldiers participate in radio operation training during Panther Strike, June 6, 2019, Camp Williams, UT.

The National Guard Bureau G-2's MI Gym enabled the brigade's Soldiers to be the first users to go through the new EW trainer. MI Gym is a new National Guard Bureau G-2 program that is an unclassified online-based training platform requiring no software installation or hardware. Trainees use standard computers or laptops to access web-based training from commercial or Department of Defense networks. MI Gym's Module 2 EW trainer provided the 300th MIB Soldiers multiple iterations to train radiofrequency theory, exploitation of target voice communications, map reconnaissance, site selection, and identification of signals of interest. The training was performed from the Soldiers' respective locations. Forty-nine SIGINT discipline Soldiers trained on the EW trainer for a total of

392 hours throughout the event. The SIGINT training audience was able to train four of seven collective and individual tasks for their assigned mission essential task lists.

Conclusion

The ARNG MI enterprise will continue to participate in exercises that develop the skill level of reserve MI Soldiers and units, and train and evaluate each of the MI specialties, including HUMINT, SIGINT, GEOINT, and CI at the team, brigade, and division levels. These opportunities provide an important focus on the basic tasks and integration of the different specialties, with Soldiers practicing and reinforcing their individual and collective training tasks, while learning how to confront peer and near-peer adversaries.

Endnotes

1. Department of the Army, *Sustainment Training Strategy & Guide* (Washington, DC: U.S. Government Publishing Office, November 2016), 68–69.

2. John Etheridge, "Panther Strike 2019," Utah National Guard website, June 18, 2019, https://ut.ng.mil/Site-Management/News-Article-View/Article/1879562/panther-strike-2019/.

MAJ Christopher Mision is a Texas Army National Guard (ARNG) Soldier on T-10 Active Guard Reserve, currently serving as the ARNG G-2 Training and Exercises Team Chief. He is responsible for support to ARNG military intelligence (MI) individual training, collective training, and lessons learned, and has coordinated to develop the ARNG G-2's Collective Training and Mentor Team. MAJ Mision has over 19 years of experience in combat arms and MI and as a military contractor. He holds a bachelor of science in chemistry and a master of arts in intelligence studies.

Military Intelligence Readiness Command Processing, Exploitation, and Dissemination: Success in Establishing Global Reach Intelligence Support

by Chief Warrant Officer 3 Scotty Stock

Introduction

In 2019, LTG Scott Berrier, then-Army Deputy Chief of Staff, G-2, wrote in the foreword to the *United States Army Intelligence Processing, Exploitation, and Dissemination (PED) Concept of Operations,* "The Army Processing, Exploitation, and Dissemination (PED) Enterprise must modernize to enable the Joint Force to compete short of armed conflict, penetrate and disintegrate adversary stand-off capabilities, exploit windows of opportunity, and return to competition."[1] To meet this objective, the Military Intelligence Readiness Command (MIRC) established four operational Army PED reach sites at selected Army Reserve Intelligence Support Centers (ARISCs). These locations allow MIRC personnel to integrate into the Army's PED enterprise to provide stakeholders with the necessary capabilities to support forces globally. From these PED reach sites, MIRC analysts provide critical information to support the requirements of the combatant commands. The MIRC adopted the Army's geospatial intelligence program of record software and training strategies to meet the Army's PED requirements. The intelligence architecture and software solution allow the MIRC PED reach sites to integrate into the multi-domain intelligence infrastructure.

Background

The MIRC is the U.S. Army Reserve's premier functional command for intelligence. It comprises over 70 percent of the Army Reserve's military intelligence force and manages intelligence training and operations throughout the continental United States. The four PED reach sites provide operational and training support to meet the Army's PED mission requirements. The MIRC is currently operating its fourth mission from a MIRC PED reach site in support of U.S. Army Forces Command (FORSCOM). The MIRC has leveraged the lessons learned from these efforts to develop training pipelines to meet future and emerging PED requirements. To establish the Army Reserve PED reach sites, the MIRC employed the U.S. Army Intelligence and Security Command's (INSCOM) Converged Infrastructure Network and software-defined workstation for the Distributed-PED. The MIRC's Fixed-PED workstation uses the Geospatial eXploitation Products (GXP) Platform™ and SOCET GXP®.

Strategic Value

As a key Army PED stakeholder, the MIRC supports operations through mobilization and as contingency sites. The key to establishing a full operational capability PED reach site was ensuring network redundancy. This redundancy provides the site with a primary and alternate capability to remain operational and is critical to establishing an effective primary, alternate, contingency, and emergency (PACE) plan. This ability enables the Army PED enterprise to incorporate the MIRC PED sites into the holistic enterprise PACE plan. The MIRC PED reach sites provide the Army PED enterprise

with more than 130 analyst positions to support PED operations. These sites have also been used as continuity of operations plan sites in support of global reach operations.

Connectivity

To install the necessary connections to sustain PED operations, the MIRC partnered with the Defense Information Systems Agency (DISA), the Unified Video Dissemination Services (UVDS) team, INSCOM, and FORSCOM. Each of these partners provides a critical piece for the PED connectivity. DISA provides the circuit connectivity, and its UVDS team provides connection to full motion video services over a redundant Layer 3 Virtual Private Network. The UVDS connection provides the video for the MIRC's Fixed-PED workstations. DISA also provides the connectivity for the Distributed-PED, and INSCOM provides the services necessary to conduct PED on the software-defined workstation. These diverse PED connections meet FORSCOM's requirements to be a full operational capability PED reach site. The diversity is key to maintaining a PACE plan at the reach sites that can be executed to minimize any loss in support. In November 2019, at the MIRC's second evaluation of the full operational capability PED reach site, the FORSCOM PED chief identified the MIRC's PED reach ability to switch between mission networks within seconds as the "gold standard." To match the facility capability, the MIRC demonstrated its ability to train and mobilize Soldiers in support of operations at the PED reach sites.

Unified Video Dissemination Services

The DISA UVDS architecture is a next-generation full motion video PED system that provides persistent, focused, real-time, operational information flow to tactical and enterprise end users worldwide. Its six globally dispersed hubs provide dynamic, proximity-based access to real-time full motion video through the unified video portals. Its data-agnostic network connects multiple Department of Defense gateways, combatant commands, military Services, operation centers, and intelligence agencies.[2]

Software

To support the missions, the MIRC employs a variety of software across both the Fixed-PED and the Distributed-PED. The Fixed-PED workstations use the GXP Xplorer® and GXP InMotion™ Video Server plugins on the GXP Platform™ for data management and video streaming. The MIRC was the first Army organization to use this solution for its PED reach sites to meet FORSCOM's full operational capability requirement. To exploit the full motion video and data on the Fixed-PED workstations, the MIRC uses SOCET GXP® and GXP InMotion™ Video Desktop. The exploitation systems are used in the Distributed Common Ground System-Army, the Army's program of record for the intelligence warfighter. The Distributed-PED, supported by the software-defined workstation, uses the Advanced Intelligence Multimedia Exploitation Suite (AIMES) to exploit and INSCOM services managed under the Converged Infrastructure Network. To publish the finished intelligence, the MIRC uses the Geospatial Intelligence Enterprise Tasking, Processing, Exploitation, and Dissemination Services (GETS). The mission manager choses the PED solution the team will use to conduct the mission.

Overview of the Software

GXP Platform™—creates software applications in the geospatial intelligence domain. The platform uses the GXP Xplorer® and GXP InMotion™ software products.[3]

GXP Xplorer®—is a data management application used to locate, retrieve, and share geospatial data.[4]

GXP InMotion™ Video Server—manages video exploitation tasks in an enterprise environment, allowing organizations to scale based on the number of video missions and analysts required.[5]

GXP InMotion™ Video Desktop—is a video analysis application.[6]

SOCET GXP®—is a geospatial-intelligence software product that uses imagery from satellite and aerial sources to identify, analyze, and extract ground features for product creation.[7] It combines image analysis, advanced photogrammetric techniques, remote sensing, and feature collection workflows into one package.[8]

Advanced Intelligence Multimedia Exploitation Suite (AIMES)—is a motion imagery exploitation system that enables intelligence analysts to fuse, exploit, and report on motion imagery data from a full range of sources. It helps break down single-source stovepipes to enable near-real-time and forensic fusion of full motion video and all-source intelligence information, as well as synchronized visualization of raw data, chat, and processed intelligence.[9]

Geospatial Intelligence Enterprise Tasking, Processing, Exploitation, and Dissemination Services (GETS)—improves situational awareness through a common, web-enabled geospatial intelligence and measurement and signature intelligence reporting and dissemination capability with a geodatabase, Google Earth, and GIS map servers.[10]

Operational Support

ARISCs are the MIRC's primary training platforms. When designated as PED sites, ARISCs shift focus and resources toward the management of the sites and support to PED missions. With additional contracting and active duty operational support resources, ARISCs have successfully maintained their PED sites and supported live operations multiple times. The MIRC provides 24/7 PED support to the

warfighter using an assigned 20-person mission through one of the MIRC's four expeditionary-military intelligence battalions. All four of the MIRC's expeditionary-military intelligence battalion formations have taken a turn at PED execution through this mission assignment, with the potential for expansion to a second PED line as Component 1 undergoes transformation in fiscal year 2023. The MIRC also developed the necessary instructors to complete the Army's job qualification standard required for all Soldiers mobilizing in support of PED operations.

The expeditionary-military intelligence brigades are the primary force support to PED missions. These organizations work directly with the MIRC's training team and ARISCs to meet the mobilization training and deployment requirements. This synergy between all elements has led the MIRC to deploy four teams in support of global PED operations for FORSCOM and more than 10 teams in support of special operations. The MIRC developed a facility and training capacity to meet the current fight but constantly looks to the future to sustain viability of support to PED operations. Training for large-scale ground combat operations remains a primary focus. Always Engaged is a MIRC-focused local training exercise held annually for its expeditionary-military intelligence brigades to complete Tier 3 and Tier 2 evaluations in support of large-scale ground combat operations. Globally Engaged increases the exercise complexity by challenging MIRC formations to employ and exercise their intelligence architecture in a remote environment. This series of exercises, coupled with the PED reach site's robust capability, enables the MIRC to aggressively modernize training and provide valuable intelligence to the warfighter.

Exercise Always Engaged

This Army Reserve military intelligence (MI) exercise develops and sustains MI Soldier technical skills by focusing on corps and theater-level intelligence operations. It is designed to train and evaluate rotational MI modified table of organization and equipment units and low-density sections/teams from non-rotational MI units in a fully integrated, multi-site, multi-discipline training environment.[11]

Exercise Globally Engaged

This Army Reserve MI exercise focuses on operational/non-rotational MI units'…capability to plan and execute tactical to strategic intelligence operations using current intelligence architecture. This exercise is designed to improve training readiness of MIRC formations and Soldiers through execution of operational intelligence support, live environment training, and reach-back support using MI weapons systems pointed at real-world, regionally focused mission data, in support of combatant commands and the intelligence community worldwide.[12]

Conclusion

PED operations continue to grow and evolve. The MIRC leverages its adaptability and innovation to meet emerging requirements for PED. As the operational environment evolves, the MIRC will be ready to meet the intelligence requirements to support the warfighter wherever the need occurs. Incorporating effective PACE plans, adopting Army solutions in innovative ways, and training Soldiers makes the MIRC ready to face future challenges. Always Engaged and Globally Engaged events will continue to challenge MIRC formations to better prepare them for large-scale ground combat operations. The MIRC stands ready to support the multi-domain intelligence infrastructure and ensure combatant command requirements are answered. It is Always Engaged!

Endnotes

1. Department of the Army, *United States Army Processing, Exploitation, and Dissemination (PED) Concept of Operations Version 3* (Washington, DC, 18 September 2019), 4.

2. "Cubic Awarded Contract from DISA to Continue Support for Unified Video Dissemination System," BusinessWire, March 5, 2020, https://www.businesswire.com/news/home/20200305005251/en/.

3. BAE Systems, *Geospatial eXploitation Products™ GXP Platform™* (2016), 1–2.

4. "GXP Xplorer® Overview," BAE Systems website, accessed 18 March 2021, https://www.geospatialexploitationproducts.com/content/product-videos/video-gxp-xplorer/.

5. "GXP InMotion™ Overview," BAE Systems website, accessed 18 March 2021, https://www.geospatialexploitationproducts.com/content/product-videos/video-gxp-inmotion/.

6. Ibid.

7. "SOCET GXP® Overview," BAE Systems website, accessed 18 March 2021, https://www.geospatialexploitationproducts.com/content/product-videos/video-socet-gxp/.

8. "SOCET GXP® v4.4," BAE Systems website, accessed 18 March 2021, https://www.geospatialexploitationproducts.com/content/socet-gxp/.

9. "SAIC Launches Advanced Intelligence Multimedia Exploitation Suite (AIMES)," Leidos website, https://investors.leidos.com/news-and-events/news-releases/press-release-details/2010/SAIC-Launches-Advanced-Intelligence-Multimedia-Exploitation-Suite-AIMES/default.aspx.

10. "MacAulay-Brown, Inc. Awarded Army Intelligence Analysis Contract," GlobeNewswire, August 5, 2013, https://www.globenewswire.com/news-release/2013/08/05/564591/10043223/en/MacAulay-Brown-Inc-Awarded-Army-Intelligence-Analysis-Contract.html.

11. Ernesto Clark, "Taking MI Professionals from 'Provide, Trained, and Ready' to 'Provide an Operational MI Army Reserve'," *Military Intelligence Professional Bulletin* 41, no. 3 (July–September 2015): 14.

12. Ibid.

CW3 Scotty Stock has served in the Army for 17 years and is a geospatial intelligence (GEOINT) imagery technician. He currently manages the classified communications branch at the Military Intelligence Readiness Command. He holds a bachelor's degree in history, a master's degree in intelligence studies, a graduate certificate in strategic leadership, and professional certifications in GEOINT fundamentals and imagery analysis, security plus, and project management professional.

U.S. Army photo by SSG Kenneth Burkhart

The 259th Expeditionary-Military Intelligence Brigade Commander speaks candidly with key leaders in the tactical operations center during a battle update brief for exercise Always Engaged 18 at Joint Base Lewis-McChord, WA, July 12, 2018.

Military Intelligence Maintainers Resource

by Sergeant First Class Joseph Hurst

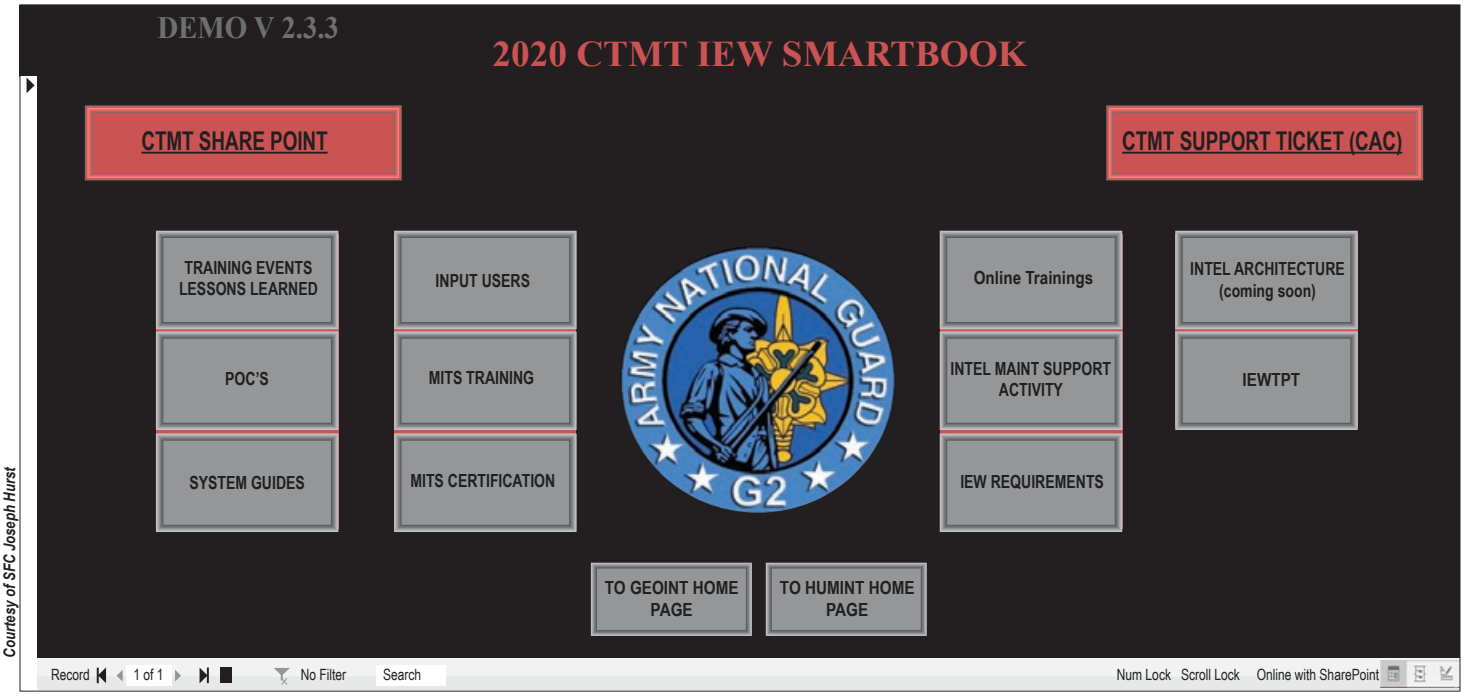
Creating the Centralized Repository

With the challenges of working during the coronavirus disease 2019 pandemic, the Army National Guard (ARNG) G-2 military intelligence (MI) systems maintainer trainer/mentors from the Collective Training and Mentor Team wanted to create a single source for documentation, training resources, and other useful information. The Collective Training and Mentor Team is a select group of subject matter experts across the MI disciplines. These individuals assist the ARNG's MI force with intelligence mission essential task list tasks and the Military Intelligence Training Strategy. Our goal was to create a centralized repository of quality information accessible by military occupational specialty (MOS) 35T (MI Systems Maintainer/Integrator) Soldiers and other government personnel who have a need-to-know, such as other 35 series (MI) or 25 series (signal corps) Soldiers when units are critically short of MOS 35T Soldiers.

We achieved this goal by consolidating a comprehensive wealth of information resourced from various intelligence and electronic warfare Soldiers throughout component 1 and component 2. Other resources included websites such as the Intelligence Knowledge Network and milSuite and the Distributed Common Ground System (DCGS) helpdesk. We produced a database with a user-friendly interface that any Solider can easily navigate.

Some of the resources included in the database are:

- Military Intelligence Training Strategy training, rosters, documentation, and certification requirements.
- System guides, technical manuals, Army regulations, and Department of the Army pamphlets for the MI systems maintainers publications library, as well as for configuration and troubleshooting.
- System administrator requirements when appointing a system administrator for various systems.
- Online training resources to assist MI system maintainers in becoming more proficient in their job.
- Lessons learned from various training events and deployments to provide understanding of current trends.
- Points of contact for the subject matter experts of the different systems and for the unit MI systems maintainers (MOS 353T [Intelligence Systems Maintenance and Integration Technician] and MOS 35Ts in the ARNG).
- Information about the Intelligence Maintenance Support Activity (the MI maintenance section) and the Intelligence and Electronic Warfare Tactical Proficiency Trainer, as well as an overview of the intelligence architecture.



Courtesy of SFC Joseph Hurst

Screenshot of the Collective Training and Mentor Team Intelligence and Electronic Warfare Smartbook Resource

Database Availability

The MOS 35T database is not yet available for wide audience use, but it was used in its Beta form during the National Training Center (NTC) rotation of the 1st Armored Brigade Combat Team (ABCT), 34th Infantry Division (1/34th ABCT). It proved to be a great resource by making user guides and configuration documentation available to the unit. This helped the unit during the reception, staging, onward movement, and integration phase at the NTC and allowed unit personnel to quickly configure their newly fielded equipment into their network architecture. This contributed to 1/34th ABCT becoming the first Army brigade combat team to be able to implement and use all of its DCGS–Army Capability Drop-1 systems during an NTC rotation.

The resource's Beta version is available for download at less than 1.5 gigabytes via MS Share Point. It is also available via mobile phone through the MS Share Point application. For access to this resource, please contact SFC Joseph Hurst or SGT Ravi Ramchandani. Their contact information can be found at https://www.milsuite.mil/book/groups/collective-training-mentor-team along with other useful information related to the mission of the ARNG G-2 Collective Training Mentor Team.

U.S. Army Photo

Military intelligence systems maintainers use testing and diagnostic equipment to troubleshoot and repair an intelligence system component.

SFC Joseph Hurst is a military intelligence (MI) systems maintainer currently serving as an MI systems maintainer and a collective training mentor for the Army National Guard (ARNG) G-2. He recently led the development of MI systems maintainer training across the ARNG for units preparing for missions around the globe. He has over 18 years of experience as a military contractor/Soldier supporting the Distributed Common Ground System-Army, MI systems maintenance, and electronic maintenance support to special operations forces. SFC Hurst holds a bachelor of science in interdisciplinary studies with a concentration in leadership and management and an associate of applied science in unmanned aerial systems technology.

Contributor:

MAJ Christopher Mision is a Texas ARNG Soldier on T-10 Active Guard Reserve, currently serving as the ARNG G-2 Training and Exercises Team Chief. He is responsible for support to ARNG MI individual training, collective training, and lessons learned, and has coordinated to develop the ARNG G-2's Collective Training and Mentor Team. MAJ Mision has over 19 years of experience in combat arms and MI and as a military contractor. He holds a bachelor of science in chemistry and a master of arts in intelligence studies.

A forward observer with 2nd Battalion, 5th Cavalry Regiment, 1st Armored Brigade Combat Team, plots points on a map to find his way during exercise Combined Resolve, 27 February 2021, at the Joint Multinational Training Center, Hohenfels, Germany. (U.S. Army photo by SSG Christopher Hammond)

Human Sensing and the Deep Fight: Closing the Division Deep Sensing Gap during Large-Scale Combat Operations

by Major Franklin G. Peachey

Author's Note: This article is an adaptation from a master of military arts and science thesis of the same title.[1]

Winter 2020—On a Dirt Road in Eastern Europe

A nameless dirt road in Eastern Europe has finally frozen solid after the tracks of an American armored division churned it into a morass of knee-deep mud. In patches, however, and off to the left and right of the road as far as the eye can see, the smoldering hulks of armored and wheeled vehicles litter the landscape. Earlier that morning, portions of the 16th Armored Division had been completing a logistical resupply to resume their movement to contact with a templated under-strength enemy motorized rifle division. As they did their work, mass rocket fire—including top-attack and thermobaric munitions—from an unseen enemy destroyed more than half of two combined arms battalions and numerous resupply vehicles in minutes. Brigade counter-fire radars tracked some of the incoming rockets originating from nearly 40 kilometers away.

The brigade combat team (BCT) that these battalions belonged to did everything right. They had their cavalry squadron screening as far to their front as their Paladins (self-propelled artillery) could shoot. The significant intelligence capabilities from the BCT military intelligence company were effectively task-organized and employed in the most favorable positions possible, with their Shadow (unmanned aircraft system) attempting to look deep within the BCT area of operations. However, a mixture of dense vegetation, rough terrain, bad weather, and electromagnetic interference routinely limited the quality and depth of the military intelligence company's sensing capabilities to the close fight.

In an ominous sign, when the BCT collection manager asked division for support from their Gray Eagle (unmanned aircraft system), the response was that division collection faced similar challenges. Also, a high enemy air defense threat imposed a limiting range on the division's combat aviation brigade up to the forward line of troops for reconnaissance purposes. Unfortunately, other division reconnaissance was unavailable—a squadron from what was supposed to be the corps reconnaissance and security BCT never materialized—and the 16th Armored Division required all of its combat effective units for the close fight. With the BCT's and division's capabilities either committed or negated, division looked to corps and above to close their deep sensing gap. The picture did not get any clearer. Corps told the division, when they were sporadically able to communicate with one another, that most assets were committed, another unit was a higher priority, or that corps assets were also operating at a degraded capacity.

No one wanted to go down this dirt path, and the undulating terrain of forested hills, rocky outcrops, and marshy fields had been an eye-opener for those accustomed to fighting in the vast expanse of the desert. Now, instead of seeing for miles and having an abundance of available collection assets, the division's BCTs were lucky if they knew what was beyond the next terrain feature. The corps headquarters was facing operational threats of its own, and the division was practically blind—outside of the sporadic intelligence reports that got through from corps—in its ability to project combat power beyond the close fight. As they would soon find out, the fire-strike received earlier that morning was only the start of their concerns as massed mechanized formations quickly overran individual BCT cavalry squadrons. For the 16th Armored Division, it was only the start of a long, cold, hard winter as its BCTs routinely made contact without advanced warning. If the 16th Armored Division was going to shape the fight for its BCTs, it needed the capability to sense deep despite dense vegetation, rough terrain, bad weather, and enemy interference.

The Problem

This fictitious scenario focuses on a nonexistent, though representative, U.S. 16th Armored Division participating in large-scale combat operations against a peer enemy in Eastern Europe. The scenario is an example of a specific type of warfare against a competent and well-equipped enemy the U.S. Army has not had to confront in nearly three decades and in routinely restricted terrain that has not posed a challenge in generations. As with Task Force Smith during the Korean War, the 16th Armored Division was not prepared to face the enemy on equal or superior terms. Its inability to sense within its deep area was one of the crucial factors inhibiting it from visualizing the battlefield, gaining an accurate situational understanding, and shaping the fight for its BCTs.

Through a 4-year study published in late 2019, the Combined Arms Center identified 17 critical capability gaps in the Army's ability to execute large-scale combat operations.[2] One area that has gained particular attention, with long-range precision fires having become the Army's top modernization priority, is the Army's ability to sense deep at echelons above the brigade.[3] While the Army focuses on sensing deep in support of potential capabilities like the strategic long-range cannon, it is important to consider a division's limited ability to sense tactically within its deep area and the way in which a human sensing capability can aid in closing this gap. Human sensing, in this context, is the activity of human sensors gathering information within a division's deep area to develop actionable intelligence for division operations.

U.S. Army photo by PFC James J. Jacquet

Men of the 19th Infantry Regiment work their way over the snowy mountains about 10 miles north of Seoul, Korea, attempting to locate the enemy lines and positions. January 3, 1951.

The current sensor gap in the division's deep area during large-scale combat operations consists of a lack of both technical and human sensing capabilities responsive to a division's deep sensing needs.[4] With most division technical and human sensing capabilities currently committed at a different echelon or gone—replaced only potentially with unequal support from expeditionary-military intelligence brigades and reconnaissance and security BCTs—the gap that battlefield surveillance brigades were meant to bridge is now a severe obstacle to a division's effectiveness. The result of this division deep sensing gap is that for a division to sense within its deep area proactively and to compete during large-scale combat operations effectively, it is "completely dependent on capabilities organic to subordinate brigades or joint, theater, or national assets."[5] While numerous technical sensing capabilities exist at corps and above, "the priority of collection for those assets is set by another commander," and access is dependent upon availability and connectivity.[6] Divisions are dependent upon the predominance of technical sensing held at echelons above the division as they prepare for the next large-scale combat operation against a threat capable of degrading access to those sensing capabilities.

This article argues that, while technical sensing advanced greatly in the last few decades, the division requires a human sensing capability to contribute in closing its deep sensing gap during large-scale combat operations. Human sensors most effectively contribute by focusing on an enemy's dispositions, composition, and course of action to provide information to a commander and their staff, which improves the time, space, and flexibility to plan and execute operations. For a division to fully leverage these advantages, it must—

- Have its own dedicated human sensing capabilities capable of collecting within the expected operational environment.
- Employ its technical and human sensing capabilities in a coordinated and complementary way.
- Actively plan and coordinate the leveraging of all human sensing capabilities within its deep area, including special operations forces (SOF) and interagency elements.

The History

Historical case studies of divisions executing large-scale combat operations in both Vietnam and Iraq demonstrate the importance of being able to sense within the division's deep area. During the 1st Cavalry Division's operations into Cambodia as part of Toan Thang 43, the division effectively leveraged both its airmobile reconnaissance squadron, the 1st Squadron, 9th Cavalry Regiment, and its company of rangers, H Company.[7] The Army had not operated inside Cambodia during its years in Vietnam, and limited intelligence was available from strategic elements like SOF and interagency elements within their area of operations. As forces crossed the border in May 1970, 1st Squadron, 9th Cavalry Regiment, and H Company proved instrumental in identifying the withdrawing enemy's dispositions, composition, and course of action throughout the area of operations. This information, along with the identification of significant enemy logistical base camps, allowed the 1st Cavalry Division to rapidly transition into base clearing operations.

A little over 30 years later, the 3rd Infantry Division crossed into southern Iraq in 2003 and began its relentless drive toward Baghdad as part of Operation Iraqi Freedom. Since 1970, numerous revolutions in military affairs occurred, drastically increasing divisional access to technical sensing capabilities to an extent unprecedented in history. It was, however, the division's reconnaissance squadron, 3rd Squadron, 7th Cavalry Regiment, in coordination with technical sensing and support from SOF and interagency elements, that rapidly assessed a situation quite different than anticipated during planning. These human sensors rapidly identified the dispositions, composition, and course of action of the well-armed and fanatically driven Fedayeen and the notable absence of significant conventional Iraqi forces.[8] This information enabled the division leadership to accept

risk and continue to press the tempo of operations. As the 3rd Infantry Division got closer to Baghdad and confronted conventional forces, the interplay of technical sensing and human sensing provided 3rd Infantry Division leaders with the time, space, and flexibility to take prompt action, ultimately resulting in the collapse of the Iraqi regime.

U.S. Army photo by SPC Dustin D. Biven, 22nd Mobile Public Affairs Det.

A cavalry scout assigned to Headquarters and Headquarters Company, 1st Battalion, 63rd Armor Regiment, 2nd Armored Brigade Combat Team, 1st Infantry Division, uses his radio to report simulated enemy activity in the area of his unit during a field training exercise for Combined Resolve X in Hohenfels Training Area, Germany, May 4, 2018.

The Assessment

The U.S. Army today fields the most lethal brigades that have ever existed, but for them to win the close fight, they require a division capable of shaping the deep fight. If divisions are to dominate within the land domain during large-scale combat operations, then the Army must focus on enabling tactical, as well as strategic, deep sensing. To start, divisions should have their own dedicated human sensing capabilities. These sensors do not have to be a cookie-cutter replication of the division cavalry squadrons employed in Iraq, nor do they need to be an imitation of long-range reconnaissance and surveillance teams borne out of Vietnam. The relative strengths and weaknesses of different human sensors vary across mission variables and are relative to the operating environment in which they are employed. Their development and structuring, therefore, must align with a division's pacing threat and the expected operational environments they are to operate within, whether in Europe, the Pacific, or elsewhere.

Finally, the realignment of dedicated human sensing capabilities to divisions must not be at the expense of technical sensing. Instead, human and technical sensors should be seen as complementary to one another and employed through a whole-of-sensor approach. In addition, divisions must recognize and seek to leverage those human sensors already operating within a division's area of operations—specifically SOF and interagency elements—as part of the approach. If divisions can rebuild their capacity to sense and effectively shape within their deep areas, through the dedication of human sensors and the development of a whole-of-sensor approach, a significant step toward the retention of land dominance will have been achieved.

Summer 2021: Deep Sensing and Land Dominance

It had been a steep learning curve for the 16th Armored Division. While U.S. forces had taken a severe blow, they were recovering and gaining windows of relative advantage across various domains against the enemy. During the spring, while the division was reconstituting in corps reserve, it received the mechanized 3rd Squadron, 89th Cavalry Regiment, to act as its division cavalry, and a long-range reconnaissance and surveillance detachment to act in direct support of its operations. The 16th Armored Division's commander and its chief of staff immediately integrated these new human sensing capabilities into the division's collection process. They appointed a chief of reconnaissance, which, in coordination with the division collection manager, ensured that both the cavalry squadron and the long-range reconnaissance and surveillance teams could execute their operations in coordination with technical sensors from the division and the joint force. In addition to the internal coordination, the chief immediately began a constant dialogue with SOF and interagency elements in the respective area of operations they were to assume in the summer.

In July, the 16th Armored Division moved out of corps reserve and promptly received a mission to attack a degraded enemy motorized division conducting a hasty defense in 72 hours. Fortunately, through continuous contact with SOF and interagency elements operating beyond the forward line of troops, the chief of reconnaissance and division collection manager had draft plans in place for the employment of available joint force and division collection assets. Because of this, the division rapidly deployed its cavalry squadron into its deep area against initial reconnaissance objectives in anticipation of the 16th Armored Division's attack. Simultaneously, the division inserted its highly mobile long-range reconnaissance and surveillance teams deep into the enemy's

support area based on information gained from SOF and interagency elements engaging with the local populace. These teams were able to both validate the condition of key infrastructure and surveil high-payoff targets for the division.

At 0600 on July 4, 24 hours before 16th Armored Division's attack, the long-range reconnaissance and surveillance teams received intelligence from a ground movement target indicator report of unidentified enemy movement inconsistent with the expected enemy defensive course of action. Corps and division unmanned aerial systems had not been able to provide additional clarification of the report because of a high enemy air defense threat; however, corps assessed the anomaly to be heavy logistical traffic. An hour later, a long-range reconnaissance and surveillance team surveilling a key intersection behind the enemy's front gained visual identification of a column of at least a battalion of enemy armor moving toward the front. The enemy was supposed to be badly mauled and, according to the most likely enemy course of action, in a hasty defense. It was not supposed to have armor, and it certainly was not supposed to be moving rapidly west along this avenue of approach. The team immediately transmitted this information back to the division, where the chief of reconnaissance informed the division cavalry, and the division collection manager began queueing available sensors to look at named areas of interest associated with the enemy's assessed most dangerous course of action—a spoiling attack.

Armed with this information early (time), the division commander rapidly considered the options available as the division cavalry prepared to meet a potential armored attack (space). If the cavalry, along with fires from the division and the joint force, was able to fix this attack, an opportunity might present itself to conduct the division attack early and under more favorable circumstances. The division began coordinating internally and externally to prepare for the armored attack and to conduct an immediate counterattack (flexibility).

At 1100 on July 4, the smoldering remains of an enemy armored column still in traveling formation sit along a dirt road in Eastern Europe. Off to the left and to the right, burned-out hulks of an enemy motorized rifle division remain in their hastily dug battle positions. Earlier that morning, as long-range reconnaissance and surveillance teams began directing long-range precision fires against enemy air defense and command and control nodes, the division's artillery and attack helicopters quickly destroyed the attacking enemy armor column as the 3rd Squadron, 89th Cavalry Regiment, first made contact and then quickly maneuvered to decisive points within the enemy's defense. Over the next hour, what had started as an enemy spoiling attack rapidly turned into an enemy rout as a coordinated and complementary sensing plan focused the full might of the 16th Armored Division and the joint force. Not only had the division regained its ability to sense within its deep area, but also, more importantly, it had reclaimed its ability to dominate on the battlefield.

Endnotes

1. This article is adapted from a previously completed master's thesis. Franklin G. Peachey, "Human Sensing and the Deep Fight: Closing the Division Deep Sensing Gap During Large-Scale Combat Operations" (master's thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 2020).

2. Dennis S. Burket, "The Evolution of the Division Formation," in *Large-Scale Combat Operations: The Division Fight,* ed. Dennis S. Burket (Fort Leavenworth, KS: U.S. Army Combined Arms Center and U.S. Army Command and General Staff College Press, 2019), 7–18, 11; and Tisha Swart-Entwistle, "Lundy retires, becoming senior mentor," *Fort Leavenworth Lamp,* January 16, 2020, https://www.ftleavenworthlamp.com/community/2020/01/16/lundy-retires-becoming-senior-mentor/.

3. Mark Pomerleau, "The Army targets systems to 'see' 1,000 miles," C4ISRNET, April 2, 2019, https://www.c4isrnet.com/c2-comms/2019/04/02/the-army-targets-systems-to-see-1000-miles/.

4. Robert S. Mikaloff, "Division Intelligence: Looking Deep to Win Close," in *Large-Scale Combat Operations: The Division Fight,* ed. Dennis S. Burket (Fort Leavenworth, KS: U.S. Army Combined Arms Center and U.S. Army Command and General Staff College Press, 2019), 79.

5. Ibid.

6. Ibid.

7. Before February 1969, H Company was an elite conventional unit (E Company, 52nd Infantry) that conducted long-range reconnaissance patrols. The Rangers of H Company executed similar dismounted human sensing operations in May 1970.

8. Gregory Fontenot, E.J. Degen, and David Tohn, *On Point: The United States Army in Operation Iraqi Freedom* (Fort Leavenworth, KS: Combat Studies Institute, U.S. Army Command and General Staff College, 2004), 127; and Jim Lacey, *Takedown: The 3rd Infantry Division's Twenty-One Day Assault on Baghdad* (Annapolis, MD: Naval Institute Press, 2007), 49.

MAJ Frank Peachey is a U.S. Army military intelligence officer and current student at the School of Advanced Military Studies in Fort Leavenworth, KS. He served a combat tour in Afghanistan as a scout platoon leader, commanded a signals intelligence company at the National Security Agency, and served in various intelligence positions at the Joint Multinational Readiness Center. He holds a master of arts in diplomacy from Norwich University and a master of military arts and sciences from the Command and General Staff College.

Be an Observer Coach/Trainer

U.S. Army photo

by Lieutenant Colonel Ian Fleischmann

Observer coach/trainers and media personnel watch as 173rd Airborne Brigade paratroopers jump onto the drop zone in Valcea, Romania, during exercise Saber Guardian 2017.

While we teach, we learn.

–Seneca the Younger
Roman Stoic philosopher (circa 4 BC–AD 65)

Introduction

One January night, I walked out of the brigade headquarters into the cold night air at Fort Drum, New York, and plodded through the snowdrifts to my car. While waiting for the engine to warm up, I listened to my voicemails, which had built up over a long day in the SCIF. One message was from Human Resources Command. "Hey, it's your branch manager. Congratulations. Your assignment to JRTC [Joint Readiness Training Center] was approved. You'll be headed to Fort Polk in the summer." Surely this was a joke. I double-checked the number and verified it came from a Fort Knox area code—no joke. After 3 years at Fort Drum, I had dreams of a joint assignment, maybe a broadening job in Europe. Maybe they had called the wrong number?

No, they had the right number. And yes, later that summer I did end up at Fort Polk. At the time, I was not pleased because I thought I was doomed to a dead-end job in a dead-end location. I was wrong. Serving as an observer coach/trainer (OC/T) is one of the most professionally and personally rewarding assignments available. Competent noncommissioned officers (NCOs), post-key developmental (KD) captains, and majors should *want* to go to the combat training centers to serve as an OC/T. The job cultivates tactical expertise, offers fantastic opportunities for professional development, and provides a great work-life balance compared to any KD position.

A Vital Role for the Army

OC/Ts serve a vital role at the combat training centers—coaching, teaching, and mentoring rotational training units to prepare them to fight and win in the most complex environments. In practice, this means that OC/Ts wear several different hats:

- First, OC/Ts coach, teach, and mentor rotational units through rigorous training and live fire exercises. This requires OC/Ts to be masters of doctrine and experienced in its practical applications. OC/Ts do this through routine engagement with their counterparts and their teams, and through planned and rehearsed after action reviews.

- Second, they facilitate the exercise by enforcing the rules of engagement to maintain a safe and realistic training environment. This takes many forms, from controlling engagements with the opposing forces to enforcing safety regulations (wearing protective eyewear, not sleeping under vehicles, etc.).
- Third, OC/Ts provide timely and relevant feedback to the larger Army on everything from trends to doctrine to force design.

All these functions are critical to the role the combat training centers fulfill in preparing units for combat, hence the reason OC/T billets are a 100-percent fill rate each manning cycle, with many of those personnel selected by name.

Even so, many NCOs, captains, and majors are hesitant to volunteer for an OC/T billet. Most see the job as intensely demanding and undesirable after coming out of hard jobs, commands, or KD positions. Some choose to look for jobs they believe will allow them to broaden professionally. Others are concerned with the reputations of Fort Polk, Louisiana, and Fort Irwin, California. However, the truth is that few jobs in the Army give you the opportunity to develop yourself tactically and professionally, while affording you the time and space to invest personally in yourself and your family.

Develop Tactically

Being technically and tactically competent is a staple of leadership. NCOs swear to it in the NCO Creed; commissioned officers hold it as a point of pride. Most leaders see themselves as tactically proficient, but after action reviews from the combat training centers consistently show that even experienced leaders can get better. Regardless of latent tactical acumen, serving as an OC/T will sharpen your tactical skills and broaden your base of experience in valuable ways.

The job of an OC/T naturally builds technical and tactical proficiency by the nature of repetitively coaching, teaching, and mentoring rotational units on the details of your profession. One of the best ways to learn and master a skill is by teaching it to others. Sometimes called the *protégé effect,* studies have shown that teaching others leads to a deeper and longer-lasting acquisition of information and skills.[1] Many fields take a shortcut to this approach by having students teach subjects to inanimate objects in a process called *plastic platypus learning* or *rubber duck debugging.* This approach is helpful, but studies have shown that reflective knowledge-building (or integrating the instructor's understanding of the material with prior experience) results in greater gains than simple knowledge-telling (or summarizing materials without integrating experience).[2] This aligns exactly with the role of an OC/T as a coach and trainer, integrating doctrinal answers with current or historical tactical experiences for the benefit of the rotational training unit.

Rubber Duck Debugging

In software engineering, rubber duck debugging is a method of debugging code. The name is a reference to a story in the book *The Pragmatic Programmer* in which a programmer would carry around a rubber duck and debug his code by forcing himself to explain it, line-by-line, to the duck. Many other terms exist for this technique, often involving different (usually) inanimate objects, or pets such as a dog or a cat.[3]

A second benefit of reflective knowledge-building is that OC/Ts rapidly expand their base of experience by observing rotational training units experiment in a broad range of environments and conditions in a short timeframe. No two brigade combat teams are the same. They all have slightly different equipment, different personnel with different strengths, different mission sets and standard operating procedures, and different commanders. Additionally, no two combat training center rotations are the same. They can be oriented in any direction across the training area, under a variety of differing operational variables, with no solidly defined "battle periods," against any permutation of a complex hybrid threat, and with orders to execute any sequence of tactical tasks. Each rotation provides a unique experience for lessons about which tactics and techniques work, training plans that breed results, and task organizations that are effective in accomplishing the mission. Given the normal rates of staff turnover, a staff officer would need to remain in a brigade combat team (BCT) for almost two decades to see the same level of experimentation by OC/Ts in a single year.

Currently, much of this experimentation centers around BCTs adapting to the Army's fundamental shift toward relearning large-scale ground combat operations, and OC/Ts are in the best position to see developing doctrine and technologies take hold. As the "engine of change for collective training in the Army," combat training centers are driving changes in tactics and equipment, from the company to the division.[4] Almost two decades of counterinsurgency operations have atrophied many of the skills necessary to fight and win these types of high-intensity conflicts. At the same time, new technologies and those same two decades of innovation-intensive combat have developed a force that is actively re-learning old tricks in new ways with new gear. OC/Ts support this role for the combat training centers by

gathering and developing tactics, techniques, and procedures and trends from every rotation, and then proliferating them back to the force through publication in professional journals, the Center for Army Lessons Learned, and video teleconferences with units and Centers of Excellence. At the same time, OC/Ts see a variety of units employ both old and emerging technologies and can learn optimal methods of employment for a wide range of missions and environments.

Develop Professionally

The mentorship doesn't stop at the boundaries of Atropia. The combat training centers are filled with a cadre of experienced officers and NCOs who want to help make each other better professionals. OC/Ts learn first and foremost from their peers. Maneuver experts become better versed in intelligence operations. Intelligence experts build their knowledge of fires and mission command systems. OC/Ts also receive fantastic and personalized mentorship from their own leadership. Every OC/T is assigned to a task force led by a post-Centralized Selection List lieutenant colonel. Military intelligence officers have the benefit of working with a post–G-2 or battalion command. For many military intelligence captains who spent their formative years in U.S. Army Forces Command (FORSCOM), this may be the first time they get regular facetime with a military intelligence lieutenant colonel. The commander of the operations group (a post-brigade command colonel) and the commanding general (a hand-selected one-star general) are actively engaged not only with every rotational unit but also with the professional development of their OC/Ts. For an NCO or a post-KD officer, no other job can provide the same level of access to battalion and brigade commanders, and their honest processes of decision making and leadership, than that of an OC/T.

Effective Leadership Techniques

OC/Ts don't just observe units; they observe Soldiers, leaders, and commanders acting under intense pressure. Every OC/T walks away from their time "in the box" with a full kit bag of leadership techniques that are effective (and often two kit bags of those that are not).

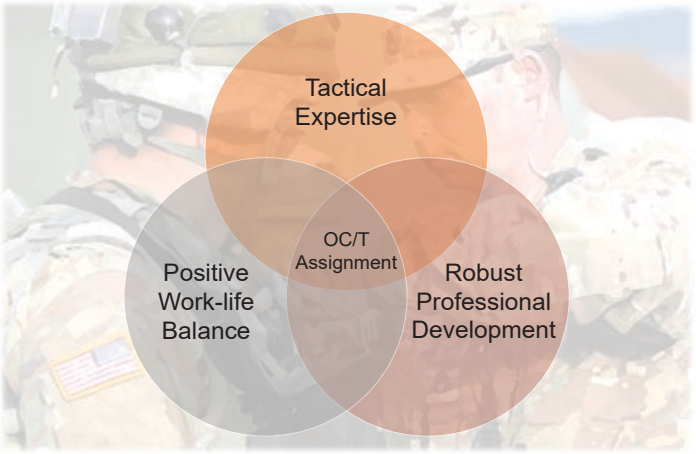
All this direct exposure to experimenting rotational training units and developing leadership places OC/Ts in a prime position to develop themselves and the profession through writing and engagement. At a minimum, OC/Ts are routinely engaging with their counterparts in BCTs across the Army as units prepare for their rotation. This kind of outreach is rewarding as OC/Ts see units taking advise-and-coach, building it into their home-station training, and putting it into practice in rotation. Beyond individual engagement, OC/Ts provide data to FORSCOM and the Centers of Excellence on performance trends, with the ability to drive larger changes in everything from equipment to doctrine to force design. And even beyond providing institutional feedback, OC/Ts have the access to directly see the results of unit experimentation and publish feedback in professional articles for broad exposure.

Develop Personally

Perhaps counterintuitively, one of the key selling points for volunteering as an OC/T is work-life balance. OC/Ts have the time to write those articles, read those books that have been piling up in the corner of the office, or catch up on that hobby they have shelved in the garage for the last few years. The rotational calendar is locked in by FORSCOM, providing a generally stable prediction of your work schedule up to a year out. Your division or brigade calendar can't compete with that. Rotations do roll through weekends and holidays, but OC/T task forces generally abide by a "work hard, play hard" mentality that respects OC/Ts as experienced professionals. Personally, I never once missed a key event for any of my three boys, and my wife can affirm that she saw me more when I was an OC/T than when I was in my KD jobs.

Location

The "dirt" combat training centers at Fort Polk and Fort Irwin do not have the best reputation for being desirable locations. After 3 years at Fort Drum, I personally had choice words for my assignment officer when the request for orders to JRTC hit my inbox. Anyone who has been to a combat training center can tell stories of the Leesville Walmart or the bustling city of Barstow, but it's important to remember your exposure as part of a rotational training unit is completely different from your life as an OC/T. What the combat training centers may lack in local metropolitan glamour, they more than make up



for in other ways. The National Training Center is a prime launching point for exploring the American Southwest, with both Los Angeles and Las Vegas only a short drive down the road. JRTC is nestled in the Louisiana "Sportsman's Paradise," surrounded by a unique local culture and cuisine. It's been said that "you'll cry when you get orders to Fort Polk, and you'll cry when you leave," and it's true. Do not let the locations dissuade you—the mission, the people, and the communities come together in ways that make up for any number of minor inconveniences.

Conclusion

Very few jobs in the Army provide the same suite of benefits as those enjoyed by an OC/T. In the Venn diagrams of jobs, the intersection of tactical expertise, robust professional development, and space to invest in a positive work-life balance is unique. The trick is in the timing. Post-KD captains and majors are at a critical point in their careers. Usually they have only a few years between command/KD and the Command and General Staff College or lieutenant colonel promotion board to invest in broadening. In both cases, the timing generally works for officers to invest in their own self-development while affording their family some of the balance they may have lost in KD assignments. The combat training centers offer a rare opportunity to combine self-development, the ability to have a real impact on the Army Total Force, and work-life balance. So go ahead, give it a shot. You won't regret it.

Endnotes

1. Annie Murphy Paul, "The Protégé Effect: Why teaching someone else is the best way to learn," *Time*, November 30, 2011, https://ideas.time.com/2011/11/30/the-protege-effect/.

2. Aloysius Wei Lun Koh, Sze Chi Lee, and Stephen Wee Hun Lim, "The learning benefits of teaching: A retrieval practice hypothesis," *Applied Cognitive Psychology* 32, no. 3 (May/June 2018): 401–410, https://onlinelibrary.wiley.com/doi/full/10.1002/acp.3410.

3. Wikipedia, s.v. "Rubber duck debugging," last modified 14 February 2021, 19:10, https://en.wikipedia.org/wiki/Rubber_duck_debugging.

4. Department of the Army, Army Regulation 350-50, *The Combat Training Center Program* (Washington, DC: U.S. Government Publishing Office, 2 May 2018), 3.

LTC Ian Fleischmann is a military intelligence officer and served as the brigade S-2 observer coach/trainer at the Joint Readiness Training Center, Fort Polk, LA, from 2018 to 2019. He is currently Chief of Operations Branch, Headquarters, Department of the Army, Deputy Chief of Staff, G-8 Force Development (Intelligence and Electronic Warfare Portfolio).

Special Operations Forces' Structured Readiness Model Makes Conventional Military Intelligence Unit More Effective

by Lieutenant Colonel Jesse Chace

Empowerment without context will lead to havoc.

—Alexis de Tocqueville
French philosopher and historian, 1805–1859

Introduction

As a U.S. Army Intelligence and Security Command (INSCOM) forward collection battalion aligned against U.S. Africa Command (USAFRICOM) requirements, the 307th Military Intelligence Battalion (MI BN) continuously deploys multi-disciplined intelligence collectors into austere and complex sociopolitical environments on a foreign continent to answer strategic intelligence requirements, sometimes with little notice. Fundamentally, these conditions are no different from those embraced by special mission units and their intelligence enablers—units that have learned that structured readiness models are critical to sustaining continuous operations of heightened sensitivity, urgency, and risk. These units rely on skilled and experienced military intelligence (MI) Soldiers who have long since mastered the fundamentals. While equally motivated, the majority of 307th MI BN collectors—human intelligence (HUMINT), counterintelligence (CI), and signals intelligence (SIGINT)—are on their first MI duty assignment. It is a population that continues to get younger and less experienced, particularly within CI, where nearly two-thirds of special agents were still on probationary status into 2020. Providing this population with ample time for focused training, as well as affording them a range of experiential opportunities, will be vital to future mission success. This makes structured readiness models all the more relevant and necessary to the 307th MI BN.

The Problem

Over the course of the unit's 4-year existence, 307th MI BN collectors have done their best to simultaneously balance lengthy training pipelines, language requirements, leave opportunities, garrison responsibilities, and preparation/support to ever-changing mission requirements in support of the Africa community of interest both at home and abroad. As an over-tasked and under-manned communal force-pool for USAFRICOM, the unit has struggled to reach optimal levels of readiness, response, technical/tactical proficiency, and command climate. Furthermore, collectors' inability to complete prescribed training pipelines in a 3-year assignment has undercut the value placed on professional competency, de-incentivizing Soldiers from extending their tour of duty at one of the United States Army's most requested duty stations, Vicenza, Italy. Failure to develop and retain experienced personnel who have mastered the fundamentals has directly affected credibility with USAFRICOM staff and key embassy officials throughout Africa. As a result, a habitual lack of permissions prevents collectors from maximizing their authorities on a continent that is presently serving as ground-zero for the convergence of global expansion. This creates opportunity for our competitors to "set the theater" in their own vision.

Perhaps more importantly, Soldiers have failed to obtain any semblance of predictability in one of the most notorious duty stations for "early return of dependents" in the United States Army (again, Vicenza, Italy).[1] Simply put, family and Soldier readiness has suffered in what should be a once-in-a-lifetime assignment inside the cradle of European civilization. We had to re-scope our operational design so that we could provide Soldiers and their families with the level of predictability they deserve, enable our higher brigade headquarters to prioritize a growing number of requirements, and meet our senior leaders' intent of mastering fundamentals and maximizing authorities.

The Solution

We chose the Joint Operations Readiness and Training System (JORTS) because of its inherent symmetry in balancing forecasted missions with rapid response requirements. The system is designed to "prepare forces for mission employment to sustain persistent [overseas] presence and provide for contingency response on a global scale."[2] The JORTS cycle is typically found within certain special operations forces (SOF) units that not only maintain a similar persistent, high operating tempo forward presence, but have also proven that structured readiness cycles can help lead to occupational excellence and job satisfaction. Within this system, operational elements independently cycle through a variation of four phases:

- ✦ Training (individual and unit).
- ✦ Alert.
- ✦ Pre-Deployment (reconstitution).
- ✦ Deployment.

Unlike many U.S. Army Forces Command (FORSCOM) models, the JORTS cycle eliminates the inherent planning fratricide that occurs when attempting to balance continuous operations with short-notice missions—something most FORSCOM units do not have to balance. The unit can actually support more missions by separating the available force pool for short-notice, limited-duration requirements (i.e., the alert team) from the available force pool for continuous long-term requirements (i.e., the deployment team). Ironically, the alert phase also improves overall predictability by narrowing the timeframe in which Soldiers know they will have no predictability at all.

How to Apply the JORTS Cycle. Cloaked by a doctrinal-sounding name, the JORTS cycle is simply a common-sense way of maintaining peak readiness while supporting a unique set of mission requirements. It does not actually exist in doctrine. As a team-centric approach to organization and mission effectiveness, it has withstood the test of time in organizations for which a frenetic pace of operations depends on strong systems.

Most conventional units are not conducive to this cycle without significant modifications to their task organization. Adjustments were relatively easy for the 307th MI BN because the battalion deploys individual collectors based on mission-requirements, not necessarily in accordance with its modified table of organization and equipment (MTOE) structure. Reducing our overall number of teams by simply increasing the size of each team enabled more capacity spread over each phase of the cycle. It also limited the number of required team leaders to only those most qualified for the job and enabled teams to better absorb short-term personnel losses caused by unpredictable events such as Noncommissioned Officer Education System courses, surgery, and emergency leave.

Selecting Team Leaders. It is important to select team leaders who have the maturity to avoid the five dysfunctions of a team: absence of trust, fear of conflict, lack of commitment, avoidance of accountability, and inattention to results.[3]

Five Dysfunctions of a Team

- ❖ **Absence of trust**—unwilling to be vulnerable within the group
- ❖ **Fear of conflict**—seeking artificial harmony over constructive passionate debate
- ❖ **Lack of commitment**—feigning buy-in for group decisions creates ambiguity throughout the organization
- ❖ **Avoidance of accountability**—ducking the responsibility to call peers, superiors on counterproductive behavior which sets low standards
- ❖ **Inattention to results**—focusing on personal success, status, and ego before team success

Photo courtesy of PublicDomainPictures.net

Though they should be skilled at their craft, the best team leader may not be the most talented collector on the team. In fact, it is more important for them to be the best planner, problem solver, and administrator—capable of holding the team together in garrison *as well as* holding their own downrange. By enabling stronger relationships at work and promoting greater feelings of safety, protection, and belonging, the team-centricity of JORTS has a significant impact on unit culture, climate, and productivity. This was on full display during the initial coronavirus disease 2019 (COVID-19) outbreak in Northern Italy, when there was no template for how military organizations would absorb the impacts of such prolonged restrictions on travel and manning. Individual and unit success during this time was predicated on team leaders who found ways for their members to remain engaged and productive despite a variety of circumstances that often made physical collaboration impossible (i.e., quarantine location and restriction-level).

As depicted in Figure 1 (on the next page), the JORTS cycle demands that specific team-level expectations be set within each phase. Focusing each team's efforts provides maximum predictability, improves readiness, builds expertise, and optimizes mission execution.

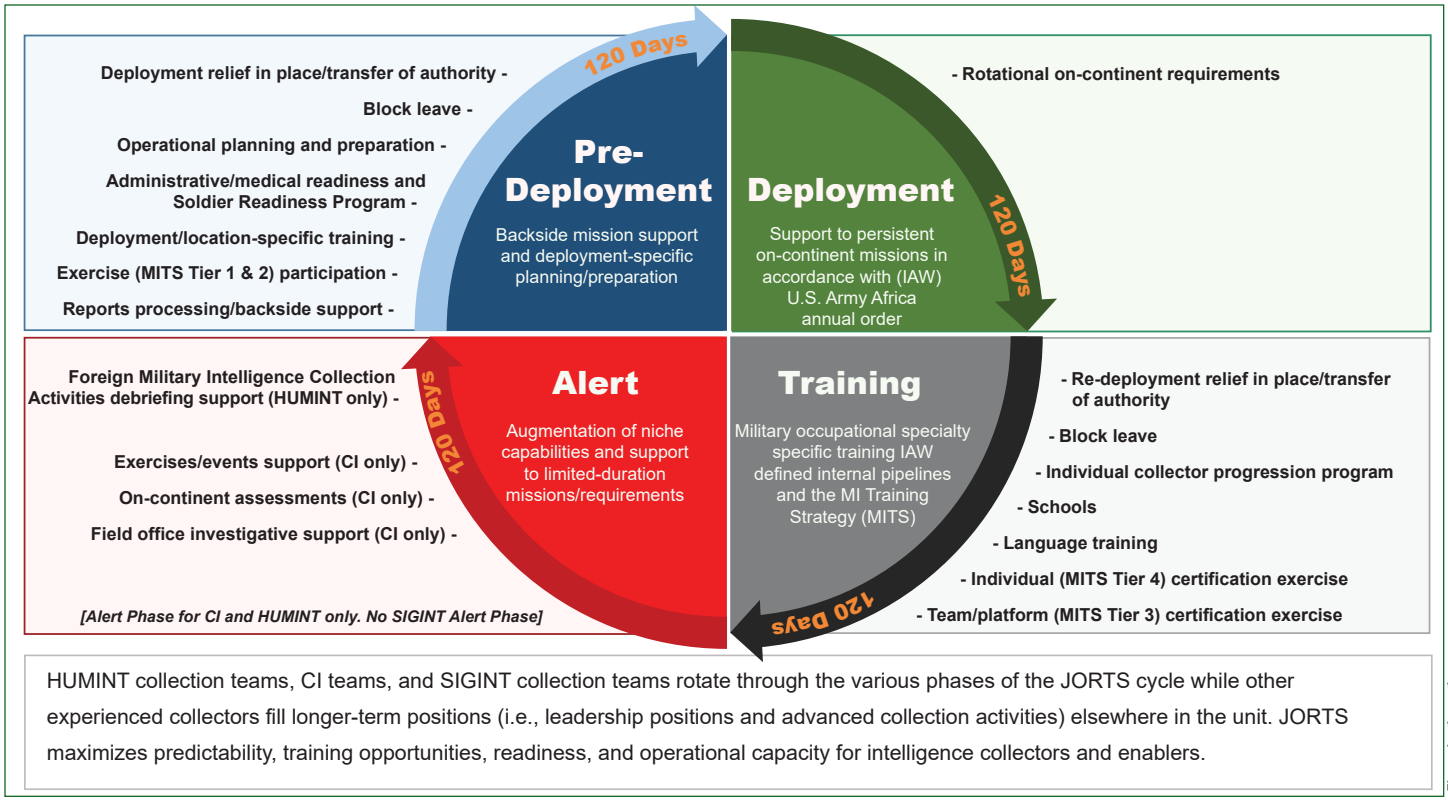


Figure by the author

Figure 1. The JORTS Model Adopted by the 307th Military Intelligence Battalion (Forward Collection Battalion)

Quoting 19th century French philosopher and historian Alexis de Tocqueville, retired GEN Stanley McChrystal writes in *Team of Teams,* "empowerment without context will lead to havoc."[4] GEN McChrystal elaborates on this concept:

> ***This is the risk run if traditional, hierarchical organizations just push authority down, ceteris paribus [i.e., if all other relevant things, factors, or elements remain unaltered]…An organization should empower its people, but only after it has done the heavy lifting of creating shared consciousness.***[5]

With this in mind, the 307th MI BN model meshes mission command and technical control in a manner that provides clear, reliable, and predictable oversight, as well as knowledgeable guidance and direction to empowered team leaders. While company commanders retain mission command of their teams throughout the cycle, technical control rotates between subject matter experts who provide clear purpose and well-understood deliverables in each phase. Meanwhile, team leaders provide precision leadership to Soldiers they know completely. This includes managing relationships, ensuring team members are employed in the most effective way possible, providing continuous counseling and mentorship, and administratively accounting for their people. In a career field where true leadership opportunities lack below the sergeant first class level, these positions are critical to promoting personal and organizational growth for our staff sergeants. Besides, team leaders who are hyper-focused "down" on their personnel and equipment better enable every echelon of leadership above them to think and influence "two levels up."

Platoon-Level Management. While companies within a forward collection battalion are small, the requirements they must simultaneously balance across multiple intelligence disciplines necessitate platoon-level management between the company commander/first sergeant and individual team leaders. Platoon leaders are ideal for managing the entirety of the JORTS cycle. They ensure teams are prepared to deploy, training is forecasted and executed consistently, personnel are counseled regularly, and gaps are accounted for and filled. In other words, platoon leaders and platoon sergeants are the lynchpins to ensuring the cycle works as designed, highlighting the value of MI second lieutenants within a forward collection battalion. Unfortunately, this unique excess capacity within the 307th MI BN is not cemented in its MTOE, and therefore it is only preserved sporadically through a close working partnership with our neighbors in the 173rd Infantry Brigade Combat Team (Airborne). The empowerment, leadership, education, and training opportunities afforded to these officers within the context of an INSCOM forward collection battalion JORTS cycle arguably surpass that of FORSCOM MI companies. Their presence also allows warrant officers to maximize their skillsets through training development and operations rather than filling leadership positions.

JORTS in a Non-SOF Environment. The utility of a JORTS cycle in a non-SOF environment sparks several commonly asked questions.

First, is the JORTS cycle flexible? Yes. Although maintaining team integrity is ideal, leaders may swap collectors between teams based on the situation, for example, an impending permanent change of station, pop-up Basic Leader Course or Advanced Leader Course dates, and pregnancy. For instance, if a HUMINT collection team (HCT) member exiting their deployment cycle is making a permanent change of station in 4 months, leaders may elect to shift him/her to the HCT entering the alert phase. This would provide more capacity to a higher-priority mission such as home station Foreign Military Intelligence Collection Activities debriefings, rather than "wasting it" in a way that will no longer benefit the unit. Platoon leaders may also adjust "transition" dates between teams based on the needs of the team or the mission. However, one must keep in mind that the intent of the JORTS cycle is to provide and enforce structure and processes that allow training and predictability to take root; if it is flexed too much and too frequently, it becomes meaningless. Proper planning, forecasting, and prioritization are crucial to making the JORTS cycle work, not its inherent flexibility.

Second, does the stove-piped nature of the JORTS cycle prevent the unit from training and operating as cross-functional teams? No, it does the opposite. The JORTS cycle enables teams to better plan and integrate with "sister teams" from other platoons that are in the corresponding phase of their cycle. For example, HCTs from Alpha Company and CI teams from Bravo Company are able to—

- ✦ Train and certify together at home station in one phase.
- ✦ Conduct mission preparation and engage with analytical counterparts together in another phase.
- ✦ Deploy to the African continent together in yet another phase.

For our organization, it offers an unprecedented level of collaboration, integration, and relationship building between disparate yet complementary capabilities.

Third, why use only 120-day deployments? Because it is much easier to sustain a high pace of operations over 120 days than, for example, 180. With teams conducting multiple deployments over a 3-year tour, 120-day deployments are more sustainable for the force and provide better flexibility should Soldiers need to extend downrange. Not only does this help prevent individual gaps in mission coverage, but it also provides flexibility in the event of sudden and unforeseen restrictions in and out of theater, such as

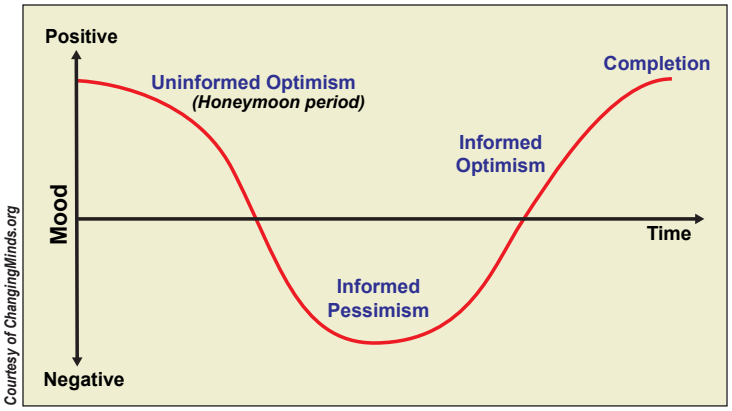
U.S. Army photo

A 307th Military Intelligence Battalion Soldier in civilian attire engages with a key partner of the Ugandan military while forward deployed to East Africa.

COVID-19. As depicted earlier (in Figure 1), 120-day deployment phases do not include relief in place and transfer of authority, which extend actual boots-on-ground timelines to about 140 to 150 days.

Creating Experienced Collectors. In addition to the valuable experience Soldiers gain through a wide variety of on-continent missions, adherence to the JORTS cycle should allow even the most junior MI Soldiers to complete their prescribed training "pipelines" after two iterations through the cycle (32 months). This creates a more seasoned and experienced population of collectors to fill key leadership positions or work dedicated mission sets, depending on their strengths and career goals. On the operational side, these include CI investigations and advanced HUMINT collection operations. On the leadership side, these include the team leader, the operational management team's noncommissioned officer in charge, and the platoon sergeant. Based on a 36-month length of tour, these opportunities incentivize extension out to 48 months for those exceptional Soldiers who qualify.

Transition and Application. The transition to a JORTS cycle, like any workplace change, required a patient and deliberate approach in order to ensure maximum buy-in and an optimal structure. For the 307th MI BN, the process took roughly 4 months, which involved identifying the need for change, communicating the change, developing a cadre of change



The Positive Change Cycle

agents, building the implementation plan, and shepherding unit members through the "positive change cycle."[6]

After an additional 45 days to allow teams to "gel" and forecast their training calendars, the unit kicked off the cycle in February 2020. The JORTS had several significant and immediate impacts. First, it allowed platoon sergeants to easily forecast team-level training calendars beyond 12 months at the name-tape level. This significantly improved both predictability and focused training. Second, the separation of limited-duration and long-term missions into separate phases enabled the unit to maximize its capacity, resulting in an increase in the number of operational requirements we are supporting for U.S. Army Africa/USAFRICOM. Third, the transition benchmarks inherent to JORTS were instrumental in keeping teams focused on specific readiness timelines and objectives amidst the chaos brought on by the initial COVID-19 outbreak from February through April 2020. As a result of the continued pandemic, this paradigm has continued to instill the necessary feelings of hope and change throughout wave after wave of new and/or extended restrictions that cause Soldiers to be left with little light at the end of a monotonous tunnel. In other words, established yet flexible transition dates between JORTS phases have continued to provide a stabilizing 300-meter target in a time filled with more unknowns than knowns.

In August 2020, the battalion conducted a comprehensive review of the JORTS experiment in order to ensure the cycle was meeting the unit's operational needs. While deliberate analysis identified the need for minor modifications to the cycle, commanders and mission managers throughout the organization agreed that the JORTS cycle should be protected at all costs and re-evaluated after at least one complete cycle (June/July 2021). In fact, the unit found that its new operational design had enforced a level of planning at the company level and below that now outpaced and outmatured its planning, prioritization, and orders processes at the battalion and higher levels.

JORTS could fail outside of its natural SOF environment. To prevent this from happening, two things must occur:

- Tactical-level leaders must properly plan and forecast individual timelines in order to prevent excessive shifting of personnel.
- Operational-level leaders must ruthlessly prioritize requirements in a way that guards dedicated training and preparation windows.

Conclusion

The JORTS cycle has withstood the test of time for organizations with a frenetic pace of operations. Not only does the JORTS cycle lead to more efficient and effective training and operational support, but it also leads to better junior leaders and command climate. Overall, it maximizes predictability, training opportunities, readiness, and operational capacity for intelligence collectors and enablers.

Epigraph

Alexis de Tocqueville, quoted in Stanley McChrystal, *Team of Teams* (New York: Penguin Publishing Group, 2015), http://community.vitechcorp.com/breaking-systems-engineering-and-three-ways-to-bind-the-fractures/.

Endnotes

1. U.S. Army Installation Management Command, *FY 2019 Early Return of Dependents Report* (2019).

2. U.S. Special Operations Command (USSOCOM), *Capstone Concept for Special Operations 2006* (MacDill Air Force Base, FL: USSOCOM, 2006), 12, https://www.hsdl.org/?view&did=479511.

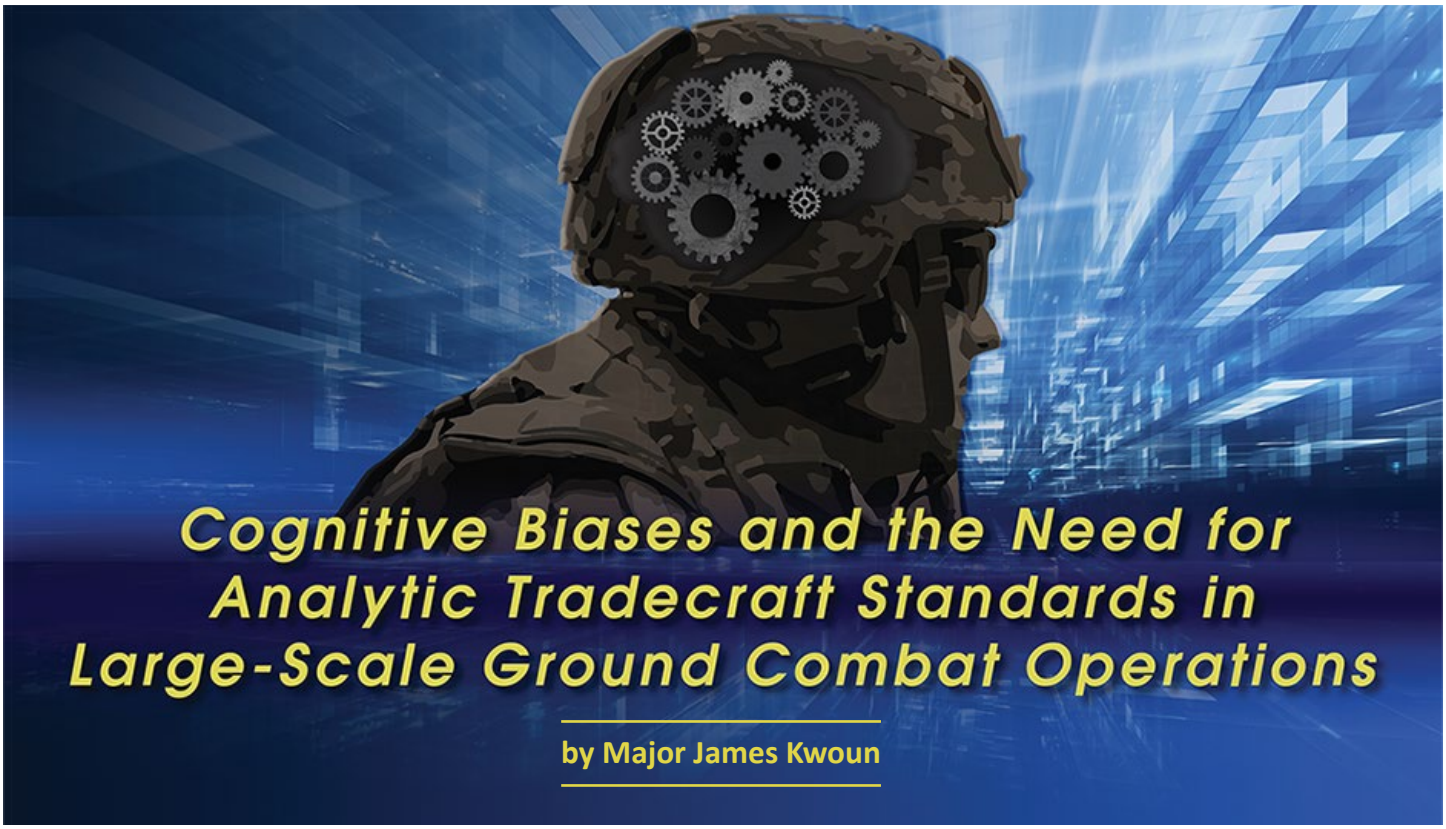
3. Patrick Lencioni, *The Five Dysfunctions of a Team* (San Francisco: Jossey-Bass, 2002).

4. McChrystal, *Team of Teams*.

5. Ibid.

6. "The Positive Change Cycle," Changing Minds website, accessed 22 January 2020, http://changingminds.org/disciplines/change_management/psychology_change/positive_change.htm.

LTC Jesse Chace is the commander of the 307th Military Intelligence Battalion (Forward Collection Battalion) in Vicenza, Italy. He is a career military intelligence officer who has served in a variety of special operations forces and interagency assignments, most recently as the Director of Operations for the Joint Special Operations Command Intelligence Brigade.



Cognitive Biases and the Need for Analytic Tradecraft Standards in Large-Scale Ground Combat Operations

by Major James Kwoun

When inferring the causes of behavior, too much weight is accorded to personal qualities and dispositions of the actor and not enough to situational determinants of the actor's behavior.

—Richards J. Heuer Jr.

Introduction

The U.S. Army's focus on prevailing in large-scale ground combat operations will present unique challenges for the intelligence warfighting function. As stated in FM 3-0, *Operations,* these types of operations have historically been "more chaotic, intense, and highly destructive than those the Army has experienced in the past several decades."[1] The enormous pressures generated during large-scale ground combat operations will make Army all-source analysts particularly vulnerable to cognitive biases. Dr. Richards Heuer Jr., author of the *Psychology of Intelligence Analysis,* defines cognitive biases as "predictable mental errors caused by simplified information processing strategies."[2] Studies have shown that these biases become more likely under ambiguous, traumatic, and time-constrained circumstances, which are exactly the challenges analysts will encounter during a large-scale ground combat operations environment.[3]

The Army's past participation in large-scale ground combat operations suggests these challenges are enduring and will require a Service-wide solution. The Army can mitigate the inevitable onset of cognitive biases in its analysts by implementing analytic tradecraft standards. Cognitive biases are manageable and even preventable because they are natural tendencies that recur throughout history. This article will examine historical lessons to identify examples of cognitive biases that could re-emerge in future large-scale ground combat operations.

Cognitive Biases and Analytic Tradecraft Standards

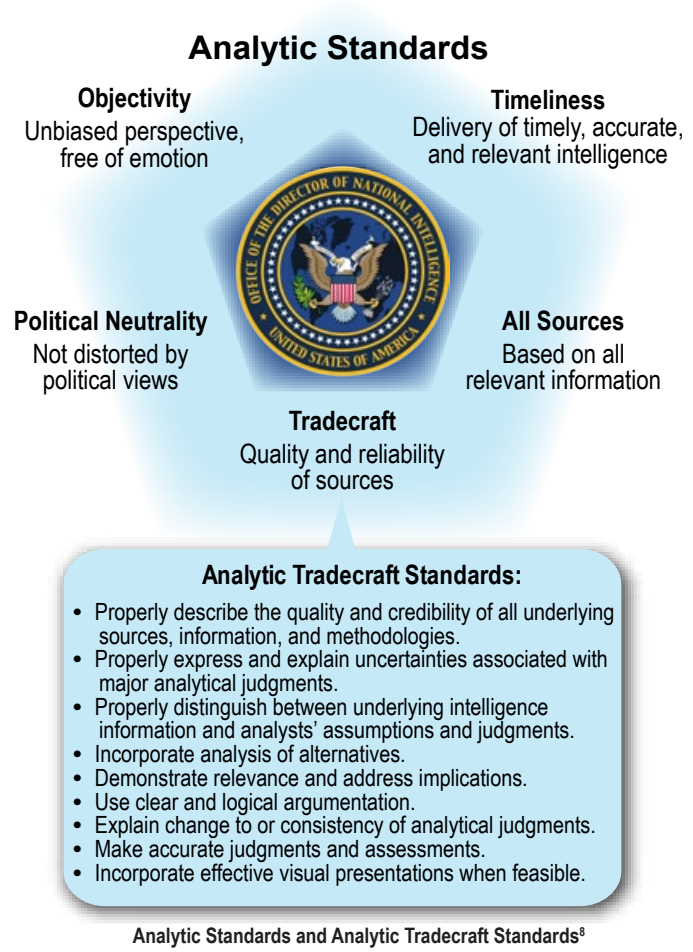
Cognitive biases are natural human tendencies to rely on experiences or what Dr. Heuer calls pre-existing "mental models" when thinking about issues.[4] Our brains subconsciously develop patterns of thought and general expectations based on life experiences. These thought patterns and expectations can be valuable, especially if they develop into expertise. They can also become a liability because they vary widely between individuals and place limits on thinking. For example, Army analysts may subconsciously filter out enemy courses of action that are inconsistent with their experiences. Additionally, analysts may automatically default to previously successful mental templates or frameworks when assessing current threats with similarities to past threats. These situations leave commanders to gamble the success of their operations on the intuition of analysts operating without a common framework to mitigate cognitive biases.

The intelligence community recognized the importance of mitigating cognitive biases and established eight analytic tradecraft standards, which eventually became nine

standards, when it first published ICD 203, *Analytic Standards,* in 2007.[5] This directive applies primarily to those all-source organizations under the purview of the Director of National Intelligence, signified by whether they received funding through the National Intelligence Program. ICD 203 is not binding on the entire Army unless directed by policy, given that only a portion of the Army Military Intelligence Corps is funded through the National Intelligence Program or conducts a national-level mission. However, ICD 203 is based on widely applicable principles that promote critical and creative thinking. An examination of past large-scale ground combat operations reveals the enduring need for critical and creative thinking to mitigate cognitive biases. The nine analytic tradecraft standards in ICD 203 provide the Army with a starting point toward this end.

ICD 203 and Army Doctrine

ATP 2-33.4, *Intelligence Analysis,* 10 January 2020, includes an appendix that details the Intelligence Community Analytic Standards established by ICD 203, as well as the integration of the standards into Army intelligence analysis in action.[6] Army doctrine forms a systematic body of thought describing how Army forces intend to operate. It applies to all operations, describing how to think about operations and what to train. It is an authoritative guide for leaders and Soldiers.[7]



Analytic Standards and Analytic Tradecraft Standards[8]

Historical Case Studies

Three case studies demonstrating cognitive bias are described below: Battle of the Bulge, Gulf War Scud hunt, and consolidating gains during Operation Iraqi Freedom.

Case 1: Battle of the Bulge. The Battle of the Bulge was the last major German offensive on the Western Front during World War II. On December 16, 1944, a German force consisting of 38 divisions and 240,000 troops attacked a weak part of the Allied line across the Ardennes forest, achieving complete surprise.[9] This operation was Adolf Hitler's risky attempt to regain the initiative and reverse the tide of the war through a decisive victory. Initially, United States Army GEN Omar Bradley assessed that the Germans were merely conducting a spoiling attack to disrupt Allied offensive preparations farther north, indicating the degree to which the Allies were caught off guard.[10] The Allies ultimately defeated the German offensive, but the cost of unpreparedness was high. Reports indicated American casualties were 41,315 people killed, wounded, and missing in the 18-day period between December 16 and January 2.[11] The actual numbers were likely higher, and American casualties may have totaled 75,000 by the time the battle ended in late January.[12]

Apparent anchoring biases existed throughout Allied formations before the battle. As Dr. Heuer describes, anchoring biases occur when "some starting point, perhaps from a previous analysis of the same subject or from some partial calculation," subconsciously influences analysts to arrive at conclusions close to that starting point.[13] This type of bias can be so powerful that even arbitrary anchors or starting points can influence analysts. Between September and December 1944, Allied "optimism" that the Germans were nearing defeat "conditioned all estimates of the enemy's plans and capabilities," according to the United States Army Center for Military History.[14] Four days before the German attack, 12th Army Group intelligence assessments were still reinforcing this optimism and highlighting the Germans' deteriorating military situation.[15] In this case, the general tone of optimism served as an anchor or starting point that appeared to have subconsciously biased analysts and commanders into making conclusions that the Germans were incapable of offensive operations.

Confirmation biases may have reinforced this anchoring effect. Confirmation biases occur when analysts subconsciously recall or interpret information in a manner that supports their existing beliefs. By December 1944, Allied intelligence had largely concluded that the rugged, heavily forested region of the Ardennes was merely a transit point for the Germans to shift forces north and south. The official United States Army history of the battle also suggests that

the Allies ruled out a German offensive in the area because of a "subconscious assumption" that the Ardennes was "impassable" for vehicles.[16] These conclusions influenced how the Allies filtered and interpreted new information. For example, two United States divisions near the Ardennes reported increased nighttime vehicle activity by the Germans in the days leading up to the battle.[17] These reports were discounted as normal occurrences as enemy units transited the area. Confirmation bias even filtered down to the regimental level. One regimental commander even "rebuked" his S-2 for labeling increased German vehicular activity as "enemy movement," according to the United States Army Center for Military History.[18]

U.S. Army photo

American troops drag a heavily loaded ammunition sled through the snow as they move for an attack on Herresbach, Belgium, January 1945.

Another cognitive bias may have influenced the Allies—*mirror imaging*. The mirror-imaging bias occurs when analysts project their own mindset onto others or assume that adversaries will act in the same manner as the United States. In retrospect, the German offensive was overly ambitious and irrational if viewed from an Allied military perspective. Hitler squandered valuable resources in a risky operation from which the German military never recovered. Allied commanders were expecting "an enemy reaction which would be rational and therefore predictable" before the battle, according to the U.S. Army Center for Military History.[19] Furthermore, the Allies expected that the highly respected German commander in the West, Field Marshal Gerd von Rundstedt, would realize the limitations of his forces and wage a defensive campaign within his means.[20] It turned out, however, that Hitler was making all the critical decisions. The decision calculus that Hitler used turned out to be far different from the one the Allies assumed the Germans would use.

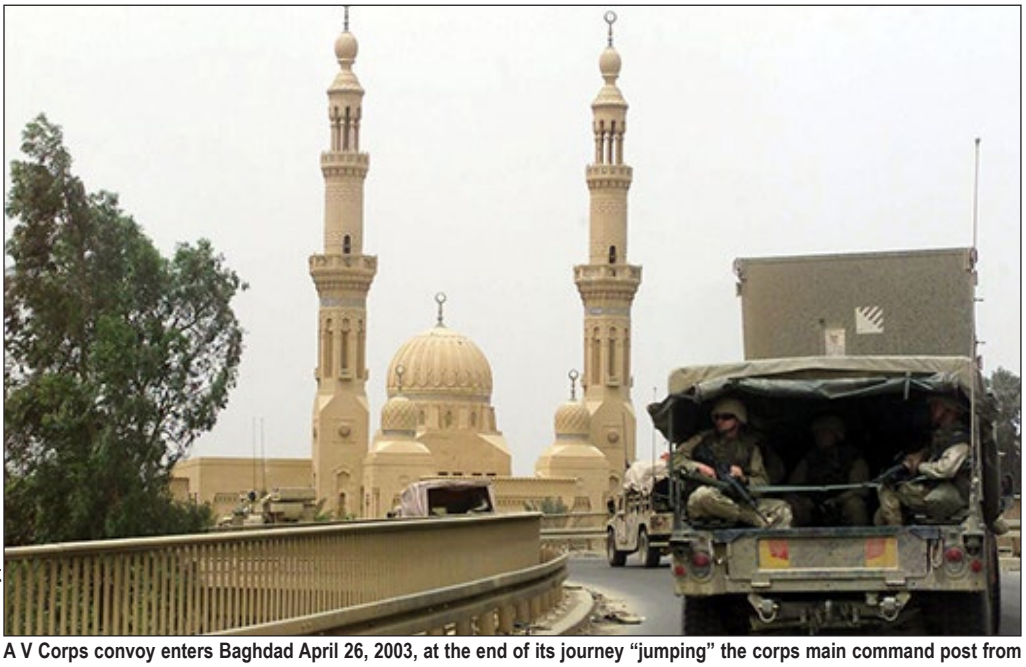
Case 2: Gulf War Scud Hunt. Iraqi Scud missiles represented a strategic concern for the George H. W. Bush administration during Operation Desert Storm in 1991. The Iraqis fired 88 Scuds against targets in Israel and Saudi Arabia throughout the 44 days of the conflict, with 26 of these attacks occurring against Israel in the first week.[21] The Scuds themselves were inaccurate, unreliable, and militarily insignificant. However, Israeli threats to retaliate against Iraq concerned the Bush administration because of the diplomatic and political implications if Israel followed through. The administration feared Israeli military action would cause Arab members to leave the coalition that formed after Iraq invaded and occupied Kuwait in August 1990. As Michael Gordon and Bernard Trainor write in *The Generals' War,* "there were few things the president and his top aides worried about more" than keeping Israel out of the war.[22] Despite this emphasis, the coalition's counter-Scud campaign failed to prevent strikes against Israel and never produced a confirmed kill of a mobile launcher.

The intelligence community made a faulty assumption that contributed to the lack of preparedness to address the Iraqi Scud threat. Cognitive biases frequently manifest themselves in the form of assumptions that analysts take for granted because of subconscious beliefs. Before the war, the intelligence community assumed that Iraqi Scud crews would follow the same launch procedures that the Soviet Union had used, which took up to 90 minutes.[23] Iraqi Scuds at the time were modified Soviet missiles that could be fired from fixed sites or mobile transporter erector launchers. These launchers proved to be particularly challenging to detect and target. If Iraq had used Soviet procedures, coalition forces could have targeted the mobile transporter erector launchers with a reasonable chance of success. Instead, Iraq skipped many Soviet calibration procedures and reduced the time for these launchers to launch and evacuate an area to 10 to 30 minutes.[24] Gen. Merrill McPeak, the Air Force Chief of Staff at the time, remarked after the war, "we put about three times the effort that we thought we would on this job [of destroying Scuds]."[25]

GEN Norman Schwarzkopf, U.S. Central Command commander at the time, provided congressional testimony that is relevant to this discussion of cognitive biases. Cognitive biases are hard to detect because they exist in the subconscious mind. At the same time, the conditions that make these biases more likely are easier to identify. After the war, GEN Schwarzkopf testified that the intelligence community needed a "standardized methodology…for making estimates and predictive analysis."[26] He criticized the intelligence community for providing "unhelpful" analysis that was "so caveated" and contained "so many disclaimers" in an apparent effort to hedge against being incorrect.[27] In one anecdote, he described the irony involved when a battle damage assessment claimed a bridge was only 50 percent destroyed despite the fact that no vehicles could cross it.[28] GEN Schwarzkopf's testimony reinforces the importance of uniform standards on how to express analytic uncertainty and clearly communicate conclusions to commanders. Enforcing these standards will prevent cognitive biases by requiring analysts to put thought into their arguments with a level of rigor that otherwise would not occur.

Case 3: Consolidating Gains during Operation Iraqi Freedom. The legacy of Operation Iraqi Freedom is one in which U.S. and coalition partners were successful in their initial military objectives but failed to consolidate gains sufficiently to enable enduring success. In March 2003, President George W. Bush ordered the initiation of Operation Iraqi Freedom to remove Saddam Hussein from power. In less than 3 weeks, United States–led coalition forces seized the capital Baghdad and ended Hussein's regime in Iraq. The coalition struggled, however, to bring stability throughout the country and adjust as an insurgency began developing. Soon, United States forces became involved in sustained counterinsurgency and counterterrorism operations in Iraq that lasted for years, stretching Army resources in particular to a critical point. The consolidation of gains will always be an important requirement during large-scale ground combat operations, one for which the Army must continuously prepare.

The U.S. military intelligence community exhibited cognitive biases when assessing the enemy that the Army expected would resist the coalition's drive to seize Baghdad. Before the war, military intelligence analysts focused on studying Iraq's elite Republication Guard and conventional army formations. An Army War College study of the war states that the United States–led coalition had an "analytical bias toward a familiar, hierarchical, Soviet-style enemy."[29] Because of this anchoring bias, analysts initially failed to forecast the significant role that Iraq's paramilitary forces would play during the fight to remove Hussein from power. Furthermore, the same Army War College report describes how intelligence analysts before the war had difficulty "analyzing new information outside their premade templates of Iraqi regime forces."[30] This description fits the classic definition of confirmation biases, in which analysts subconsciously filter new information in a manner that supports their pre-existing beliefs or mental frameworks. Thus, an initial anchoring bias appears to have influenced military intelligence analysts, which confirmation biases continued to reinforce.



U.S. Army photo

A V Corps convoy enters Baghdad April 26, 2003, at the end of its journey "jumping" the corps main command post from Camp Virginia, Kuwait, to Camp Victory on the outskirts of Baghdad.

These biases endured even after the fall of Baghdad as coalition forces began efforts to consolidate gains. The U.S.-led coalition remained anchored in a conventional warfighting mindset even as the focus turned to counterinsurgency operations. Consequently, military intelligence analysts "continued to try to explain the enemy in terms of large land forces," according to the same Army War College report cited earlier.[31] COL Derek Harvey, an intelligence officer in Iraq at the time, expressed frustration that "unless you could lay out a military-style hierarchy of command and control, a bad organization didn't

exist."[32] These anchoring biases prevented intelligence analysts from achieving a more comprehensive understanding of the political, social, and economic factors driving the growing violence at the time. The coalition's continued fixation on conventional warfighting even as an insurgency was developing suggests that confirmation biases occurred as well, with analysts interpreting new information through a lens that reinforced the initial anchoring bias.

Recommendations

The Army must recognize the importance of mitigating cognitive biases to prepare for future large-scale ground combat operations and avoid repeating the mistakes of the past. Cognitive biases are inevitable to varying degrees, but they can be managed and even prevented if deliberate steps are taken. Analysts can mitigate the biases illustrated in the case studies, for example, by employing three techniques.

- First—Routine checks of key assumptions can increase the odds of recognizing subconscious biases. Cognitive biases often manifest themselves as hidden assumptions that analysts do not even realize they are making.
- Second—Analysts should identify at least one plausible alternative and associated indicators every time a major analytic conclusion is being made. This process will ensure analysts consider all plausible possibilities, rather than settling on the first reasonable conclusion that comes to mind.
- Third—An emphasis on inclusivity can prevent groups from being dominated by a single mental paradigm of how to approach problems. In short, teaching analysts good habits can mitigate cognitive biases.

As the Army prepares for future large-scale conflicts, it will need a comprehensive approach for mitigating cognitive biases beyond these three historical examples. The case studies provide only a mere sampling of the many cognitive biases that occur routinely. The Army will need to institutionalize analytic tradecraft standards across the force to establish a common set of expectations and a culture that demands rigor in all-source analysis at all levels. Furthermore, the Army should teach structured analytic techniques that can help analysts adhere to tradecraft standards and avoid common mental pitfalls. Application of these tradecraft standards and structured techniques can be deliberate or done in an abbreviated manner, depending on the circumstances. They can also be applied at the lowest echelon. Analysts at the tactical level are arguably the most vulnerable to cognitive biases. Dr. Heuer states that cognitive biases affect accurate perception the most when analysts encounter ambiguous situations, vivid or traumatic events, and time-sensitive circumstances.[33] Army analysts at the tactical level in a future large-scale conflict are likely to encounter these conditions simultaneously.

When implementing analytic tradecraft standards, the Army should align itself with the rest of the intelligence community and the Defense Intelligence Enterprise to ensure interoperability. The nine tradecraft standards in ICD 203 represent a starting point for all-source analytic organizations in the intelligence community. The Defense Intelligence Agency (DIA), for example, has its own tailored standards nested under those in ICD 203. Most civilian analysts assigned to combatant commands are also subject to DIA standards as agency employees. The Army should ensure its analytic tradecraft standards are also nested under ICD 203 and consistent with DIA-specific tradecraft, while ensuring these standards are sufficiently tailored to the Army's mission.

Conclusion

This careful balancing of analytic tradecraft standards can be achieved through frequent working groups and annual tradecraft conferences between the military Services, combatant commands, DIA, and the rest of the intelligence community. This type of collaboration will ensure that all-source analysts throughout the intelligence community are mitigating cognitive biases and adhering to the same standards of rigor in support of Army and joint commanders.

Epigraph

Richards J. Heuer Jr., *Psychology of Intelligence Analysis* (Langley, VA: Center for the Study of Intelligence, Central Intelligence Agency, 1999), 127, https://www.ialeia.org/docs/Psychology_of_Intelligence_Analysis.pdf.

Endnotes

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

2. Heuer, *Psychology of Intelligence Analysis,* 2.

3. Ibid., 14, 116.

4. Ibid., 4.

5. "Our Values: Objectivity," Office of the Director of National Intelligence website, accessed April 27, 2020, https://www.intelligence.gov/mission/our-values/342-objectivity?fbclid=IwAR1hBf94t-3QSphCajJBWhIYvfjS1P8SvCUap9-8Be_p3V29PO3kELF2Q-4.

6. Department of the Army, Army Techniques Publication (ATP) 2-33.4, *Intelligence Analysis* (Washington, DC: U.S. GPO, 10 January 2020), xiv.

7. Department of the Army, Training and Doctrine Command (TRADOC) Regulation 25-36, *The TRADOC Doctrine Publication Program* (Washington, DC: U.S. GPO, 21 May 2014), 16.

8. Department of the Army, ATP 2-33.4, *Intelligence Analysis,* 1-8. Adapted from Figure 1-4. Analytic standards.

9. Mark Perry, *Partners in Command: George Marshall and Dwight Eisenhower in War and Peace* (New York: The Penguin Press, 2007), 339.

10. Ibid., 340.

11. Hugh M. Cole, *The Ardennes: Battle of the Bulge* (Washington, DC: U.S. Army Center for Military History, 1964), 674, https://history.army.mil/html/books/007/7-8-1/CMH_Pub_7-8-1.pdf.

12. "Battle of the Bulge," U.S. Army Center for Military History, accessed May 7, 2020, https://history.army.mil/html/reference/bulge/index.html.

13. Heuer, *Psychology of Intelligence Analysis,* 150.

14. Cole, *The Ardennes,* 57.

15. Ibid.

16. Ibid., 59.

17. Ibid.

18. Ibid.

19. Ibid., 57.

20. Ibid.

21. Anthony H. Cordesman, *The Gulf War* (Washington, DC: Center for Strategic and International Studies, 1994), 68, https://www.csis.org/programs/burke-chair-strategy/lessons-war/gulf-war; and William Rosenau, *Special Operations Forces and Elusive Enemy Ground Targets: Lessons from Vietnam and the Persian Gulf War* (Santa Monica, CA: RAND Corporation, 2001), https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1408/MR1408.ch3.pdf.

22. Michael R. Gordon and Bernard E. Trainor, *The Generals' War* (New York: Little, Brown and Company, 1995), 231.

23. Cordesman, *Gulf War,* 65.

24. Ibid.; and Rosenau, S*pecial Operations Forces,* 32.

25. Stewart Powell, "Scud War, Round Two," *Air Force Magazine,* April 1, 1992, https://www.airforcemag.com/article/0492scud/.

26. "Schwarzkopf Critiques of Intelligence," *Intelligence Successes and Failures in Operations Desert Shield/Storm, Report of the Oversight and Investigations Subcommittee of the Committee on Armed Services, House of Representatives* (Washington, DC: U.S. GPO, August 16, 1993), 30, https://apps.dtic.mil/dtic/tr/fulltext/u2/a338886.pdf.

27. Ibid.

28. Ibid., 29.

29. Joel D. Rayburn and Frank K. Sobchak, eds., *The US Army in the Iraq War: Volume 1* (Carlisle, PA: United States Army War College Press, 2019), 248, https://publications.armywarcollege.edu/pubs/3667.pdf.

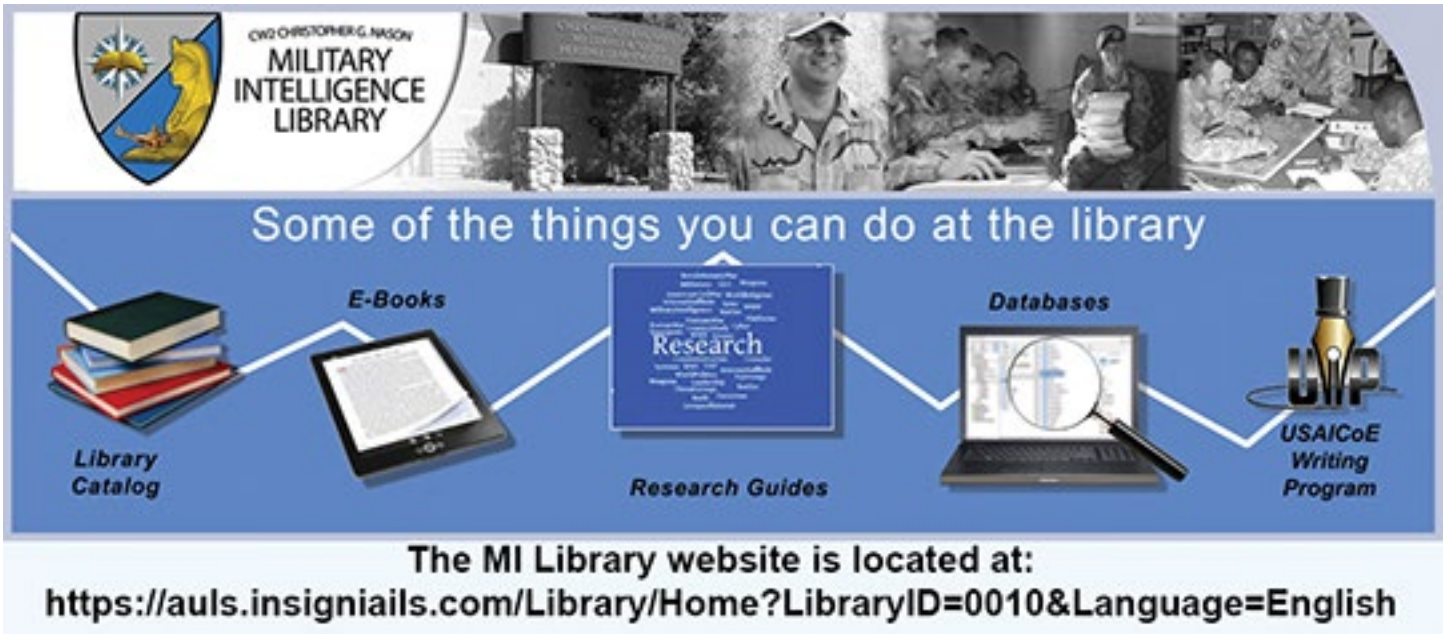
30. Ibid., 104.

31. Ibid., 179.

32. Ibid.

33. Heuer, *Psychology of Intelligence Analysis,* 14, 116.

MAJ James Kwoun is a Functional Area 34 officer currently serving as a senior analytic tradecraft instructor at the Defense Intelligence Agency (DIA). He previously served as a branch chief at DIA, supervising strategic all-source analysts. Before his service at DIA, MAJ Kwoun served in intelligence positions at the combatant command level and various assignments at the brigade level and below. His overseas tours and deployments include Iraq, Afghanistan, and the Republic of Korea.



U.S. Army photo by Joy Dulen

United States Army Soldiers from the 3rd Infantry Division line up to meet United States and Polish dignitaries during an event at Drawsko Pomorskie Training Area, Poland, in support of DEFENDER-Europe 20, March 11, 2020. The Pentagon ordered a halt to the deployment of forces and curtailed the exercise in early March over concerns about the coronavirus.

The USAREUR Intelligence Enterprise and Intelligence Support in a Pandemic Crisis

by Colonel Derrick S. Lee, Mr. James Scofield, and Lieutenant Colonel Christopher J. Heatherly

Introduction

This article outlines the experiences of an Army Service component command G-2 staff in responding to an operational environment (OE) ravaged by the nontraditional threat of a pandemic that completely shut down national borders, restricted movement, and changed the operational focus lines of effort overnight. We address a variety of challenges of the initial crisis period and share how the intelligence warfighting function overcame them while still maintaining vigilance over the OE and managing more traditional threats and intelligence activities. The authors recommend a further look into military intelligence readiness, as well as doctrine and tactics, techniques, and procedures, in meeting the analytical demands of a nontraditional OE once the pandemic crisis has ended, data is collected, and additional lessons learned are identified.

DEFENDER-Europe 20 and the Challenge of Unexpected Events

In late 2019 and early 2020, the U.S. Army Europe (USAREUR) had its focus on preparing for DEFENDER-Europe 20, the largest training event in the European theater since the end of the Cold War. DEFENDER-Europe 20

was the heir to the series of annual REFORGER (Return of Forces to Germany) exercises that ended in 1993. Planning for this exercise demanded a significant portion of the command's attention because the event involved the deployment of more than 20,000 Soldiers from the United States, the movement of 9,000 USAREUR-assigned troops, and the contribution of 8,000 allied and partner forces from 18 nations—all conducting carefully orchestrated mobility operations and training across the theater. The USAREUR intelligence enterprise itself was consumed by the intelligence, surveillance, and reconnaissance (ISR) preparations for DEFENDER-Europe 20. These included conducting an ISR rehearsal of concept drill and executing initial ISR operations such as aerial collection. It also involved planning and coordinating multiple signals intelligence (SIGINT), geospatial intelligence, open-source intelligence (OSINT), human intelligence (HUMINT), and counterintelligence (CI) operations—both exercise and real-world threat support.

Going into 2020, intelligence professionals from the USAREUR G-2, 66th Military Intelligence Brigade, and the collective enterprise, including intelligence agencies and analysts from several European and North Atlantic Treaty Organization (NATO) partner nations, were maintaining focus on several areas, including—

- Collection and analytical efforts against the principal theater threat.
- Frozen conflicts in Ukraine, Georgia, Moldova, and the Balkans.
- Instability in Lebanon.
- Conflict in Syria and Libya.
- Simmering tensions in the Levant.
- The ever-present specter of terrorism.

Then on 3 January, the strike against and killing of Qasem Soleimani, commander of the Quds Force, part of Iran's Islamic Revolutionary Guard Corps, provided a new challenge that was to consume the USAREUR intelligence enterprise's attention.[1] The USAREUR G-2, in conjunction with U.S. Central Command and U.S. European Command (EUCOM), went into a full surge. It marked an abrupt end to the Christmas holiday period as the headquarters moved into a full, 24/7 battle rhythm effort to track and assess a likely response from Iran while continuing to focus on the Iranian-associated terrorist network and personnel in the European theater that posed a threat to United States forces.

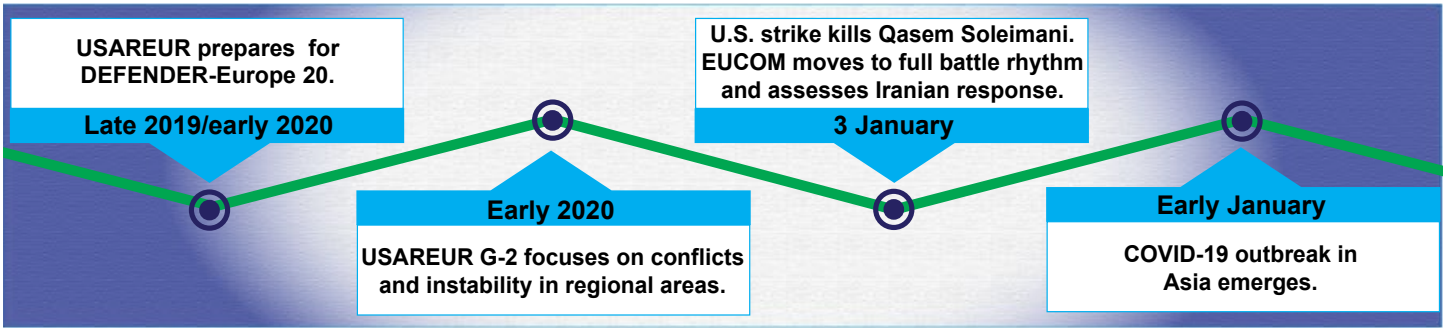
To further compound the challenges, far away in Asia, the nascent coronavirus disease 2019 (COVID-19) outbreak emerged as a concern when early estimates from medical experts and agencies warned of the potential global impacts from the spread of the disease. When the virus emerged in the European theater in late February, the USAREUR command and its intelligence enterprise had to pivot yet again, this time against a nontraditional threat in the form of a pandemic, unsure of how the OE would unfold in the face of an unprecedented global event.

Initial Detection and Evolution of an Unprecedented Threat

USAREUR's attention to the potential threat of the virus grew throughout February 2020 as COVID-19 made its first identified appearances in Europe on 24 January: two in Paris and one in Bordeaux, France.[2] At first, individual European governments were somewhat oblivious to the severity and velocity of the threat, and their reactions were slow and unsynchronized. Over the next several weeks, however, European nations began implementing a series of border closures and restriction of movements as COVID-19 quickly spread and new clusters of infection appeared in various locations: Munich, Germany (27 January), Rome, Italy (31 January), the Canary Islands, Spain (1 February), and Northern Italy in late February.[3] The virus eventually reached USAREUR when the first USAREUR member tested positive on 12 March.[4] By then, Office of the Secretary of Defense and Headquarters, Department of the Army (HQDA) had largely curtailed DEFENDER-Europe 20 and stopped the flow of U.S. Army personnel and equipment into Europe.

The Command Pivots

By early March, USAREUR Headquarters, in Wiesbaden, Germany, was beginning its effort to understand and



confront the growing pandemic. The command's reaction was informed by the initial actions, lessons learned, and best practices at U.S. Army Africa Headquarters in Northern Italy where the COVID-19 outbreak had first rapidly spread in the European continent.

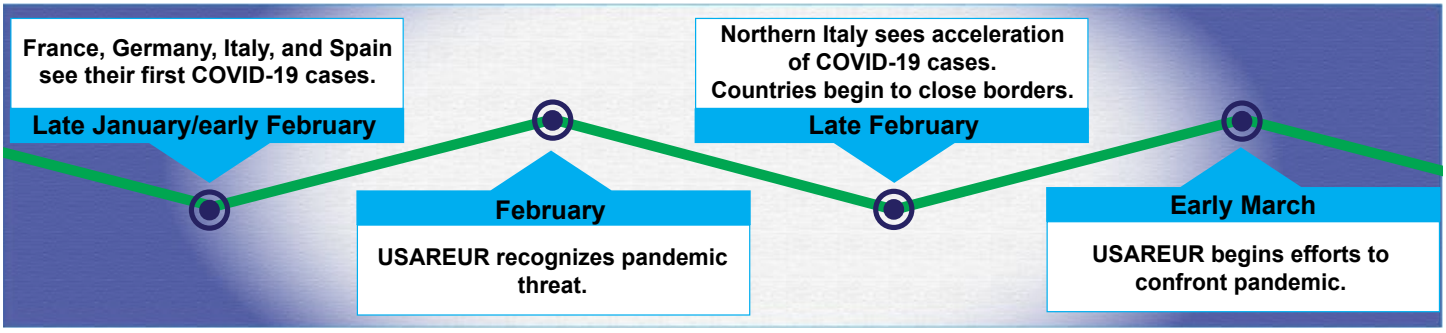
By 7 March, based on the virus's initial spread throughout Western Europe, the cancellation or downsizing of the strategically important DEFENDER-Europe 20 was a real risk. The USAREUR G-2 began to extrapolate the COVID-19 threat to the rest of the theater, based on trends that United States Army forces in Italy and South Korea had observed. The goal was to project the spreading pattern of the virus that could necessitate the command's and HQDA's decision to scale back or cancel DEFENDER-Europe 20. The USAREUR G-2 analysis and control element (ACE) began to develop a model to project the spread of the virus in Germany, Poland, the Netherlands, and Belgium (i.e., key reception, staging, onward movement, and integration nodes and port locations) in order to inform the command on likely OE conditions with regard to the COVID-19 infections. The USAREUR G-2 also commenced assessments of potential impacts, which it shared with the EUCOM J-2 and HQDA G-2, and developed contingency plans to turn off inbound ISR deployments.

U.S. Air Force photo by SSgt. Devin Nothstine

Airmen prepare to off-load COVID-19 patients during the first operational use of the Transport Isolation System (TIS) at Ramstein Air Base, Germany, April 10, 2020. The TIS is an infectious disease containment unit designed to minimize contamination risk to aircrew and medical attendants, while allowing in-flight medical care for patients afflicted by a disease—in this case, COVID-19.

By 10 March, the command battle rhythm transitioned to crisis battle rhythm and commenced daily commander's update briefs, up from one per week. Additionally, a daily operations and intelligence update was instituted to track the rapidly changing OE, both in Europe and in other key strategic locations throughout the globe. The update was provided to the commanding general, major subordinate command commanders, senior responsible officers, Director of the U.S. Army Installation Management Command–Europe, U.S. Army garrison commanders, and key USAREUR staff.

On 11 March, as the virus spread across Europe, EUCOM issued a press release announcing a scaling back of the scope of DEFENDER-Europe 20;[5] by 14 March, USAREUR Headquarters adopted significant movement and activity restrictions, mandated protection measures against the virus, and commenced shift and telework operations. Based on the developed contingency plans, the G-2 immediately acted to halt and reverse DEFENDER-Europe 20 ISR deployments and activities, cancelled all engagements with foreign partners—many at the host nations' request—and rebalanced standing analysis and production requirements against the rapidly growing need to address the new, nontraditional threat posed by COVID-19. USAREUR released a tasking order directing the G-2 to reorient its analytical capability in coordination with the USAREUR Office of the Surgeon, the EUCOM J-2 and Surgeon, and national-level



intelligence agencies, including the National Center for Medical Intelligence. The G-2, including the assigned 66th Military Intelligence Brigade ACE and 60th Engineer Detachment/Geospatial Planning Cell (60th GPC), began to reorganize and reorient its personnel. The tasking order also directed the G-2 to monitor the Defense Intelligence Agency's pandemic watch condition.

The G-33, Current Operations, initially led the staff hand-in-hand with the command surgeon (Office of the Surgeon), with direct support to the garrisons, in understanding and responding to COVID-19. The USAREUR Office of the Surgeon and G-2 played key roles on the assessment side of this effort by providing both expert knowledge and analytical capabilities. Progress in understanding and analyzing the pandemic was initially slow because of a lack of information about the virus and analysts' unfamiliarity with a pandemic threat. Yet the USAREUR intelligence enterprise undertook the mission with a positive, can-do attitude, driven by the need to adapt to the new, unique challenge.

The Intelligence Enterprise Challenge

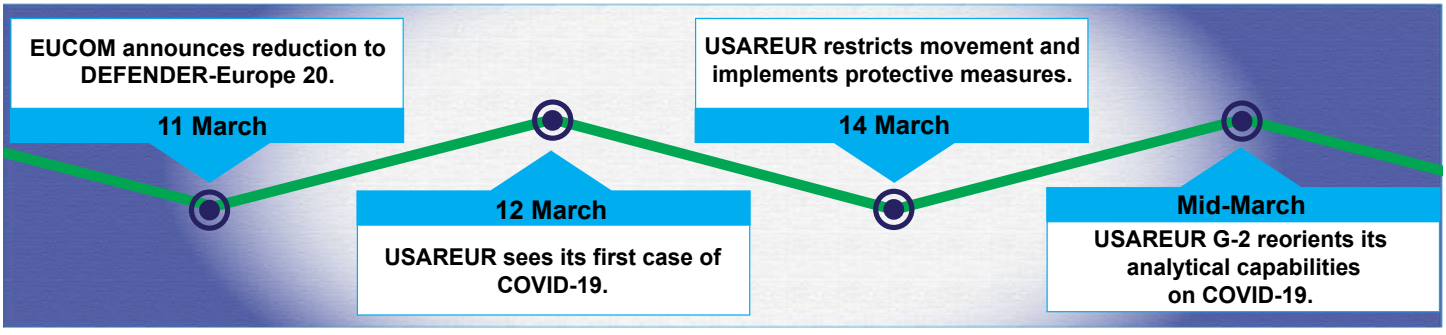
Initially, to drive the intelligence effort, the USAREUR Commanding General provided guidance to the G-2 to focus on—

- Indications of adversaries and near-peer threat opportunism in Europe to destabilize or threaten U.S. and NATO interests.
- Threat situations in other strategic locations (such as the Pacific and the Middle East) that could affect the Euro-Atlantic Alliance.
- Indications of non-state actors and violent extremist organizations attempting to exploit the environment to target U.S. personnel and interests in the USAREUR footprint.

This overarching guidance became the framework by which the USAREUR intelligence enterprise gathered, collected, coordinated, and synchronized intelligence to shape operations and intelligence and the commander's update brief products, as well as recurring intelligence assessments and summaries. The intelligence enterprise effort, based on this guidance and direction, would support USAREUR's two equally vital goals: to sustain wartime readiness by protecting Soldiers, personnel, and families from COVID-19; and to continue to maintain readiness and the operational posture.

A Two-Pronged Analytical Effort. As the pandemic unfolded and the command mobilized to respond, the G-2 shifted to a two-pronged analytical effort. The first was monitoring the "traditional" threat as outlined through the Commanding General's guidance. The second was monitoring the "non-traditional" threat, understanding the rapidly changing OE, especially the rate at which COVID-19 was spreading, and providing requisite analytical support to help mitigate the spread within the USAREUR garrison footprint. The G-2 team quickly conducted mission analysis with the rest of the USAREUR staff and began collecting information to provide the common intelligence picture related to the OE as shaped by the spread of the virus. In gathering the information to build a common OE picture, they considered several questions:

- What type of data did they need? Given the numerous sources of information related to COVID-19, which ones should they use? Possible options were U.S. medical research universities, worldwide pandemic trackers, U.S. Government health agencies, and various European nations' health agencies.
- How could they get data in an automated fashion to preclude manual-intensive data input?
- Who/what were the authorities, in particular with regard to intelligence oversight constraints, because tracking the virus's spread among U.S. installations and personnel involved accessing U.S. person information.
- What were the best manner and frequency to disseminate products to the command group and staff? Were visual products, such as a common intelligence picture/common operational picture, or text-based intelligence summaries more effective?
- How should they disseminate in order to standardize reporting and eliminate duplicative or conflicting reporting between different echelons and commands?



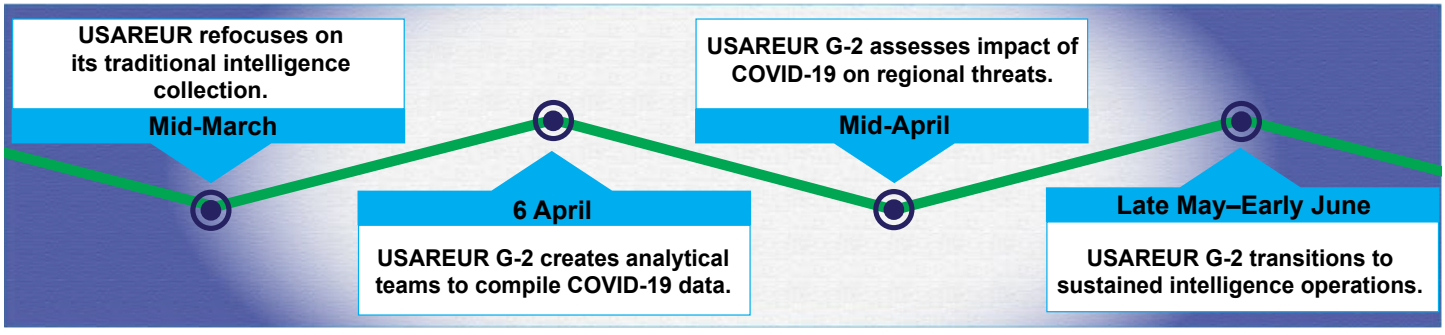
The G-2 was tracking new COVID-19 information streams and data for the European nations in order to understand the spread rate and its potential effect on U.S. installations in the region. We required this information to determine measures that each garrison and senior responsible officer would need to take to protect the U.S. population on those installations. However, we had to take care to avoid exceeding intelligence oversight authorities and to avoid the perception of "friends collecting on friends" as we considered allied or partner data. There was considerable discussion on synchronizing COVID-19 activities and information within the intelligence, operations, protection, and plans divisions and Office of the Surgeon because they all held a piece of the larger picture. Initial information requests focused primarily on COVID-19 statistics for individual nations, such as the number of people infected, the number of deaths, and the number of patients who had recovered from the virus, as well as the continued spread of the virus across Europe.

U.S. Army photo by CPT Ellen C. Brabo

These United States Army Soldiers were the first to arrive in Germany for exercise DEFENDER-Europe 20, which was intended to test the Army's ability to deploy a division-sized, combat-credible force from the United States to Europe.

Creation of Two Analytical Teams. On 6 April, the G-2 created two separate but complementary analytical teams dedicated to compiling COVID-19 data for all of Europe. One team worked on securing information to track spread rates and examine activities and restrictions. The other team's focus was on pattern and link analysis in order to identify potential patterns of spread among the U.S. population in the garrisons.

The first team worked to secure host nation and other unclassified information in order to develop 3-, 7-, and 14-day rolling averages and spread rates for host nation regions and to provide broader national assessments for multiple countries in theater. Then the team used that information to feed a COVID-19 common operational picture. Analysts in this team met with the USAREUR Office of the Surgeon and the medical command G-3 to gain a greater understanding of the pandemic as they examined political activities, social restrictions, and other related events. The team, which consisted of military personnel, Army civilians, and contract analysts encompassing all intelligence disciplines, made extensive use of data sets, including R-naught numbers (i.e., calculations to determine the average "spreadability" of an infectious disease) and infection rates per 100,000 individuals. The team also considered COVID-19 numbers for overall cases, new cases, new deaths, total deaths, newly recovered, total recovered, and infection doubling time. The team pulled information from various sources, including host nation authoritative data provisioned by each country's health ministries (when available), or data being tracked by country teams in each of the key nations. The team provided its analysis to NATO, U.S. Africa Command, the USAREUR staff, subordinate units, and garrison headquarters at the country, region, and state level. The team also worked in partnership with other U.S. European–based commands to develop a consistent



information flow to HQDA in Washington, DC. As of this writing, they continue collaboration with the 60th GPC, U.S. Army Intelligence and Security Command (INSCOM), HQDA G-2, USAREUR Office of the Surgeon, and other commands to develop a COVID-19 predictive modeling chart.

The second team was the COVID-19 network analytical cell with responsibility for providing direct support to the G-34 (Protection) in partnership with the Office of the Surgeon and the Landstuhl Regional Health Command. The team focused on pattern and link analysis in an effort to complement contact tracing and identify potential patterns of spread within U.S. populations in garrison locations. The team devised a plan to detach the COVID-19 network analytical cell personnel from intelligence authorities and to subordinate them directly under the G-34's purview because of the sensitivity of working with U.S. person information. To create the plan, the USAREUR G-2 collaborated with the USAREUR G-3, HQDA G-2, and INSCOM intelligence oversight officers and staff judge advocate. This team brought skills to the G-34 team; however, it was not tied to the G-2 intelligence structure, nor did it use intelligence systems to conduct and provide its analysis. This ensured compliance with intelligence oversight guidelines. The COVID-19 network analytical cell primarily supported the U.S. Army garrisons in southern Germany. It also assisted the USAREUR-designated senior responsible officers across Europe. The cell identified key trends and patterns that allowed effective preventive measures for the command and garrisons.

Assessing Regional Adversaries and Threats. COVID-19 infection rates increased, and the virus spread to Eastern Europe, the Middle East, and the rest of Asia. In mid-April, USAREUR undertook a subsequent analytical effort to begin assessing the impact of COVID-19 on some of the near-peer adversaries and other regional threats at national and economic levels, as well as their general military readiness. (Armed forces of various adversary and threat nations were continuing with training activities, readiness drills, and exercises, necessitating greater vigilance on our part.) Of particular importance to the command were adversary and threat nations' disinformation, misinformation, and influence campaigns that sought to exploit the COVID-19 situation in various parts of Europe, directed against U.S. and NATO equities and interests.

Before the pandemic, the USAREUR intelligence enterprise had made extensive use of OSINT in its daily work. Once re-tasked against the pandemic, the G-2 ACE found the best and most timely pandemic information from previously unfamiliar and unused sources. Analysts found particular value from various European Union nations' health department pandemic updates, as well as information reported by select European news organizations, European and U.S. health institutes, and several websites providing real-time statistics and updates on the ongoing pandemic. Host nation data proved to be the most reliable and timely, although not always packaged or visualized as well as some of the consolidated data websites.

Given the adversary's proclivity for disinformation operations that attempted to exploit the pandemic situation to bolster their information and influence operations, intelligence professionals routinely scrutinized OSINT in the course of their work. Moscow and Beijing, in particular, made extensive use of disinformation to downplay U.S., European Union, and NATO response efforts, redirect "blame" for the virus, and obscure the impact of the virus among their own citizenry. The OSINT effort became the indications and warning in the information domain, picking out adversary disinformation and misinformation efforts to better posture the command's strategic messaging and communications effort to counter these attempts by Moscow and Beijing.

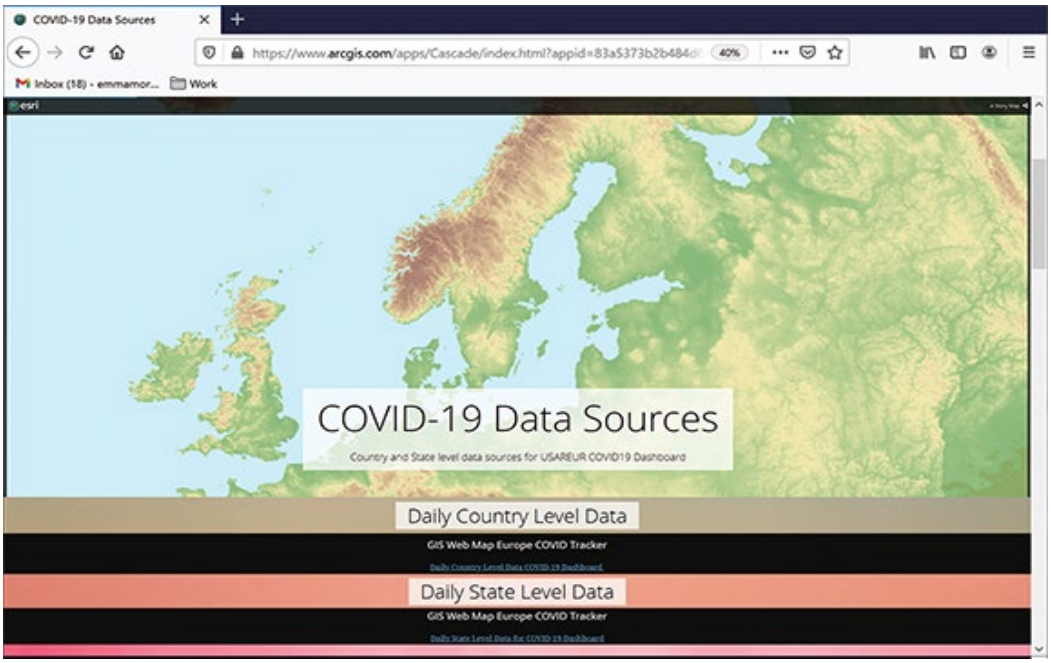
Working with In-Country Teams. Beyond web-based OSINT, there was another vital source of information on allied nation infections, management, and medical capabilities throughout the crisis—U.S. country teams and USAREUR

U.S. Army photo by Jason Johnston

An Army major tests COVID-19 samples at Drawsko Pomorskie Training Area, Poland, July 15, 2020, during Phase II of DEFENDER-Europe 20, an exercise used to build strategic readiness in support of the United States National Defense Strategy and NATO deterrence objectives.

military coordination offices working with host nation personnel across Europe. Their daily contact with local government and military and civilian leadership provided unfiltered information vital to the G-2's analysis. The early decision to maximize the use of unclassified communication systems eased the information flow with allies and partners as well as U.S. country teams. The G-2 used a variety of digital communication platforms, including secure video teleconferences, email, and teleconferences, as a means to uphold engagement commitments with vital partners in lieu of in-person meetings and to preserve operations security.

Dashboards and Real-Time Views. The G-2 identified a new requirement to display COVID-19 information within USAREUR's area of responsibility, allowing the command team to visualize the situation. In order to meet the requirement to generate the common intelligence picture, the 60th GPC repurposed Esri's ArcGIS dashboard using a borrowed infrastructure from the Army Geospatial Center. After identifying country-specific authoritative COVID-19 databases, the 60th GPC populated the ArcGIS dashboard with new cases, total cases, deaths, and recovery statistics. This dashboard used ArcGIS's configurable web applications to provide location-aware data visualization and analytics for a real-time view of hot spots to track the spread of the virus down to the state/region level on one map. This interface became interactive when the 60th GPC used the data to populate charts, graphs, lists, indicators, layers, and maps for user-specific requirements. The 60th GPC also worked with other staff sections to include 3- and 7-day rolling averages of newly reported cases for analytical purposes. As the dashboard became a "one-stop-shop" for the command and staff, the 60th GPC included a story map displaying virus-related health facts like symptoms and proper hygienic care. This added to the overall concept, and the dashboard effectively became the USAREUR common operational picture for COVID-19.



Screen capture courtesy of Esri

The homepage and data entry point for the U.S. Army Europe COVID-19 Dashboard created by repurposing Esri's ArcGIS platform.

Transition to Sustained Intelligence Operations in a COVID-19 Environment

As the COVID-19 threat situation across Europe improved in late May and early June, the G-2 settled into a more routine COVID-19 battle rhythm and rebalanced efforts against other theater priorities. The status of the OE became essential for risk assessment decisions associated with Department of Defense policies governing personnel movement. Visualized COVID-19 trends and forward-looking assessments facilitated exception-to-policy and conditions-based decisions on emergency leave, deployments, temporary duty, training, and permanent change of station moves.

While the USAREUR intelligence enterprise made a tremendous investment in tackling the COVID-19 pandemic, it could not surrender its traditional mission of conducting collection operations, implementing and following through on initiatives to enhance theater collection capabilities, monitoring theater threats, and conducting partner engagement activities (when possible, in person or virtually) to enhance intelligence interoperability and combined collection capabilities. The USAREUR G-2 staff continued the planning, coordination, and execution of theater ISR activities and scaled-back support to DEFENDER-Europe 20, in coordination with the EUCOM J-2, HQDA G-2, and INSCOM.

From mid-March to the present, great strides have been made regarding the Guardrail Common Sensor aerial SIGINT collection and cross-cue collection operation with United States Air Forces in Europe, United States Naval Forces Europe, and United Kingdom collection assets; coordination and implementation of additional terrestrial collection capability in the Baltics and Poland; and implementation of bilateral HUMINT and CI collection operations throughout

the theater. In particular, efforts by USAREUR G-2X analysts, who were teleworking on unclassified systems and coordinating with other CI analytic elements in the USAREUR intelligence enterprise, conducted an analytical review of an Iran-associated threat network in Europe. Sharing this review with host nations paid great dividends in terms of neutralizing some of the financing networks in Germany.

Army Service Component Command G-2 Lessons Learned

With the COVID-19 crisis still unfolding, it may be premature to assess the alignment of doctrinal roles and responsibilities with the reality of a pandemic or to determine lessons from the conduct of response to the crisis. However, some initial observations and possible shortfalls are worth highlighting.

USAREUR's mission objectives were to protect the military community from the pandemic and ensure sustained Army operational readiness across the theater. For the USAREUR G-2, the crisis provided an opportunity to align tasks and organizational structure to prevent a duplication of effort, ensure compliance with regulation and policies (most importantly, intelligence oversight), and prioritize limited collection platforms and analytical capacity to meet the requirements.

Much of the expertise for understanding the virus threat lay in the Army medical community. The intelligence enterprise complemented the medical community with its analytical expertise and structured, collaborated method to collect data, forecast health threats to theater garrisons, and support medical and force protection operations. At the outset of the pandemic, virus-related data and metrics were not readily available from theater or national sources. Theater intelligence professionals demonstrated initiative and resourcefulness in uncovering valuable sources of data and health/medical knowledge at an unclassified level from host nations, nongovernmental organizations, and academic organizations. Analysts sought to collaborate with the Office of the Surgeon to understand disease characteristics, models, and tracking and forecast tools, but the operational response requirements levied against the Office of the Surgeon limited support to broader analytical efforts pursued by G-2.

As the crisis unfolded, it became increasingly apparent that many commands and theater organizations were doing similar work to understand and track the COVID-19 threat. In retrospect, we can see this was a duplication of effort as the G-2 team worked to ensure data assessments, processes, and visualizations provided timely, accurate, and standardized products. This further highlights the need for top-down driven data standards and processes, especially in support of a complex yet open, data-rich environment. Such a structured method for conducting analysis and disseminating and sharing information between echelons and commands is necessary to preclude duplication of effort.

Understanding and adhering to established operational authorities represents another difficult challenge for intelligence professionals to identify early and present to the command for decision. The theater enterprise worked within the scope of intelligence oversight regulations when assessing potential theater threats to U.S. garrisons and facilities. There are ways to get to a "yes," provided that the right staff sections, subject matter experts, and leadership come together to devise a solution within the limitations of regulations and policies.

Commanders and military intelligence professionals must also maintain a broad vision of the comprehensive threat picture and various requirements related to the assessment of the OE. Clear guidance from the USAREUR Commanding General provided the framework in which the intelligence enterprise was able to execute intelligence operations and analysis along multiple lines of effort. The G-2 could not place its entire effort against COVID-19 analysis at the expense of overlooking other threat streams, for example, major adversaries and terrorism, because the drastic change in the OE required constant vigilance against the various threats. In this crisis, the G-2 allocated additional personnel to supporting current operations in the command center while at the same time standing up four COVID-19–specific teams (including the two teams described earlier):

- Current threat analysis team centered in the ACE.
- Longer-term trend team centered on the G-2's operations and plans division.
- Training team to provide expertise to the G-34's COVID-19 contact tracing efforts.
- Analysis and inspection team to support the decision-making and control activities that the garrison and senior responsible officers were making with regard to COVID-19.

Conclusion

Providing routine, predictive analysis in an OE defined by a viral pandemic presented unique challenges. The USAREUR intelligence enterprise—its highly trained Soldiers and civilians—demonstrated tremendous flexibility, initiative, resourcefulness, energy, and a positive attitude in tackling this mission that extended beyond the traditional responsibilities and training. By early May, through the careful

alignment of priorities with theater intelligence resources and coordination between various echelons and commands, the G-2 was able to provide comprehensive intelligence support to the command.

Endnotes

1. Wikipedia, s.v. "Assassination of Qasem Soleimani," last modified on 30 January 2021, 13:43, https://en.wikipedia.org/wiki/Assassination_of_Qasem_Soleimani.

2. "First cases of coronavirus disease 2019 (COVID-19) in France: surveillance, investigations and control measures, January 2020," *Eurosurveillance* 25, no. 6 (13 February 2020): 20–26, https://www.eurosurveillance.org/content/10.2807/1560-7917.ES.2020.25.6.2000094.

3. Wikipedia, s.v. "COVID-19 pandemic in Germany," last modified on 3 February 2021, 07:38, https://en.wikipedia.org/wiki/COVID-19_pandemic_in_Germany; Wikipedia, s.v. "COVID-19 pandemic in Italy," last modified on 3 February 2021, 17:24, https://en.wikipedia.org/wiki/COVID-19_pandemic_in_Italy; and Wikipedia, s.v. "COVID-19 pandemic in Spain," last modified on 1 February 2021, 08:34, https://en.wikipedia.org/wiki/COVID-19_pandemic_in_Spain.

4. Tammy Servies, "Characteristics of U.S. Army Beneficiary Cases of COVID-19 in Europe, 12 March 2020–17 April 2020," Health.mil, December 1, 2020, https://health.mil/News/Articles/2020/12/01/US-Army-Beneficiary-MSMR-2020.

5. "Exercise DEFENDER-Europe 20 Announcement - COVID-19 implications," Supreme Headquarters Allied Powers Europe website, March 17, 2020, https://shape.nato.int/defender-europe/defender/newsroom/exercise-defendereurope-20-announcement-covid19-implications.

COL Derrick Lee commissioned into military intelligence (MI) in 1993 after graduating from the U.S. Military Academy. His recent assignments include G-2, North Atlantic Treaty Organization Allied Land Command; G-2, U.S. Army Europe; Commander, 501st MI Brigade; and G-2, 101st Airborne Division (Air Assault). He holds a bachelor's degree in economics from the U.S. Military Academy and a master's degree in management and strategic studies from the University of Maryland University College. Additionally, he completed the Senior Service College Fellowship at Harvard Kennedy School.

Mr. James Scofield has over 35 years of service with U.S. Army intelligence. He has served in Washington DC, Europe, and Hawaii, to include assignments at U.S. Army Pacific G-2, U.S. Army Europe G-2, and U.S. European Command J-2. His current assignment is as senior advisor, U.S. Army National Ground Intelligence Center. Jim is a graduate of the University of Hawaii and holds master's degrees from the University of Virginia and the National War College.

LTC Christopher Heatherly enlisted in the U.S. Army in 1994 and earned his commission through Officer Candidate School in 1997. He has held a variety of assignments in special operations, Special Forces, 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.

New J2X Training Opportunity

by Mr. David C. Summers

Introducing a New Distance Learning Course

A new training opportunity is available at the Human Intelligence Training–Joint Center of Excellence (HT–JCOE), which will be conducted on the SECRET Internet Protocol Router Network (SIPRNET) Blackboard Learning Management System. Because of the coronavirus disease 2019 pandemic, the Defense Intelligence Agency and the U.S. Army Training and Doctrine Command asked training institutions to examine alternative delivery methods that make training more accessible to the Defense Counterintelligence and Human Intelligence Enterprises. For military and civilian personnel who will serve in combatant command, sub-unified command, or Joint Task Force J2X staff positions, training is available via the J2X Staff Officer Course Distance Learning (DL), which will be conducted in lieu of the former resident J2X Course.

The J2X Staff Officer Course (DL) is a robust instructor-mediated, collaborative course that covers the same content as the previous resident course and ensures the same educational outcomes. The first pilot course occurred from 4 January to 2 March 2021 with 16 joint Service military and civilian graduates. The length of the course is 40 training days, or 8 weeks.

The Training Method

In general, distance learning courses are more rigorous than their resident counterparts. The J2X Staff Officer Course (DL) uses problem-solving as its method of instruction. The students will not only be responsible for individually completing assignments (solving problems), quizzes, and summative assessments, but also for collaborating with their classmates, participating in discussion forums, and completing the Capstone exercise.

Students will require SIPRNET access an average of 20 to 25 hours per week for the duration of the course. For the non-collaborative portion of the course, students can proceed at their own pace, meeting the minimum deadlines for each assignment, quiz, and assessment. For the collaborative portion of the course, they must adhere to timelines (schedule) for practical exercises and discussions.

Some individuals have asked why the distance learning version of the course (or any course) is longer than the previous resident version, considering that both versions cover the same critical tasks, have the same content, and assess the students to the same level of proficiency. In order to deliver distance learning via the most beneficial means, HT–JCOE allotted a total time of 40 training days, with the expectation that students will spend between 20 and 25 hours per week on the course. All input must be in written form, including the collaborative discussions, and therefore may require additional time from some students.

This training method has three additional challenges:

- First, students are "sent away" for training so that they are removed from their daily work environment, allowing them to concentrate on the task at hand. Allotting 40 training days for the completion of all course requirements takes into account the competing requirements at home station. HT–JCOE experienced this issue when it sent out mobile training teams to conduct training, during which students were often "pulled" out of class but still expected to receive a certificate of completion. However, we believe it to be a realistic expectation that students will be able to devote between 20 and 25 hours per week to the course.
- Second, the time zone differences are a challenge, within and outside the continental United States. Getting everyone together at the same time is not realistic.
- Third, the communication challenges to this synchronous learning method could be insurmountable because every organization and Service has different capabilities and regulations.

To view the current HT–JCOE course catalog, go to Intelligence Knowledge Network (IKN) on SIPRNET at https://ikn.army.smil.mil/, click on the TAAP icon, and then click on HTJCOE Information.

Mr. David Summers is the Director of the J2X Staff Officer Course Distance Learning at the Human Intelligence Training–Joint Center of Excellence (HT–JCOE), Fort Huachuca, AZ. He has served as an Army civilian for 12 years, working initially as a doctrine writer at the U.S. Army Intelligence Center of Excellence and later as an instructor at HT–JCOE. Mr. Summers retired after a 26-year career as a U.S. Army military intelligence officer. From 2003 to 2004, he served as the CJ2X, Combined Joint Task Force 7 in Iraq.

Fifth Wave Terrorism:

Threats, Implications, and Risk Management for U.S. Forces

by Captain Matthew A. Hughes

Editor's Note: ***The U.S. Department of Defense is a partner organization in an integrated, whole-of-government approach to international counterterrorism. The U.S. State Department is the lead organization for this effort. Other U.S. national security partners include the Departments of Homeland Security, Justice, and Treasury, and the intelligence community.***

Introduction

Terrorism has ripped through society's fabric, causing violent disturbances throughout the past 150 years. During this period, four distinct waves of terrorism have eroded democratic foundations and toppled governments. Such was the objective of 28-year-old Leon Czolgosz in September 1901. The young anarchist Czolgosz stood in a line at the Temple of Music in Buffalo, New York, waiting to come face-to-face with President William McKinley. He gripped a .38-caliber revolver in his left hand, hidden beneath a white handkerchief, drawing no attention because sweat towels were frequent among attendees of the Pan-American Exposition on that hot day. When Czolgosz finally reached the front of the line and the President extended his hand to greet him, Czolgosz fired two rounds into the President's abdomen from point-blank range. The infected wound killed McKinley within days. As Theodore Roosevelt assumed the mantle of the presidency, he denounced anarchy and demanded immediate legislation, initiating "America's original war on terror."[1] More than a century and four waves of terrorism later, society now faces a fifth wave that, much like the first four, will propagate across the globe, carrying violence and destruction.

The Next Wave

Terrorists like Czolgosz have threatened U.S. forces at various echelons for over a century, targeting individual constituents ranging from new recruits to the commander in

Photo of wash drawing by T. Dart Walker (1869-1914). Image courtesy of the Library of Congress.

Assassination of William McKinley. Czolgosz shoots President McKinley with a concealed revolver, at Pan-American Exposition reception, September 6, 1901.

chief. Despite efforts to extinguish such threats, terrorism continues to be a chief concern for U.S. forces, prompting military responses both domestic and abroad, institutional changes, and at times, a paradigm shift in strategies and conflict as a whole. As a concept or idea, terrorism is a formidable adversary because of its ever-evolving nature and dynamic factors, including ideologies, objectives, and tactics. Extensive analysis of terrorism has produced models to understand and conceptualize characteristics, feeding strategies to counter ideologies and predictive analysis to plan against future threats. Political scientist David Rapoport developed one such model, dividing the past 150 years of terrorism among four distinct waves based on characteristics that defined each wave. In this model, Rapoport outlines terrorists' predominant ideologies, objectives, targets, and tactics, as well as conditions that influenced the emergence or decline of prevalent ideologies.

Wave	Catalyst	Goals	Targets	Tactics	Reasons for Decline
Anarchist (1870s-1910s)	• Slow political reform • Declining legitimacies of monarchies	• Instigate revolution • Eliminate government oppression	Heads of state	• Assinations using dynamite • Bank robberies	• Agressive state opposition • Beginning of World War I
Nationalist (1920s-1960s)	• Versailles Peace Treaty • Increased desire for self-determination	• Eliminate colonial rule • Create new states	Police and military	Guerrilla style hit-and-run attacks	• Achieved goals • Colonial rulers withdrew from territories
New Left (1960s-1980s)	• Vietnam War • Cold War tensions	Eliminate the captialist system	• Governments • Increased focus on United States	• Hijackings • Kidnappings • Assinations	End of Cold War
Religious (1979-2020s) (predicted)	• Iranian Revolution • New Islamic century • Soviet invasion of Afghanistan	Create a global Islamic Caliphate	• United States • Israel • Europe • Mass transportation systems • Public venues	• Suicide bombings • Aircraft and vehicles as weapons	Unknown

Table 1. Defining Characteristics of David Rapoport's "Four Waves of Modern Terrorism"[2]

Based on previous waves spanning around 40 years, Rapoport believes a *fifth wave* may begin around 2025, but he also acknowledges challenges in forecasting the next wave's characteristics and timeline because it may erupt unexpectedly in response to some political issue.[3] Various terrorism studies experts and others have conjectured about the predominant ideologies or characteristics of a fifth wave emerging in the 2020s, often focusing on cultural or technological factors. As predominant global terrorism trends transition from religious ideologies to a Fifth Wave of Modern Terrorism in the 2020s, U.S. forces will encounter emerging terrorism threats possibly characterized by one or more of the following:

- New Tribalism.
- Jihadist groups.
- Technology.
- Anti-globalization.

New Tribalism Wave Characteristics and Implications

In the post-Cold War era, culture has overshadowed ideological, political, or economic distinctions as the most important factor behind wars and conflict.[4] Professor Jeffrey Kaplan's assertion that an emerging fifth wave will be characterized by mass violence associated with ethnic, racial, or tribal mysticism nests with this observation of culture driving modern conflict.[5] Under New Tribalism, terrorists pursue a utopian vision to build a perfect society in their regions during their lifetime.[6] Genocide and rape provide the means to bring this goal to fruition and transform society within one generation.[7] Children are the vanguard of New Tribalism: adherents kidnap young men to serve as soldiers and young women to serve as child brides.[8] Kaplan hypothesizes that the Khmer Rouge of Cambodia will initiate this fifth wave and that the Lord's Resistance Army in Uganda will be the wave's paradigmatic standard.[9]

A fifth wave characterized by New Tribalism would likely involve U.S. special operations forces intervening in New Tribalist conflicts or regionally aligned forces engaged in security cooperation efforts with neighboring countries of those conflicts, as well as in competition below levels of armed conflict or containment. U.S. forces would also develop contingency operations for likely hotspots. The prospect of localized conflicts and genocide in areas with weak governance would prompt consideration for armed intervention, by the United States, neighboring states, multinational coalitions, or United Nations peacekeeping forces. U.S. intervention could lead to small wars with heavy financial costs and a risk of troop loss. Kinetic actions have inherent risks of collateral deaths of children because of the New Tribalism adherent group techniques involving children, carrying risks of domestic and

Leahy Vetting

Protection of human rights is an essential American value—one enshrined in the Constitution and increasingly extended in foreign policy. One way Congress has extended this value to foreign policy is through the "Leahy laws" (named for their author, Sen. Patrick Leahy, D-Vt.). These laws prohibit the U.S. government from providing assistance or training to members of a unit of any nation's security forces that has perpetuated a gross violation of human rights with impunity. The process by which individuals are examined for possible human rights violations is referred to as *Leahy vetting.*[10]

international moral criticism. As these movements are likely to erupt in areas of weak governance rife with corruption, Leahy vetting would probably identify several military units and leaders among host or neighboring nations' armed forces that committed human rights violations in the recent past, limiting potential for security cooperation activities.

Jihadist Groups Wave Characteristics and Implications

Dr. Anthony Celso, Associate Professor at Angelo State University, proposed a fifth wave dominated by Jihadist groups in which notions against apostate Muslims and non-Muslims provoke attacks. A central end state involving isolation from society distinguishes Jihadist groups like Boko Haram and the Islamic State from other religiously motivated terrorist groups dominating the fourth wave of modern terrorism.[11] Jihadist groups, largely motivated by *jahiliyyah* to reject manmade governments' and institutions' dominion over man, seek to replace modern governments with a new Caliphate based on practices instituted in the times of the Prophet Muhammad. Tactics in this wave would likely include unrestrained violence targeting ethnic groups and communities of other religious denominations, as well as attacks against Muslims perceived to be corrupt or deemed apostates for their acceptance or tolerance of worldly institutions. Jihadist terrorist groups may inflict severe damage to communities and wage brutal campaigns in pursuit of their goal, but ultimately, their objective of a utopian society based on strict interpretations of Islamic doctrine is irrational and unattainable.

A wave dominated by Jihadist groups would likely involve special operations forces in urban environments or rapid deployment forces for escalating events in austere locations. Conflict, poverty, and other conditions prompted diasporas of Muslims in recent decades, and these trends of refugees and displaced persons show no signs of slowing down. While relatively few migrants become involved in Jihadist groups, conditions like poverty, ostracism from society and failure to assimilate, exposure to propaganda, and returning foreign fighters may influence second-generation migrants' susceptibility to radicalization. Muslim enclaves in migrant-rich areas of France and other parts of Europe raise concerns for governments where law enforcement cannot penetrate and ethnic jurisprudence replaces national rule of law. Hence, this wave poses varied risk for domestic terrorism among Western countries and communities around the globe. Attacks most likely perpetuate contemporary terrorism trends of small arms and bombs targeting masses, but sponsors among Islamist governments present the possibility of weapons of mass destruction. Jihadist cells present a widespread threat of varying degrees of sophistication, especially against U.S. Government stationary long-term targets such as embassies or military bases. Jihadist terrorists prioritize attacks against U.S. targets due to incompatibility with Jihadist ideology, culture, and vision of how society should function. This global movement could also inspire green-on-blue attacks, especially where U.S. forces operate in Islamic societies and are perceived to be encroaching on local culture.

Wave	Catalyst	Goals	Targets	Tactics	Reasons for Decline
New Tribalism (2020s-?)	• Same as wave in which group emerged • Cultural differences • Local conditions • Weak muiltinational cooperation	Establish local/regional utopia within one generation	• Government institutions • Children • Women • Outside ethnic groups	• Rape • Child soldiers • Child brides • Ethnic cleansing/ genocide	Unknown

Table 2. Defining Characteristics of a Fifth Wave Characterized by New Tribalism

Wave	Catalyst	Goals	Targets	Tactics	Reasons for Decline
Jihadist Groups (2020s-?)	• Weak state authority in rural areas • Takfiri groups' separation from larger Islamist movement	• Isolate from society • Restore idyllic past in modern utopian society	• Governments • Ethnic groups and other religious denominations • Apostate Muslims	• Unrestrained violence • Ethnic and sectarian cleansing	Unknown

Table 3. Defining Characteristics of a Fifth Wave Characterized by Jihadist Groups

Technology Wave Characteristics and Implications

Dr. Jeffrey Simon, president of Political Risk Assessment Company, Inc., and a former RAND Corporation analyst, offers an alternative theory for a fifth wave. He theorizes a wave wherein "there will be no single type of terrorist ideology…in the same way anarchism, anti-colonialism, new left/Marxism, and religious fundamentalism dominated the preceding four waves."[12] Rather, he suggests that "the influential role of technology will be the defining characteristic of the Fifth Wave" and that methods by which terrorists conduct operations will more accurately reflect global terrorism trends than ideologies.[13] While various aspects of technology will influence this fifth wave, the principal catalyst setting this wave in motion is the internet, acting as a force multiplier for individuals and small groups attempting to influence or harm large groups or formidable targets. Groups rely on the internet for recruitment, logistics, and planning. They further leverage the internet to conduct large-scale and dangerous attacks. According to Simon, terrorist groups in the Technology Wave access critical information (i.e., maps, blueprints, and security measures), which they use to plan strikes and wage successful cyberattacks targeting critical infrastructure, financial systems, and vulnerable aspects of government and business.[14]

Wave	Catalyst	Goals	Targets	Tactics	Reasons for Decline
Characterized by technology, not specific ideology (2020s-?)	Advent of the internet	• Vary among groups • Influence masses • Harm stronger targets	• Critical infrastructure • Financial systems • Government business	• Access critical information for use in planning attacks • Large-scale cyber attacks	Unknown

Table 4. Defining Characteristics of a Fifth Wave Characterized by Technology

A wave characterized by technology would likely involve heavy reliance on the National Guard in response to domestic attacks, as well as the prioritization of cyber defense initiatives, counterintelligence activities, and operations security measures. Attacks in this wave would predominantly take place in the cyberspace domain and pose unconventional and asymmetric threats. While weapons of choice may not be the small arms and bombs typical in prior waves, attacks in this wave will likely yield more widespread and devastating effects. Weak security measures of targets and high attack sophistication of terrorists may yield high payoffs for surprise and audacity of attacks, but indications and warning frameworks can help detect pending attacks and identify targets. The cyber domain also affords combatants with geographic standoff, decreasing the risk for terrorists because they can attack virtually anywhere from anywhere. Technology also enables lone wolves to conduct large-scale, sophisticated attacks, which may be difficult to detect because of limited indications or warning. U.S. response may vary based on attacker size, sophistication, affiliation (e.g., anonymous/unknown, lone wolf, or state-sponsored), and political considerations (i.e., if the attacker is located in another nation's sovereign land); however, one likely implication and key distinction from other theories on a fifth wave involves heavy reliance on the National Guard. The prospect of cyberattacks targeting critical infrastructure increases the probability of states leveraging the National Guard in defense support of civil authorities' roles. This may involve disaster response or addressing other effects of an attack, such as riots following an attack on the financial sector. In addition to cyber defense measures, U.S. forces must also emphasize counterintelligence and operations security in order to deny terrorists access to information on potential targets.

The Fifth Wave: Anti-Globalization

Another theory, which Erin Walls introduced in her thesis for Georgetown University, centers on far-right populist ideologies and strict nationalist stances often perceived as xenophobia. According to this theory, events such as the United Kingdom's referendum to leave the European Union ("Brexit") and the United States 2016 presidential election served as catalysts for the transition from an era of religious terrorism to one fueled by ideologies based on xenophobia and nationalism.[15] Extremists would likely seek to polarize societies through controversial content using the internet and benefiting from free speech liberties in their countries. Terrorists would frequently develop "targeted violence campaigns to weaken the institutional weight of the world's largest international alliances and organizations like the [European Union] EU, [United Nations] UN, [North Atlantic Treaty Organization] NATO, and World Trade Organization," attacking international organizations and institutions in support of a global free market or propagating the "increasingly liberal world order led by U.S. hegemony."[16]

Domestic threats, weakening international coalitions, and widely adopted protectionist policies among Western nations may lead U.S. forces to focus inward to ensure domestic security. Because of U.S. Government prominence among several international alliances and organizations, such as the United Nations and NATO, terrorists in this

Wave	Catalyst	Goals	Targets	Tactics	Reasons for Decline
Anti-Globalization (2020s-?)	• Brexit • U.S. 2016 presidential election	• Polarize societies • Weaken liberal world order led by U.S. hegemony	• International alliances or financial organizations • Multinational corporations • U.S interests	• Lone wolves • Explosives • Cyber-attacks • Commercial drones	Unknown

Table 5. Defining Characteristics of a Fifth Wave Characterized by Anti-Globalization

wave would likely directly target U.S. Government facilities or personnel. An indirect result of perceived links between terrorism and migration may lead to U.S. forces securing national borders to enforce immigration guidelines. This broader mentality among Western countries, turning inward to provide security and adopting protectionist policies, may weaken international coalitions' and U.S. forces' abilities to provide security abroad.

Recommendations

The following are key actions concerning U.S. forces that U.S. Government parties can take to prepare for likely threats in a Fifth Wave of Modern Terrorism:

The U.S. Government should increase defense institution building efforts in likely hotspots of fifth wave terrorism. Extensive research and evidence indicate that political reforms and strengthening institutions are some of the most effective ways to lower violent extremist organizations' activities, especially those related to ethnic insurgencies and terrorism.[17] Defense institution building focuses on these reforms because defense institution building is a long-term approach to support partners in "developing the strong institutional foundations needed for legitimate, effective, professional, and sustainable defense sectors" by focusing engagements to guide reforms at the ministerial, military headquarters, and operational defense sector levels.[18] The traditional preparation for or reaction to conflicts abroad has been a rapid train-and-equip approach with the partner nation wherein the conflict erupts; however, the Malian Army's collapse in the face of al-Qaeda in the Islamic Maghreb in 2012, despite tens of millions of dollars and in U.S. training and equipping, revealed that such an approach is bound to fail when there are deep institutional flaws in the partner nation's defense or political apparatus.[19] Defense institution building is a more sustainable approach in staving off security crises by enhancing partners' abilities to provide internal security and manage threats. Embassy country teams should be heavily involved in developing comprehensive defense institution building plans with experts for likely breeding grounds of New Tribalism or Jihadist ideologies, such as sub-Saharan Africa and Southeast Asia.

As fifth wave terrorism groups emerge, the United States should assist organizations battling these groups below the level of armed conflict. As New Tribalist or Jihadist groups begin to challenge security forces in areas with weak government institutions, U.S. regionally aligned forces and/or special operations forces should train, advise, and assist rivals of these groups. Intelligence support to these rival groups can aid in targeting efforts and disrupt terrorist groups' operations. Additionally, the United States should leverage soft power tools to enhance local governance, which can help to delay the spread of such groups' influence. These actions afford the United States time to assess the dynamic situation and escalate to armed conflict, if deemed necessary.

Expand the National Guard's State Partnership Program in sub-Saharan Africa. The State Partnership Program involves partnerships between individual (U.S.) states and foreign nations through which states' National Guard units conduct formal engagements and training with partner nations' armed forces, law enforcement, emergency response personnel, and other organizations. The State Partnership Program contains only 13 partnerships among the 46 sub-Saharan countries in Africa, a region likely containing hotspots for fifth wave threats associated with New Tribalism and Jihadist groups.[20] New partnerships with fragile states demonstrating institutional capacity can strengthen security cooperation efforts by establishing long-term relationships fostering professionalization of armed forces, partner capacity, and interoperability. Furthermore, upper echelons of National Guard units can enhance defense institution building at the operational defense sector level by providing partner nation counterparts with assistance and expertise in readiness, command and control, logistics, and operational planning.[21]

Facilitate ease of information sharing with private sector and partner nations through formal agreements and expansion of existing tools. The U.S. Government should improve information sharing efforts with the private sector, which have stagnated because of a lack of engagement, and sign information sharing agreements with international partners. Sharing tactics, techniques, and procedures, threat information, or lessons learned can enhance security within the United States and abroad. Interagency and multinational exercises would facilitate information sharing through wargaming scenarios and preparing

appropriate responses to threats. Information sharing is especially relevant in preparing for and confronting threats associated with a global wave of terrorism characterized by technology. For instance, the U.S. Government should dedicate more resources to the Office of the Director of National Intelligence's Intelligence Community Analysis and Signature Tool, a tool designed to draw from various sources and disseminate threat information. Additional funding and manpower can expand the tool's scope from disseminating only top-secret information to sharing secret and unclassified information throughout the interagency and with select international partners.[22] Similarly, prioritizing a related annual exercise called Ice Storm, which investigates and evaluates "cybersecurity information sharing capabilities between the Intelligence Community, [Department of Defense] DOD, law enforcement agencies and international partners," can improve the practical ease of engaging with partner nations and rapidly responding to cyber threats.[23]

Explore possible fifth wave threats through research and wargaming. The geopolitical nature of terrorism and the military implications involved in these emerging threats make further research ideal for students attending professional military education institutions, such as the Army War College or National Defense University. Case studies, alternative futures, and wargaming-specific scenarios will help researchers to identify doctrinal and policy gaps concerning this anticipated wave of terrorism. Findings can shape policy, such as the prioritization of security cooperation efforts, develop or enhance contingency plans, and contribute to scenarios for multinational exercises.

Conclusion

Of the four proposed *fifth wave* theories, Kaplan's New Tribalism is the most likely to draw a response from U.S. forces. The Fund for Peace ranks nearly half of sub-Saharan African countries in its Fragile States Index "alert" category, indicative of political, security, and other conditions making the region ripe for New Tribalism violence.[24] In sub-Saharan Africa, violence against civilians (i.e., abduction, attack, and sexual abuse) conducted by identity militias—"armed and violent groups organized around a collective, common feature including…ethnicity [or] religion"—increased by nearly ten times in 8 years, growing from 83 incidents in 2010 to 817 incidents in 2018.[25] Unless drastic changes occur to strengthen political institutions within the region, sub-Saharan Africa will likely be a hotbed for New Tribalism terrorist activities threatening regional stability and prompting a response by U.S. forces.

A cyber wave would prove to be the most dangerous for U.S. forces because successful attacks would likely cause exceptionally grave damage to national security through the sabotage of critical systems or the compromise and unlimited distribution of classified information. State-sponsored groups or lone wolves may successfully breach security networks and destroy systems with sophisticated tactics. Stuxnet, a malicious computer worm, demonstrated extreme possibilities for sabotage when it destroyed one-fifth of Iran's nuclear centrifuges.[26] Other direct threats to U.S. forces, such as hacking Department of Defense assets like Pentagon databases, could yield devastating effects by exposing vulnerabilities and critical information about forces. Activities by an organization such as WikiLeaks could weaken U.S. ties with partner nations, expose national security vulnerabilities, and compromise intelligence-gathering methods and sources.

Evolving security conditions, cultural and technological factors, and global political dynamics bolster theories of a new wave of modern terrorism commencing in the near future. Waves dominated by New Tribalism, Jihadist groups, technology, or anti-globalization all present unique challenges for U.S. forces. Despite uncertainties about future threats, U.S. forces can brace for the next wave of modern terrorism through concerted efforts to hinder its momentum or mitigate its impact, primarily through increased defense institution building and security cooperation in areas of weak governance.

Endnotes

1. Michael Wolraich, "Theodore Roosevelt: The Original War on Terror," The History Reader website, June 16, 2016, https://www.thehistoryreader.com/historical-figures/theodore-roosevelt-war-terror/.

2. Erin Walls, "Waves of Modern Terrorism: Examining the Past and Predicting the Future" (master's thesis, Georgetown University, 2017), 20, https://repository.library.georgetown.edu/bitstream/handle/10822/1043900/Walls_georgetown_0076M_13610.pdf?sequence=1.

3. David C. Rapoport, "The Four Waves of Modern Terror: International Dimensions and Consequences," in *An International History of Terrorism: Western and Non-Western Experiences,* ed. Jussi M. Hanhimäki and Bernhard Blumenau (New York: Routledge, 2013), 300.

4. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 2011), 21.

5. Jeffrey Kaplan, "The Fifth Wave: The New Tribalism?" *Terrorism and Political Violence* 19, no. 4 (2007): 545-570, https://doi.org/10.1080/09546550701606564.

6. Ibid.

7. Ibid.

8. Ibid.

9. Ibid.

10. Michael J. McNerney, Jonah Blank, Becca Wasser, Jeremy Boback, and Alexander Stephenson, *Improving Implementation of the Department of Defense Leahy Law* (Santa Monica, CA: RAND Corporation, 2017), ix.

11. Anthony N. Celso, "The Islamic State and Boko Haram: *Fifth Wave* Jihadist Terror Groups," *Orbis* 59, no. 2 (2015): 249–268, https://doi.org/10.1016/j.orbis.2015.02.010.

12. Jeffrey D. Simon, "Technological and Lone Operator Terrorism: Prospects for a Fifth Wave of Global Terrorism," in *Terrorism, Identity and Legitimacy,* ed. Jean E. Rosenfeld (New York: Routledge, 2011), 48.

13. Ibid.

14. Ibid., 59.

15. Walls, "Waves of Modern Terrorism," 75, 77.

16. Ibid., 74, 82.

17. "I-VEO Knowledge Matrix," National Consortium for the Study of Terrorism and Responses to Terrorism website, http://start.foxtrotdev.com/ (reference hypotheses 145, 149, and 152) and http://start.foxtrotdev.com/descriptives.

18. Alexandra Kerr and Michael Miklaucic, eds., *Effective, Legitimate, Secure: Insights for Defense Institution Building* (Washington, DC: Center for Complex Operations at National Defense University, 2020), ix, 29.

19. Ibid., 21.

20. "New York and the Republic of South Africa State Partnership Program (SPP)," New York State Division of Military and Naval Affairs website, last modified 17 August 2020, https://dmna.ny.gov/spp/.

21. Kerr and Miklaucic, *Effective, Legitimate, Secure,* 42–44.

22. Derek B. Johnson, "Government information sharing efforts remain a mixed bag," *Federal Computer Week,* 23 December 2019, https://fcw.com/articles/2019/12/23/information-sharing-efforts-in-government-remain-a-mixed-bag.aspx.

23. Ibid.; and Office of the Director of National Intelligence, *Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan* (August 2019), 19.

24. "Fragile States Index Heat Map," Fund for Peace website, accessed 25 May 2020, https://fragilestatesindex.org/analytics/fsi-heat-map/.

25. *Armed Conflict Location & Event Data Project (ACLED) Codebook,* Armed Conflict Location & Event Data Project website, 22, https://www.acleddata.com/wp-content/uploads/dlm_uploads/2017/10/ACLED_Codebook_2019FINAL_pbl.pdf.

26. Michael B. Kelley, "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought," *Business Insider,* November 20, 2013, https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

CPT Matthew Hughes is a U.S. Army foreign area officer (Western Hemisphere). He is currently a student at the Command and General Staff Officer Course at the Western Hemisphere Institute for Security Cooperation, Fort Benning, GA. He holds a master of arts in intelligence studies from American Military University. He also holds a bachelor of science degree from the U.S. Military Academy, where he majored in Arabic/Spanish and minored in terrorism studies.

Scouts, Collection Managers, and Unmanned Aerial Vehicles in Large-Scale Combat Operations

by Captain Jordan M. Peters

You can never have too much reconnaissance.

—GEN George S. Patton Jr.

Introduction

Our Nation's focus has decisively shifted from conducting counterinsurgency and train-advise-assist operations in Iraq, Syria, and Afghanistan in an effort to prepare for great-power competition. The establishment of Security Force Assistance Brigades in particular has enabled traditional Army brigades and divisions to refocus training on combating traditional standing armies, albeit with a hybrid twist. Relieved from continuous deployment cycles to the Middle East, conventional units now have the opportunity to plan and prepare for peer-to-peer combat. For the infantry, it is a renewed emphasis on breaching enemy fortifications and clearing trenches. For cavalry scouts, it means trading in training on patrolling and security force operations for face-paint and camouflage netting. For many, peer-to-peer combat means going back to basics.

The Effectiveness and Proliferation of Unmanned Aerial Vehicles

The wars in Iraq, Syria, and Afghanistan have unquestionably benefited the Army with experience and a wealth of new tactics and technologies. Undoubtedly, among the most impactful technologies are the unmanned aerial vehicles (UAVs), colloquially referred to as "drones." These have been instrumental in supporting efforts to locate, track, and eliminate al-Qaeda, Islamic State, and Taliban targets. The difficulties of distance and terrain, coupled with the virtual nonexistence of air defense capabilities on the part of terrorists and non-state actors, have helped fuel the rapid expansion of UAV programs. Between 2001 and 2008, the United States conducted 50 drone strikes. Between 2008 and 2012, that number increased to 400 and, according to at least one study, accounted for the elimination of approximately 3,300 al-Qaeda and Taliban members. The proliferation of UAVs further attests to their usefulness, as more than 90 nations have purchased or developed

Photo by Army SPC Javan Johnson

A Soldier looks through binoculars to check for simulated opposing forces during a field training exercise at the Vaziani Training Area near Tbilisi, Georgia, March 4, 2020.

reconnaissance UAVs. Currently, China is spearheading the proliferation of UAVs by offering a variety of relatively inexpensive platforms for sale.[1]

Along with the rapid development of a number of military technologies, China's efforts in the field of UAVs have yielded dramatic results. The new DR-8 UAV, reportedly able to deploy from China's first indigenous aircraft carrier, is a long-range reconnaissance aircraft.[2] Designed to fly at supersonic speeds, the DR-8 is reportedly able to evade both missile and air defenses, thereby making it one of the few UAVs theoretically capable of operating in a large-scale combat environment. The Chinese newspaper, *South China Morning Post,* reporting the newly developed drones, boasts that China is the only nation possessing a supersonic stealth UAV. This means China is, apparently, the only nation claiming to be able to conduct unmanned intelligence, surveillance, and reconnaissance in a large-scale combat environment.[3]

In Russia, UAVs under the control of the Russian Aerospace Forces focus on reconnaissance at the operational level. The newest UAV, the Forpost-R, boasts a range of 250 kilometers, a speed of 200 kilometers per hour, a ceiling of 6 kilometers, and a dwell time of 18 hours. At the strategic level, the 6-ton, twin-engine Altius enjoys the same speed but operates for up to 48 hours. While Russia is developing UAVs capable of kinetic strikes, most of its existing fleet appears unarmed and thus highly vulnerable in large-scale combat operations. Besides intelligence collection, Russia's military uses the Orlan-30 to lase targets, making laser-guided munitions, both from artillery and aircraft, exceptionally accurate as demonstrated during Russian operations in Syria. In a large-scale combat environment, such practices would obviously be contingent on Russian control of the airspace, without which precision-guided munitions would be without their silver bullet.[4] Undoubtedly, UAVs designed for reconnaissance and kinetic operations are effective tools in the counterinsurgency kit bag. However, their usefulness in large-scale combat operations is far from certain.

Antisatellite Technologies

Collection managers rely not only on UAVs for collection but also on national assets in space. Once thought untouchable, these platforms may well be among the first casualties in any future conflict between the United States and a peer threat. Recognizing the importance of space-based intelligence collection assets, China and Russia have labored to develop antisatellite missile systems. For Russia, tests began in the Soviet Union during the 1960s and 1970s to develop a missile that could approach enemy satellites in orbit before detonating. With the end of the Cold War, the global development of antisatellite capabilities largely fell by the wayside until, in 2007, China successfully destroyed an outdated weather satellite 500 miles from Earth in high orbit. Much like the weather satellite, the global moratorium on antisatellite missile technology was obliterated. Since then, antisatellite technology has slowly proliferated, with India in 2019 joining the ranks of the United States, Russia, and China as one of the few countries to successfully develop an antisatellite missile capability. As space becomes increasingly shared and contested, the proliferation of antisatellite missile technology will likely continue.[5]

"Both states [China and Russia] are developing jamming and cyberspace capabilities, directed energy weapons, on-orbit capabilities, and ground-based antisatellite missiles that can achieve a range of reversible to nonreversible effects" [6]

Unfortunately for American military and intelligence planners, missiles are not the only antisatellite tools in a potential adversaries' kit bag. At a 2018 technology summit, Defense Intelligence Agency (DIA) Director LTG Robert Ashley discussed the national competitor's focus on "the ability to interdict satellites both from a ground standpoint and from a space standpoint," and added, "the technology is being developed right now. It is coming in the near future."[7] In February 2019, DIA reported that the development of Russian and Chinese antisatellite laser technology was just 1 year away from achieving the capability to target satellites in low Earth orbit. Chemical sprayers, high-power microwaves, radiofrequency jammers, kinetic kill vehicles, robotic mechanisms, and, yes, lasers, are among those tools and capabilities that China is developing. The targeting of American satellites to degrade or deny intelligence collection and Global Positioning System capabilities may well be among the opening blows of any conflict between China and the United States. While unable to match Chinese investment in developing offensive space capabilities, Russia inherited a comprehensive technical expertise in satellite and rocket technology from the Soviet Union and, according to a public DIA report, "began delivering a laser weapon system to the Aerospace Forces that likely is intended for an [antisatellite] mission."[8] Just as American commanders and collection managers cannot rely upon the utilization of UAVs in large-scale combat operations, neither can they rely on space-based collection assets.

Aerial Superiority

The winning and maintaining of aerial superiority has for nearly a century served as a staple of American

military planning and strategy. Not since World War II, has an enemy air force seriously opposed American airpower. In large-scale combat operations with a peer threat, the United States can expect to encounter staunch opposition not only from a hostile air force but also from a network of integrated ground-based missile defenses. Expanding upon such a scenario, in 2017, U.S. Air Force Maj. Gen. (then Brig. Gen.) Alex Grynkewich said, "We may no longer be able to prevent adversaries from operating within their own integrated air defenses. Instead, we will control their airspace for a discrete time and over a limited area, as defined by the needs of the joint force team. Control of the air is not an end in and of itself—we set the air superiority condition only so we may then exploit the air domain to maximum effect and preclude an adversary from doing the same."[9] In such an operational environment, the survivability of even the most advanced combat aircraft is far from assured. As prospects of our own aerial superiority are far from certain, potential adversaries work diligently to develop UAVs and incorporate them into their services. What then does this say for the potential survivability of American UAVs tasked by collection managers attempting to conduct reconnaissance operations?

What, then, does this mean for American commanders at all levels operating in a large-scale combat environment? While utilization of UAVs as surveillance platforms and reconnaissance assets may occur in a large-scale combat operations environment, until aerial superiority is achieved, it is difficult to see how the entire range of collection platforms can be safely employed. The conflicts in Afghanistan, Iraq, and Syria have understandably nurtured reliance on UAVs for real-time and long-range reconnaissance. However, in an operational environment with an opponent that boasts modern integrated air defense systems—an environment in which even the aerial superiority that leaders have counted on for decades is not guaranteed—UAVs will not perform the majority of reconnaissance and collection. At the tactical level, large-scale combat operations will revert the reliance for reconnaissance back to ground-based sensors. In short, the return of peer-to-peer war heralds the return of the preeminence of the cavalry scout.

The Significance of Ground-Based Reconnaissance

Ground-based reconnaissance units stood for thousands of years as a commander's eyes and ears on the battlefield. Only with the development of airplanes and satellites in the 20th century and UAVs in the 21st century could a commander enjoy an overhead view of the area of operations. Contested airspace therefore diverts commanders back to a more traditional form of reconnaissance—scouts. FM 3-90-2, *Reconnaissance, Security, and Tactical Enabling Tasks, Volume 2,* reflects this transition, stating, "Reconnaissance primarily relies on the human dynamic rather than technical means."[10]

Meant to collect and provide information about the terrain, civil considerations, and enemy forces, ground-reconnaissance forces enable both commanders and intelligence to plan operations and fill intelligence gaps especially at the battalion, brigade, division, and corps levels. Commanders direct these assets, ensuring their employment falls within the scope of their capabilities and limitations. There is an expectation that commanders will use every method of collection available to them, following the principle of reconnaissance that no reconnaissance assets are to be held in reserve. The intent of having a variety of platforms is to complement one another, filling in the gaps and covering the limitations of various methods. For example, while inclement weather may preclude UAV collection, ground reconnaissance elements are an all-weather asset.[11]

U.S. Army photo by SPC Dustin D. Biven

A U.S. Army cavalry scout assigned to Headquarters and Headquarters Company, 1st Battalion, 63rd Armor Regiment, 2nd Armored Brigade Combat Team, 1st Infantry Division, uses leaves and branches in the fields of Hohenfels Training Area to camouflage himself while looking for opposing force soldiers during Combined Resolve X in Hohenfels, Germany, May 4, 2018.

Reconnaissance and IPB

FM 3-90-2's Chapter 13 reads, "Reconnaissance is a focused collection effort. It is performed before, during, and after other operations to provide information used in the intelligence preparation of the battlefield (IPB) process, as well as by the commander in order to formulate, confirm, or modify his course of action (COA)."[12] Put simply, reconnaissance fuels the IPB process. In planning for reconnaissance operations, however, squadron and brigade-level S-2's conduct an (often hasty) IPB process to prepare reconnaissance units to depart prior to a brigade's main body. The information collected by these reconnaissance assets then serves as an input to higher-level staffs conducting a more in-depth IPB process.

To effectively manage the IPB process and plan collection management at the squadron and brigade levels, intelligence officers and collection managers require a thorough understanding of the capabilities and challenges of ground-based reconnaissance. To understand the symbiotic relationship between reconnaissance and the IPB process, intelligence professionals should study the reconnaissance-pull and reconnaissance-push methods. Reconnaissance-pull is reconnaissance that determines which routes are suitable for maneuver, where the enemy is strong and weak, and where gaps exist, thus pulling the main body toward and along the path of least resistance. Commanders opting for the reconnaissance-pull method use the products of the IPB process in an interactive and repetitive way. Combat information is used to determine a preferred course of action based on the tactical situation. Reconnaissance-push is reconnaissance that refines the common operational picture, enabling the commander to finalize the plan and support shaping and decisive operations. The commander uses the products of IPB interactively with combat information to support a course of action already identified. In contrast, leaders opting for the reconnaissance-pull method rely on the information obtained and relayed by reconnaissance assets to determine a course of action in concert with IPB products.[13] Despite the difference between the two, it is important to note that both IPB products and reconnaissance serve as key inputs into a commander's decision-making process.

Before deploying a reconnaissance unit, the commander should establish the overall objective of reconnaissance with input from intelligence staff and collection managers. Like aerial reconnaissance, ground-based reconnaissance can focus on locating enemy forces. While aerial reconnaissance can identify terrain features, ground-based reconnaissance is uniquely equipped to identify, classify, and map obstacles and terrain features of all kinds. A useful though often overlooked tool reconnaissance units can provide is the route report, or ROUTEREP. In it, reconnaissance units examine and report route trafficability, location and description of built-up areas, lateral routes, bridge classifications, fording sites, bypasses (overpasses, underpasses, culverts), and obstacles (natural and manmade).[14] At the squad level, reconnaissance units are trained to use mathematical formulas to calculate slope, gradient of a curve, and surface velocity of streams and to classify bridges. This information is subsequently reported up to the squadron leadership and back to brigade-level intelligence and operations planners in the form of a ROUTEREP. The graphic depiction of a ROUTEREP into a route-classification overlay is incredibly useful, as it drives planning for both the subsequent deployment of the main body of forces and resupply operations.

Modern collection managers and intelligence professionals receive instruction on collection platform capabilities and limitations—from tactical-level UAVs to national-level space-based assets. Unfortunately, unless they have ever served in a ground-based cavalry unit, few understand the capabilities and limitations of a standard reconnaissance unit at the platoon, troop, or squadron level. Stealthy reconnaissance, for example, is methodical and time consuming. Small groups of scouts, often dismounted, will use terrain to maximize cover and concealment as they work to accomplish the reconnaissance objective undetected. Though accustomed to comparatively quick UAVs ranging the battlespace freely, S-2s relying on information from ground-based reconnaissance should be prepared to wait.

Ground-Based Technical Capabilities

The greatest capability of a ground-based reconnaissance unit is its ability to observe and report. The newest version of the Long-Range Advanced Scout Surveillance System, the LRAS3, enables scouts to observe as far as 20 kilometers. Expected to be fielded by fiscal year 2025 and equipped with forward-looking infrared, the LRAS3 enables users to identify targets and obtain a 10-digit grid coordinate without having to leave concealed positions.[15] While UAVs may prove impractical in large-scale combat operations, unattended ground sensors may not. Fielded in the early 2000s in Iraq and Afghanistan, unattended ground sensors act as a form of remote reconnaissance and force multiplier for traditional reconnaissance units and collection managers alike. Equipped with optical, acoustic, and seismic sensors, the system can consistently monitor an area in many of the same ways a cavalry scout could without having to place a Soldier in harm's way. And unlike the limited dwell time restraints considered by collection managers during collection

planning, the unattended ground sensors remain in a sleep mode until the sensors are triggered, whereupon the system automatically activates to process and transmit back to its control cell. These systems are a force multiplier for any reconnaissance unit and offer the potential to conduct continuous reconnaissance and intelligence collection.[16]

Photo by Air Force MSgt Mark C. Olsen

Researchers with the Army's Communications-Electronics Research, Development and Engineering Center at Fort Belvoir, VA, are upgrading the Long-Range Advanced Scout Surveillance System sighting system to give troops high-definition visuals and allow them to use it while concealed.

Just as collection managers and military intelligence (MI) professionals retain a working knowledge of the capabilities of various UAV platforms, so too should they acquire knowledge of the capabilities and limitations of ground-based reconnaissance assets. The Army Reconnaissance Course held at Fort Benning, Georgia, trains Soldiers primarily from the Armor and Infantry branches to plan and conduct reconnaissance operations. As the Army transitions from counterinsurgency to large-scale ground combat operations training, collection managers and MI Soldiers should push to attend the school, as it provides an understanding of ground reconnaissance largely lost during 20 years of counterinsurgency operations. Ultimately, every collection manager and MI professional needs to understand the fundamentals of reconnaissance in order to perform their wartime missions.

Conclusion

Collection managers perform an essential function in intelligence support to both counterinsurgency and large-scale combat operations. In nearly 20 years of continuous counterinsurgency operations, the science of collection management in support of such operations has advanced considerably while the collection managers themselves have received invaluable experience in performing their roles. While a single reconnaissance asset has never been able to answer every intelligence requirement, the technological advancements have multiplied commanders' and collection managers' options. Collection managers have increasingly grown accustomed to developing complex collection plans involving technical platforms. However, the fast-paced and contested nature of large-scale ground combat operations requires the utilization of collection assets on a tactical scale. Collection managers operating in large-scale combat environments will need to get creative because of the vulnerability of technical intelligence collection from UAV and space-based platforms. The relationship between unit commanders, scouts, MI professionals, and collection managers will need to adapt to reflect this coming reality. In training centers and at home stations, we should reexamine, outline, and finalize these relationships before events force their development on the battlefield. The future of our military depends on it.

Endnotes

1. Daniel L. Byman, "Why Drones Work: The Case for Washington's Weapon of Choice," Brookings, June 17, 2013, https://www.brookings.edu/articles/why-drones-work-the-case-for-washingtons-weapon-of-choice/.

2. Cindy Hurst, "China's Cutting-Edge Military Unmanned Vehicles," *OE Watch* 9, no. 11 (November 2019): 28.

3. Ibid.

4. Chuck Bartles, "The Proliferation of Russian Reconnaissance UAVs," *OE Watch* 9, no. 11 (November 2019): 6–8.

5. Gerry Doyle, "Factbox: Anti-satellite weapons: rare, high-tech, and risky to test," Reuters, March 27, 2019, https://www.reuters.com/article/us-india-satellite-tests-factbox/factbox-anti-satellite-weapons-rare-high-tech-and-risky-to-test-idUSKCN1R80UW.

6. Defense Intelligence Agency, *Challenges to Security in Space* (Washington, DC, January 2019), iii, https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

7. Patrick Tucker, "Pentagon Intelligence Chief: Russia And China Will Have Weapons in Space 'In the Near Future,' " *Defense One,* June 27, 2018,

https://www.defenseone.com/technology/2018/06/pentagon-intelligence-chief-russia-and-china-will-have-weapons-space-near-future/149335/.

8. Patrick Tucker, "China, Russia Building Attack Satellites and Space Lasers: Pentagon Report," *Defense One,* February 12, 2019, https://www.defenseone.com/technology/2019/02/china-russia-building-attack-satellites-and-space-lasers-pentagon-report/154819/.

9. Alex Grynkewich, "The Future of Air Superiority, Part I: The Imperative," War on the Rocks, January 3, 2017, https://warontherocks.com/2017/01/the-future-of-air-superiority-part-i-the-imperative/.

10. Department of the Army, Field Manual 3-90-2, *Reconnaissance, Security, and Tactical Enabling Tasks, Volume 2* (Washington, DC: U.S. Government Publishing Office [GPO], 22 March 2013), 1-1.

11. Ibid., 1-5.

12. Ibid., 1-1.

13. Ibid., 1-12.

14. Department of the Army, Army Techniques Publication 3-20.98, *Scout Platoon* (Washington DC: U.S. GPO, 4 December 2019), 3-27, A-4.

15. Todd South, "Shovel or RPG? Army upgrades will help scouts better identify targets," *Army Times,* February 26, 2018, https://www.armytimes.com/news/your-army/2018/02/26/shovel-or-rpg-army-upgrades-will-help-scouts-better-identify-targets/.

16. Clarence A. Robinson, Jr., "Sensors Bolster Army Prowess," *Signal*, March 2004, https://www.afcea.org/content/sensors-bolster-army-prowess.

CPT Jordan Peters commissioned in 2014 through Dickinson College's Army Reserve Officer Training Corps program. He holds a bachelor of arts in political science and security studies and graduate degrees in public policy and intelligence studies from Liberty University and American Military University, respectively. From June 2015 to January 2019, he served as a squadron assistant S-2, scout platoon leader, headquarters troop executive officer, squadron rear-detachment commander, and plans officer in 3rd Squadron, 89th Cavalry Squadron, 3rd Brigade, 10th Mountain Division, at Fort Polk, LA. CPT Peters is currently assigned to Bravo Company, 312th Military Intelligence Battalion, 470th Military Intelligence Brigade, at Fort Sam Houston, TX.

Enabling Success of Brigade Combat Team's Collection Management in the Era of Multi-Domain Operations

by Captain Matthew F. Smith

U.S. Army photo by SSG True Thao

U.S. Army cavalry scouts with the 1st Battalion, 16th Infantry Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division, maneuver toward cover after an air assault during exercise Platinum Lion 19 at Novo Selo Training Area, Bulgaria, July 9, 2019.

Introduction

The Army's operating concept for multi-domain operations (MDO) has generated much discussion on how Army formations will conduct warfare into 2040. The core idea of MDO is that the Army must maneuver at echelon and leverage all organic capabilities across all domains to achieve periods of overmatch. By successfully employing maneuver, MDO enables the joint force to create multiple dilemmas and mass effects on enemy forces, creating conditions to achieve commander's desired effects at decisive points. For brigade combat teams (BCTs) and collection managers specifically, achieving information collection success at the commander's desired decisive point will require increased synchronization across all domains and echelons. Combat training center trends indicate that the current BCT modified table of organization and equipment structure does not adequately enable detailed synchronization of collection assets organic to the BCT or at echelons above brigade. Within the MDO construct and the envisioned future operational environment, this gap in collection management capability at the BCT diminishes lethality and leaves an opportunity for overmatch unexploited.

Doctrine versus Concepts

A key to developing concepts is to understand their relationship with doctrine and the inherent differences between concepts and doctrine.

Doctrine provides fundamental principles by which the military forces or elements thereof guide actions in support of national objectives. It is authoritative, requiring judgment in application.[1] Doctrine describes the current (and near-term) force, current and programmed force capabilities, and the current (and near-term) force's ability to apply those capabilities to accomplish missions in support of national security objectives. In addition, doctrine serves the following purposes:

- Provides a common language to facilitate shared understanding during military operations.
- Drives how the Army is organized and equipped.
- Serves as the basis for all Soldiers and leader training and education.

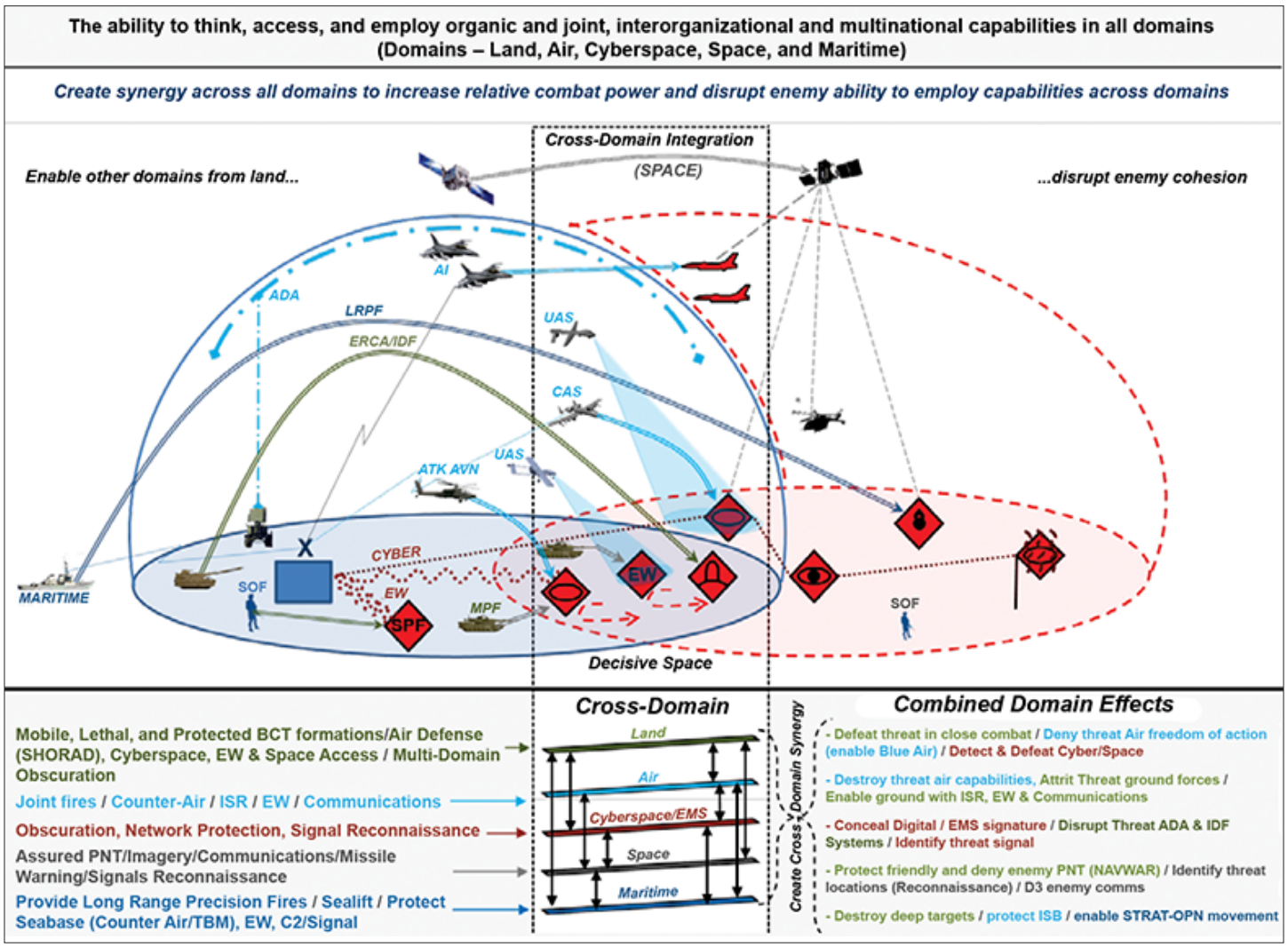
Concepts, in contrast, describe future operational requirements that the Army will likely have to meet. Restated, doctrine guides today's force and influences near-term change; concepts stand years in the future and pull today's force forward to anticipate operations in the future operational environment.[2]

Evolution from Concept to Doctrine

Emerging technologies and our strategic competitors are driving a fundamental change in the character of war. The American way of war must evolve and adapt so that our warfighting methods enable the joint force of the future. *The U.S. Army in Multi-Domain Operations 2028* is the first step in this evolution. It is the foundation for continued discussion, analysis, and development. The evolution of the concept into doctrine and practice will inform the way the Army recruits, trains, educates, and operates now and into the future.[3]

Planning for and managing collection assets in the envisioned operational environment will be a challenging task. At division and higher echelons, there are dedicated cells responsible for information collection planning. Currently at the BCT, there are no designated cells for information collection planning. The collection management function is typically assigned to a military intelligence officer in the BCT S-2 section who is supported by the operations and intelligence staffs as one of their many other functions.[4] The cross-domain maneuver concept coupled with the tenets of MDO adds complexity to how collection management is planned to support BCT commanders and should include a dedicated collection management element. The Army is in the process of validating an adjustment to the structure of the BCT military intelligence company and BCT S-2 section to create a collection management element from existing billets. However, this concept is still in the approval process and it will require time for all necessary adjustments to be implemented.

While the Army decides how to staff and organize collection management elements in the future, BCT collection managers must build their capabilities *now*—not only within the BCT but also through increased involvement with higher headquarters. To prepare for collection management during large-scale ground combat operations, individuals currently assigned as collection managers can immediately



Brigade Combat Team Conducting Cross-Domain Maneuver[5]

increase their value to commanders if they develop an in-depth understanding of a few key areas. Specifically—

- ✦ Collection capabilities and how to employ them.
- ✦ Linkage of collection to targeting.
- ✦ Functions of a Joint Air Ground Integration Center (JAGIC), air defense airspace management/brigade aviation element (ADAM/BAE), tactical air control party, and fires cell.
- ✦ Role of information collection personnel at echelons above brigade.

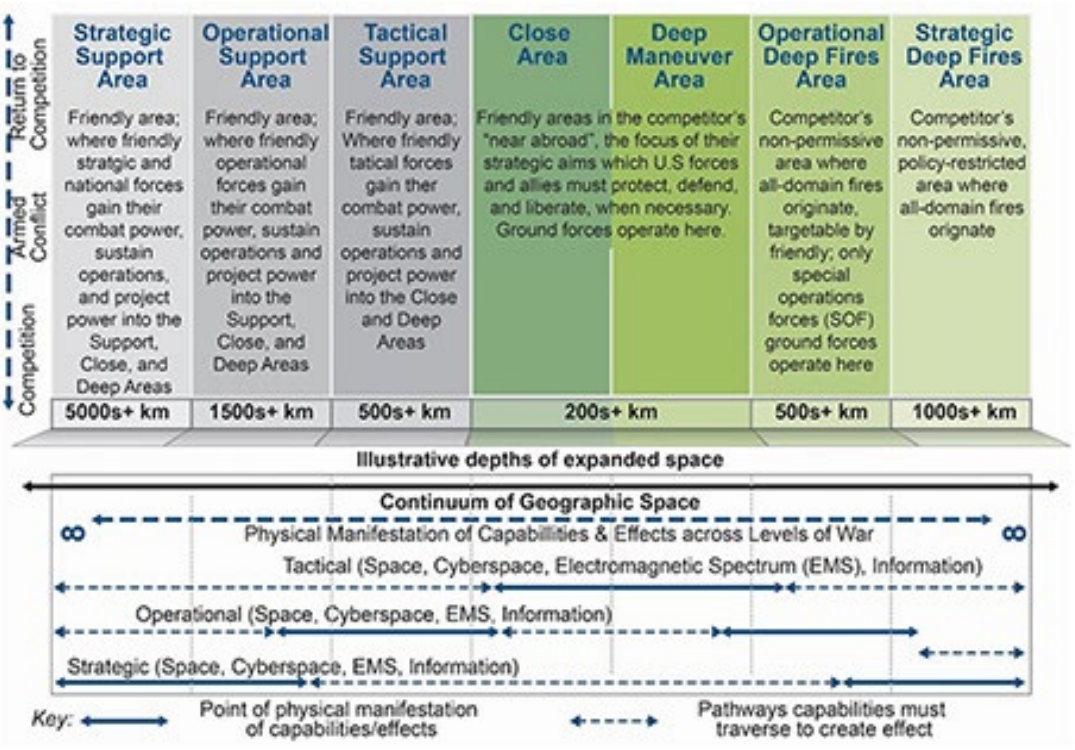
BCT collection managers who focus on these processes can prepare now to successfully execute information collection operations.

How Does Multi-Domain Operations Change the Role of the Brigade Combat Team?

The envisioned future operational environment is complex, chaotic, and unforgiving. Within MDO, Army divisions are specifically organized, equipped, and trained to dominate the close fight against a near-peer adversary in large-scale combat operations.[6] Within the last few years, BCTs have begun to transition to operating within the construct of the future operational environments and large-scale combat operations. The MDO concept fully solidifies the need for BCTs to train with and develop skills required to conduct cross-domain maneuver as part of the joint force. In MDO, defeating the enemy at the decisive point requires Army forces to operate at echelon. Army forces execute MDO with echeloned formations that conduct intelligence, maneuver, and strike activities across all five domains.[7] Division reconnaissance and security forces gain and maintain enemy contact to locate points of penetration while providing reaction time and maneuver space to the flanks of attacking BCTs. In support of the divisions, BCTs maneuver in the close area to destroy enemy maneuver forces and seize objectives. Division fires and aviation will shape the deep maneuver area to enable further BCT exploitation or pursuit to complete the defeat of the enemy's forces.[8]

How Does Multi-Domain Operations Change the Role of Collection Management?

During large-scale combat operations, divisions will array forces within the tactical support and close areas of the MDO concept's framework. The division shapes deep maneuver and close areas while executing collection activities in support of deep maneuver. Based on operational conditions, the division employs BCTs and enabling units to defeat enemy forces in the close area, simultaneously consolidating gains achieved.[9] To accomplish these tasks, BCTs will maintain the ability within MDO to converge organic information collection, maneuver, and fires capabilities with limited amounts of available aviation, maneuver support, electronic warfare, joint fires, and offensive space capabilities. According to the Army MDO operating concept, BCTs will habitually access intelligence, electronic warfare, cyberspace, and space capabilities through the division, corps, and field army.[10]



Multi-Domain Operations Framework[11]

In MDO, information collection should still be an activity that synchronizes and integrates the planning and employment of sensors and assets as well as processing, exploiting, and disseminating systems in direct support of current and future operations.[12] What MDO has changed is the degree of synchronization required by a BCT collection manager. At the tactical level, commanders use reconnaissance, surveillance, security, and intelligence operations to plan, organize, and execute shaping operations that answer their commander's critical information requirements (CCIR) and

support decisive operations.[13] The commander's choice of CCIR is the launching point for successful collection planning. The challenge for collection managers has been and will continue to be developing effective collection plans that answer the commander's requirements with timely, relevant, and accurate intelligence that enables sound decisions.[14]

In addition to a properly developed CCIR, the foundation of an effective information collection plan is based on the initial threat assessment that is regularly modified as the intelligence running estimate changes. In the operational environment envisioned in MDO, if the threat assessment is not updated and shared with the collection manager, information collection efforts will fall behind the operational conditions and opportunities of combat. The information collection plan must synchronize with the scheme of maneuver and be updated as that scheme of maneuver changes. The collection manager should work closely with the BCT S-2 in order to have an understanding of the threat characteristics, enemy templates, enemy course of action statements, and enemy event template. This understanding will help shape the collection manager's understanding of the enemy in time and space and aids in aligning asset capabilities.[15]

MDO will require brigade and division intelligence staffs to request collection support from theater, joint, and national assets.[16] Corps, divisions, and BCTs will require information from the same assets. The requirement for layering information collection capabilities and processing, exploitation, and dissemination of those assets to support MDO will require management and synchronization between brigades and echelons above brigade.[17] In MDO, forward-postured divisions and brigades employ their organic ground reconnaissance and unmanned aircraft systems to develop the immediate tactical situation, while the field army supports lower echelons with organic high-altitude surveillance and joint intelligence, surveillance, and reconnaissance (ISR) capabilities deployed from the forward edge of the tactical support area. Low-observable manned and unmanned aircraft, space surveillance, and cyberspace intelligence supplement these organic capabilities. Currently, the Army's structure supports collection management at the operational level through regionally focused joint information centers, theater intelligence brigades, Army aerial exploitation battalions, and joint aerial assets. At the tactical level, assets include the expeditionary-military intelligence brigades, target acquisition radars, reconnaissance and cavalry squadrons, attack reconnaissance aviation units, and unmanned aircraft systems.

How Can Brigade Combat Teams Enhance Collection Management Success?

Regardless of how the Army decides to staff and organize collection management elements in the future, as former Secretary of Defense Donald Rumsfeld said, "You go to war with the army you have, not the army you might want or wish to have at a later time."[18] Individuals currently assigned as collection managers can immediately increase their value to commanders if they can accomplish a few critical tasks. Mastering the skills and developing the knowledge essential to completing these tasks require selecting the right personnel and promoting the right balance of operational, institutional, and self-developmental preparation. In a resource-constrained environment, BCTs must train in a way that utilizes and incorporates the use of all collection functions at every opportunity. Collection management goes beyond layering unmanned aircraft systems on an information collection synchronization matrix. The current trends from combat training centers indicate that when incorporation of all assets is not properly planned and resourced, the plan does not achieve the results commanders need. The selection of collection management personnel needs to be for their potential to apply information collection principles and gain the repetitions required to develop functional experience while leveraging the systems and processes that are unique to each formation.

To prepare for collection management within large-scale combat operations, collection managers should develop an in-depth understanding of the following areas:

Understand Collection Capabilities and Their Employment. Information collection requires a continuous, collaborative, and parallel planning process involving the BCT, its higher headquarters, and subordinate battalions. The commander at each echelon must be closely involved in the information collection planning process and must quickly and clearly articulate CCIRs to the staff. Staff officers must develop, prepare, and disseminate the information collection plan. As opportunities become available, modifications to the information collection plan must be identified by the staff and executed by the unit.[19] Personnel assigned in a collection management role must know and address the practical capabilities and limitations of all BCT information collection assets and the capability of any BCT unit to provide information.[20] They must review all available collection assets and create an inventory of capabilities to apply against collection requirements.[21]

While reviewing the available collection assets, the collection manager should evaluate the assets according to their capability and availability. To best measure the capabilities

of the collection assets, collection managers must know and address the practical capabilities and limitations of all unit organic assets.[22] Capabilities include—

- Range.
- Day and night effectiveness.
- Technical characteristics.
- Reporting timeliness.
- Geolocation accuracy.
- Durability.
- Threat activity.
- Sustainability.
- Vulnerability.
- Performance history.

Collection managers should also consider resource requirements not only for the current CCIR but also for the transition to the next operation. Transitions require planning and preparation before their execution to maintain the momentum and tempo of operations.[23] The key to mastering transitions as a collection manager is to continuously refine the list of potential information requirements, understand the current available assets for immediate or future tasking, and refine the threat array. By maintaining an understanding of these three critical collection management areas, collection managers will be able to plan and posture capabilities to answer the CCIR and enable the commander to make decisions.

Understand the Linkage of Collection to Targeting. With a firm understanding of collection asset capabilities, the collection manager can have an immediate impact in informing the targeting process. The BCT staff uses the targeting products of the division to coordinate and integrate targeting actions of the brigade. BCT targeting addresses targets assigned to the brigade by division and the employment of assets under brigade control. Collection managers should recommend the sensor or observer that will answer the specific information requirement/task to the unit and validate the weapon system required to detect, track, and perform battle damage assessments of the high-payoff targets.[24] To best accomplish this critical process, the timing of the targeting working group sessions should be carefully planned. While the planning focus for a BCT is normally 24 to 36 hours out, the BCT target nominations and air support requests must be planned in advance and in conjunction with the division, corps, theater Army, and joint air tasking cycle. For these reasons, the BCT targeting focus is 24, 48, and 72 hours out. Within MDO, commanders must understand that the planning and targeting cycle should provide flexibility to seize opportunities presented based on the pace of operations.[25]

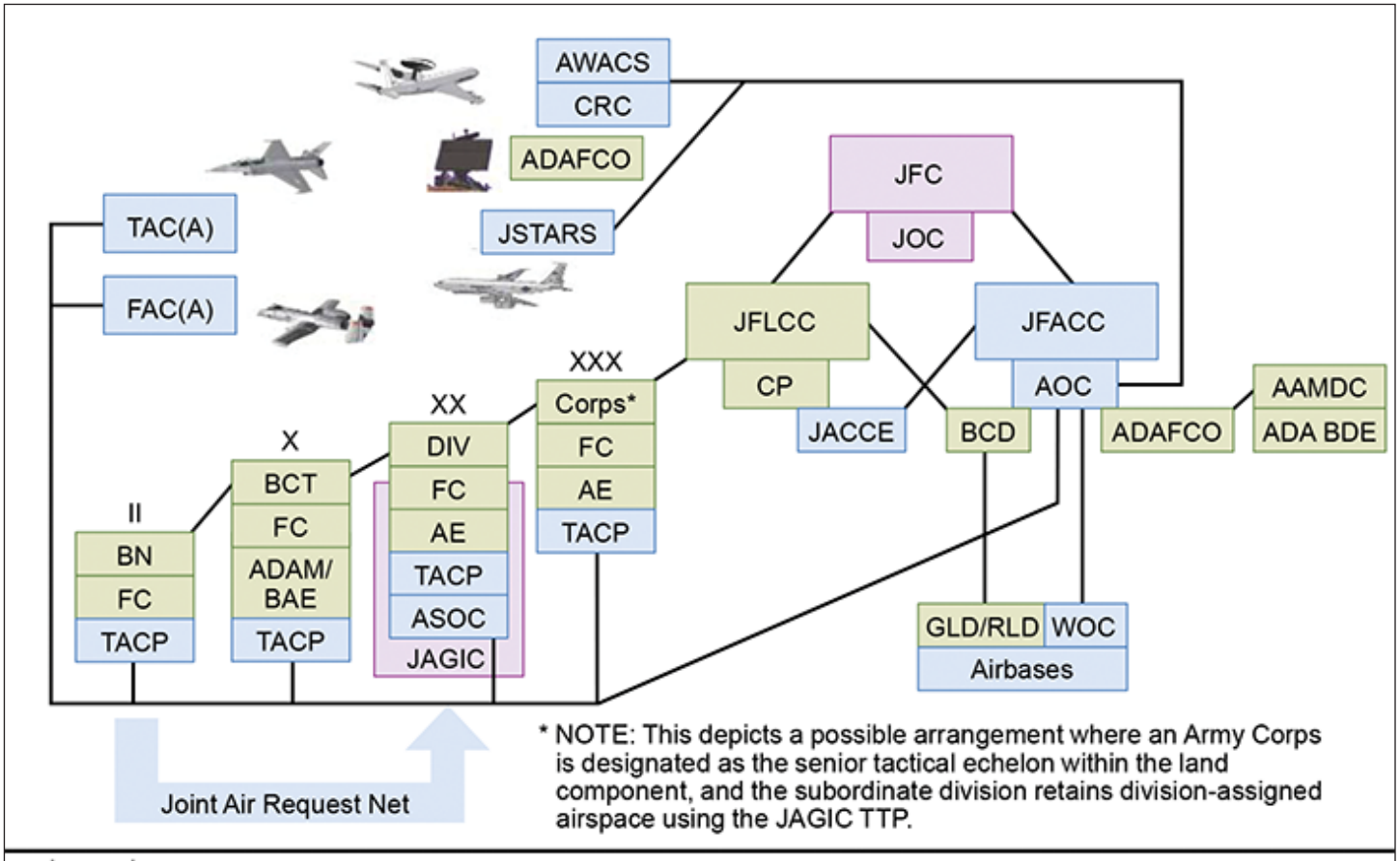
Understand the Functions of the JAGIC and the Tactical Air Control Party. BCT collection managers should understand the process for targeting within the division JAGIC and fires cell. The JAGIC controls the division airspace. It also enforces the division commander's distribution decision, priority of fires and air support, and priority for airspace use by managing the fire missions and supporting aircraft airspace requirements for subordinate units.[26] The JAGIC ensures that BCT fires cells have current fire support coordination measures and air coordination measures and that all BCT fires are executed within BCT airspace parameters.[27]

Collection managers should also understand the functions of the tactical air control party and how collection facilitates successful tactical air control party operations. The air liaison officer is typically the expeditionary air support operations squadron commander overseeing not only the division tactical air control party but also the air support operations center. At echelons below division, an air liaison officer is a tactical air control party member attached to the unit to advise the ground commander on air operations. At each echelon, the air liaison officer plans and facilitates the execution of airpower in accordance with both the ground commander's and joint force air component commander's guidance and intent.[28] BCT tactical air control parties provide liaisons to joint command and control nodes that control joint fires assets, provide assistance with planning for and integrating airpower into ground operations, and provide primary terminal attack control of close air support.[29] The BCT tactical air control party is a vital capability because they provide critical understanding of collection capabilities and recommend targeting solutions. BCT collection managers should work alongside the tactical air control party and BCT fire support officer to better synchronize their plans to that of the air tasking order because the air operations center normally establishes a 72-to-96-hour air tasking planning cycle.[30]

Understand How BCTs Coordinate Airspace Management. BCT collection managers should understand that the JAGIC coordinates airspace for division aerial assets conducting information collection and target acquisition as well as airspace for joint aerial information collection assets operating in and above the division's area of operations. As the division airspace control element in the command operations and information center, the JAGIC is a potential source of information for division and BCT collection and assessment efforts.[31]

BCTs have something similar in the ADAM/BAE responsible for integrating brigade airspace, including air and missile defense and aviation functions. The ADAM/BAE develops, coordinates, and executes requirements at brigade level and below by coordinating with higher, subordinate, and adjacent elements. The ADAM/BAE receives air coordination measures requirements from subordinate units or develops airspace requirements during the military decision-making process. It then submits them in the form of a unit airspace plan to the division airspace element for inclusion in the airspace control order. During mission execution, the ADAM/BAE coordinates directly with the JAGIC for all dynamic airspace requirements. The ADAM/BAE works closely with the BCT fire support, tactical air control party, and collection personnel to ensure all airspace requirements are in accordance with the commander's priorities.[32]

Understand the Role of Information Collection Personnel at Echelons above Brigade. Within the MDO construct, collection managers will be required to interact with division and higher elements at a much higher frequency. As a result, BCT collection managers must understand the role they play within the joint fight. Developing the functional understanding and relationships at the division will better prepare collection managers to meet the challenges of synchronizing collection efforts in that environment. Aside from interacting with the information collection cell within



Legend

AAMDC	Army air and missile defense commander
ADA BDE	air defense artillery brigade
ADAFCO	air defense artillery fire control operations
ADAM/BAE	air defense airspace management/brigade aviation element
AE	airspace element
AOC	air operations center
ASOC	air support operations center
AWACS	Airborne Warning and Control System
BCD	battlefield coordination detachment
BCT	brigade combat team
BN	battalion
CP	command post
CRC	control and reporting center
DIV	division
FAC(A)	forward air controller (airborne)
FC	fires cell
GLD	ground liaison detachment
JACCE	joint air component coordination element
JAGIC	joint air ground integration center
JFACC	joint force air component commander
JFC	joint force commander
JFLCC	joint force land component commander
JOC	joint operations center
JSTARS	Joint Surveillance Target Attack Radar System
RLD	reconnaissance liaison detachment
TAC(A)	tactical air coordinator (airborne)
TACP	tactical air control party
TPP	tactics, techniques, and procedures
WOC	wing operations center

Theater Air Control System/Army Air Ground System[33]

the division G-2, BCT collection managers should also become familiar with the role of the current operations integration cell collection manager and Air Force liaison officers.

The current operations integration cell collection manager is assigned at tactical levels in the Army. The Air Force ISR liaison officer advises the division on use of ISR capabilities, including national and theater assets and processing, exploitation, and dissemination cells. At the operational level, the ISR liaison officer may be located within the joint air operations center.[34] The information collection current operations manager acts as a liaison to the various information collection stakeholders and is incorporated with the command post fires cell, intelligence current operations, and air liaison officer. The role is vital because they are responsible for managing the current collection plan and maintaining situational understanding of all collection assets operating in the assigned airspace.[35] The Air Force ISR liaison officer is assigned to a supported ground unit, often with the air liaison officer or tactical air control party, to assist with collection planning functions and advise on optimizing information collection capabilities. At a division, the Air Force ISR liaison officer works in the JAGIC and complements the knowledge of the division collection manager and intelligence officer.[36]

Conclusion

The collection manager assignment is critical to the success of a BCT conducting cross-domain maneuver in MDO. As the Army continues to develop a solution for the collection management element, commanders, with input from the BCT S-2, should focus on selecting the right personnel to assign as collection managers. Personnel assigned as collection managers must take steps now to better prepare for the future operational environment and the more complex roles required of them. BCT collection managers direct, plan, and manage the efforts to answer information requirements that allow commanders to make informed decisions. As the right people fill the role of collection manager and apply the foundational concepts discussed above, BCTs will see an increase in successful collection planning and greater support during operations.[37]

BCTs should select collection managers with organizational experience and reinforce this experience with both institutional and operational training. Examples of institutional training for collection managers are the Information Collection Planners Course (ASI Q7) and the Joint Firepower Course (ASI 5U). An important consideration for operational training is ensuring it incorporates brigade and division staffs. This will empower those BCT collection managers with the skills necessary to synchronize assets in a way that allows the commander to make informed decisions. Officers who performed best in this role during a rotation at the National Training Center were senior military intelligence captains who completed key developmental assignments in the cavalry squadron or a maneuver battalion and were assisted by a key developmental complete military intelligence lieutenant from the military intelligence company who was familiar with the organic intelligence systems. This pairing provides the understanding and experience needed as the foundation for developing collection managers who can quickly develop and synchronize collection needs in a rapidly changing environment. Collection managers who are developed in this way will be capable of understanding and developing collection management tasks with higher echelons. The challenge has been, and will continue to be, for collection managers to generate collection plans that answer the commander's requirements with timely, relevant, and accurate intelligence that enables commanders to make sound decisions.[38] BCT commanders, staffs, and collection managers who focus on the steps outlined in this article can prepare today to successfully exploit the operational conditions and opportunities of MDO.

Endnotes

1. Department of the Army, Training and Doctrine Command (TRADOC) Regulation 25-36, *The TRADOC Doctrine Publication Program* (Fort Eustis, VA: TRADOC, 21 May 2014), 5.

2. Department of the Army, TRADOC Pamphlet 71-20-3, *The U.S. Army Training and Doctrine Command Concept Development Guide* (Fort Eustis, VA: TRADOC, 6 December 2011), 6.

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

4. Department of the Army, Field Manual (FM) 3-55, *Information Collection* (Washington, DC: U.S. Government Publishing Office [GPO], 3 May 2013), 2-5.

5. Department of the Army, TRADOC Pamphlet 525-3-6, *The U.S. Army Functional Concept for Movement and Maneuver 2020–2040* (Fort Eustis, VA: TRADOC, 24 February 2017), 23.

6. Department of the Army, TRADOC, *The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025–2045* (Fort Eustis, VA: TRADOC, 24 September 2018), 47.

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

8. Department of the Army, TRADOC, *Concept for Multi-Domain Combined Arms,* 42.

9. Ibid., 51.

10. Department of the Army, TRADOC Pamphlet 525-3-1, *Multi-Domain Operations 2028,* 23.

11. Ibid., 8.

12. Department of the Army, Army Techniques Publication (ATP) 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington: U.S. GPO, 10 February 2015), 3-18 (common access card login required).

13. Department of the Army, FM 3-55, *Information Collection,* 1-3.

14. Ibid., iv.

15. Ibid., 3-1.

16. Ibid., 5-2.

17. Ibid., 5-11.

18. Eric Schmitt, "Iraq-Bound Troops Confront Rumsfeld Over Lack of Armor," *New York Times,* December 8, 2004. https://www.nytimes.com/2004/12/08/international/middleeast/iraqbound-troops-confront-rumsfeld-over-lack-of.html.

19. Department of the Army, ATP 2-19.4, *Intelligence Techniques,* 3-19.

20. Ibid., 3-22.

21. Department of the Army, FM 3-55, *Information Collection,* 3-4.

22. Department of the Army, ATP 2-19.4, *Intelligence Techniques,* 3-22.

23. Ibid., Appendix C.

24. Department of the Army, ATP 3-60, *Targeting* (Washington, DC: U.S. GPO, 7 May 2015), 4-1.

25. Ibid., 4-2.

26. Department of the Army, ATP 3-91.1, *The Joint Air Ground Integration Center* (Washington, DC: U.S. GPO, 17 April 2019), 2-1.

27. Ibid., 2-13.

28. Ibid., 1-14.

29. Ibid., 2-13.

30. Department of the Army, ATP 3-60, *Targeting,* D-9.

31. Department of the Army, ATP 3-91.1, *Joint Air Ground Integration Center,* 1-5.

32. Ibid., 2-12–2-13.

33. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-30, *Joint Air Operations* (Washington, DC: The Joint Staff, 25 July 2019), II-11.

34. Department of the Army, ATP 3-91.1, *Joint Air Ground Integration Center,* 1-15.

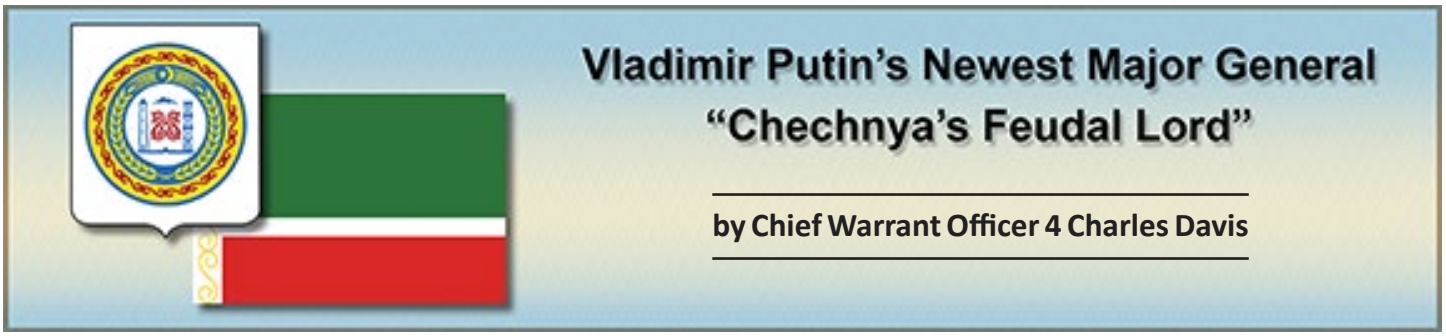
35. Department of the Army, ATP 2-19.4, *Intelligence Techniques,* Appendix C.

36. Department of the Army, ATP 3-91.1, *Joint Air Ground Integration Center,* 1-5.

37. Department of the Army, Training Circular 2-50.5, *Intelligence Officer's Handbook* (Washington, DC: U.S. GPO, 6 January 2010 [obsolete]), B-17.

38. Department of the Army, FM 3-55, *Information Collection,* iv.

CPT Matthew Smith is currently assigned to the National Ground Intelligence Center in Charlottesville, VA. Previous assignments include higher command/exercise control deputy G-2 at the National Training Center; squadron S-2 observer coach/trainer at the National Training Center; and infantry battalion S-2 in 1st Stryker Brigade Combat Team, 1st Armored Division. He holds a bachelor of science in political science and a master of arts in executive leadership.



Vladimir Putin's Newest Major General "Chechnya's Feudal Lord"

by Chief Warrant Officer 4 Charles Davis

Introduction

On 24 July 2020, *Sobesednik,* a popular Russian magazine, reported President Vladimir Putin had awarded the rank of major general in the Russian National Guard to Ramzan Kadyrov.[1] Kadyrov was not an officer of any rank in the Russian military; he was and remains the current president of Chechnya. Kadyrov also has a highly negative profile within the U.S. State Department. Just days before Putin's announcement of Kadyrov's newest accolade, the United States placed Kadyrov on the restricted travel list, along with his wife and daughters. Kadyrov responded by posting a photo of himself with two AK-47s and a caption stating, "[Mike] Pompeo, we accept the fight. Things are about to get more interesting."[2] Was Putin's action intended as a snub to the United States? And why the need to award a sitting president a military rank and authorities?

Establishing a Family Dynasty

Estimating Putin's motivations for this decision requires a greater understanding of his relationship with Kadyrov and Putin's desires for Chechnya. Ramzan Akhmadovich Kadyrov is the son of former Chechen President Akhmad Kadyrov. The senior formed a militia (much like the mujahideen of Afghanistan) during the First Chechen War, calling for jihad against Russia. Akhmad Kadyrov later supported Russia during the Second Chechen War, and upon Russia's victory, Vladimir Putin installed him as the temporary leader in 2000.[3] Akhmad remained loyal to Russia and was officially elected to the position of president in 2003. In May 2004, when Akhmad was assassinated, Ramzan was 27 years old and serving as the commander of the Kadyrovtsy (his father's former militia group).

On the day of Akhmad's death, Ramzan was flown to Moscow and received personal condolences from Putin, along with an appointment as the first deputy prime minister.[4] In November 2005, he assumed the role of acting prime minister and in March 2006 was officially installed as prime minister. Throughout this period, Ramzan retained the allegiance of and authority over an ever-growing Kadyrovtsy militia group.

One might liken Putin's behavior to the Taliban's acknowledgment of Jalaluddin Haqqani's influence among the eastern provinces and the ultimate placement of his son Sirajuddin Haqqani as the military commander for the Taliban. This comparison is strengthened by the fact that Putin is dealing with a Sunni Islamic state, heavily influenced by Sufism. Tribalism and patriarchal approaches are ingrained in the culture. Similar to the Afghan regional loyalties to their mujahideen heroes, Chechen loyalties are strong and lasting, developing through family and communal ties, especially in the mountainous northern regions of Chechnya.[5]

Putin understands these similarities—leading him to invest in Kadyrov as a family dynasty best equipped to continue to provide Moscow with stability in Chechnya. To this end, Putin removed Alu Alkhanov as president in February 2007 and promoted Ramzan from prime minister to acting president, ultimately securing parliamentary support and instatement as the president in March 2007.[6] This timing is not happenstance. Chechen law requires the president to be at least 30 years old. Ramzan turned 30 in October of 2006.

Courtesy of the Russian Federation

Ramzan Kadyrov (right) with Russian President Vladimir Putin in February 2008.

A State within a State

In *A State within a State: the Case of Chechnya,* the author, Hanna Zimnitskaya, references a book about Putin, a self-portrait that sheds some light on the Russian president's personal thoughts and fears regarding the ongoing threat

of insurgency from the region and its effect on the country. To quote Putin—

> ***If we don't stop the extremists now, then some time later we'll be faced with another Yugoslavia in the entire territory of Russia, the* Yugoslavization *of Russia...First Dagestan will be overrun. Then the entire Caucasus would separate; that's clear. Dagestan, Ingushetia, and then up the Volga River to Bashkorstan and Tatarstan. This means advancing right into the middle of the country.[8]***

Putin's concerns are justified, especially when considering attacks like the 23 October 2002 seizing of a Moscow theater, which involved taking up to 700 people hostage and resulting in the death of many of the 50 hostage-takers along with 120 hostages.[9] The Beslan school siege serves as another example, with Chechen separatists taking approximately 1,000 hostages, resulting in the deaths of 340, many of them children.[10]

Putin has given almost unconditional personal support and tremendous financial resources to Ramzan in an effort to rebuild and stabilize Chechnya. Ramzan has led massive infrastructure developments in the country, which now boasts the largest mosque in the Russian Federation. When asked about his relationship with Ramzan, Putin stated, "I look upon him as a son. We have in recent years developed friendly, really friendly, personal relations, and I am convinced this has played a tremendously positive role in the life of the Chechen nation and for Russia."[11]

Photo by Vyacheslav Argenberg[12]

The Akhmad Kadyrov Mosque ("The Heart of Chechnya" Mosque) at night in Grozny, Chechnya, Russia. The mosque, designed with a set of 203-foot tall minarets, is based on the Sultan Ahmed Mosque in Istanbul.

Ramzan's Enduring Influence

Ramzan's effect in Chechnya could be compared to the popularity of General Charles de Gaulle among the French during World War II or of GEN Douglas MacArthur in the United States. Ramzan is a demigod for many, including his Kadyrovtsy militia group, which is about 30,000 strong and accountable directly to him.[13] However, he is not without criticism at home and abroad. He is accused of human rights abuses, most recently directed against Chechnya's homosexual population. Additionally, critics assert he directed numerous assassinations of those who challenged his methods.[14]

While accusations of human rights violations continue, and are echoed by the United States, Ramzan endures and is effectively consolidating both military and religious power in the North Caucasus region. Ramzan has co-opted the Qadiriya (Sufi Muslim brotherhood), shifting their message to anti-extremism.[15] In *Ramzan Kadyrov: Insecure Strongman?,* the author, Martin Breitmaier, alludes to Ramzan's effectiveness as Russia's ambassador to the Muslim nations:

> ***[Ramzan contributes] to diplomacy between Russia and Muslim countries in the Middle East and North Africa (MENA). In what is rather unusual for Russian regional politicians, the Chechen president has received or visited many senior political leaders of the MENA on behalf of Moscow (the Saudi king or Afghan vice president last year, for example). His role as one of Russia's 'Muslim ambassadors' is especially important since several countries in the region view Russia in a negative light and the fate of Moscow's key regional ally Bashar al-Assad remains uncertain.[16]***

Ramzan's Chechen militia has garnered a reputation of effectiveness and brutality. As such, during the color revolutions and anti-regime demonstrations in Moscow throughout 2011, elements of the Chechen president's personal bodyguard regiment were reportedly stationed in Moscow. Reports indicated the force would be used to dispel protestors near the interior ministry building.[17] Other reporting indicates elements of Ramzan's militia are able to travel armed throughout Russia with little to no restriction.[18]

The Russian National Guard

In response to Ramzan's consolidation of power throughout the North Caucasus, the Russian Federation attempted to purge his military power through a consolidation of his forces under the Russian National Guard. This element of Russia's military arm has been fully operational only since 2018 and is identified as a security agency structure. In *Kremlin Kontrol: Russia's*

Political-Military Reality, the author, Timothy Thomas, describes the structure and responsibilities:

> ***[The main tasks include] the joint protection of law and order together with the police; the fight against terrorism and extremism; the protection of state establishments and special freight; the protection of the territorial defense of the country; and the assistance to border guards to protect the state border. Powers included the ability to arrest lawbreakers, enter residential premises to conduct searches or arrests, cordon off terrain or residential areas, and use physical force, along with special weapons and equipment.***[19]

The National Guard that reports directly to the Russian president includes the Special Purpose Mobility Unit, Special Rapid Response Unit, and Extra-Departmental Protection Service of the Chechen Ministry of the Interior, and totals about 250,000.[20] The perceived attempt to purge or reduce Ramzan's influence over military elements of his country may be inaccurate, as his cousin Sharip Delimkhanov was selected as chief of the Russian Guard Directorate for Chechnya.[21] In an article titled "Creation of Russian National Guard Could Affect Kremlin Policies in the North Caucasus," the author, Valery Dzutsati, argues that Kadyrovtsy militia ties to the National Guard are not likely to reduce Ramzan's control or influence even as his forces change appearance and formal affiliation.[22]

Establishment of the National Guard and its heavy reliance on Kadyrovtsy militia brings us to the most recent announcement and some insight as to why Ramzan Kadyrov is now not only the president of Chechnya but also one of the most senior officers within the Russian National Guard. Putin has likely experienced some national resistance to leaving Kadyrovtsy under Kadyrov's direct control. This would explain Delimkhanov's selection as chief of the Russian Guard Directorate for Chechnya. It is not likely the Kadyrovtsy militia group leaders took these changes lightly, and in the end, Putin acquiesced and gave Ramzan military rank to ensure there was no degradation of the force.

Conclusion

Ramzan's reach into emigrated populations of Chechens in Poland, France, and Austria is of significant importance as is the security of the North Caucasus and oil pipelines running from the south. Additionally, the soft power influence Ramzan wields within the Islamic countries opens doors for Putin in a difficult region. Putin has also been a constant supporter of Ramzan and has strong personal ties to the leader, which is openly apparent to Putin's cabinet and staff. Who else would he want under direct control of his 250,000-strong security force in the event critics or the Russian people gain traction in attempts to push him out of office?

From a strategic perspective, it will be important to monitor Putin's deployment of the Russian National Guard and the level of involvement Ramzan Kadyrov maintains in operations and decision making. Ramzan's continued involvement in Russian Muslim politics will also provide insight as to Putin's priorities when it comes to the Arab states.

Endnotes

1. Akhmirova Rimma, "Gudkov: Putin gave an indulgence to Kadyrov, conferring the rank of Major General of the Russian Guard," *Sobesednik,* 24 July 2020, https://sobesednik.ru/politika/20200724-gudkov-putin-dal-indulgenciyu.

2. "The U.S. sanctioned Ramzan Kadyrov's family members and he isn't taking it well," *Meduza,* July 24, 2020, https://meduza.io/en/feature/2020/07/24/the-u-s-sanctioned-ramzan-kadyrov-s-family-members-and-he-isn-t-taking-it-well.

3. "Russia appoints Chechen leader," *BBC News,* 12 June 2000, http://news.bbc.co.uk/2/hi/europe/787811.stm.

4. Charu Singh, "Crisis in Chechnya," *Frontline,* June 4, 2004, https://frontline.thehindu.com/world-affairs/article30222673.ece.

5. Subhranil Ghosh, "Chechnya: The ethno political flashpoint plaguing a former Super power," *Modern Diplomacy,* May 17, 2020, https://moderndiplomacy.eu/2020/05/17/chechnya-the-ethno-political-flashpoint-plaguing-a-former-super-power/.

6. "Putin Dismisses Chechen President, Puts Prime Minister In Charge," Associated Press, February 15, 2007, https://web.archive.org/web/20080308153448/http://www.foxnews.com/story/0,2933,252203,00.html.

7. The Ramzan Kadyrov photo is published under the Creative Commons Attribution 4.0 International license by the Press Secretary for the President of the Russian Federation. https://commons.wikimedia.org/wiki/File:Ramzan_Kadyrov_(2018-06-15)_02.jpg.

8. Vladimir Putin, Nataliya Gevorkyan, Natalya Timakova, and Andrei Kolesnikov, *First Person: An Astonishingly Frank Self-Portrait by Russia's President Vladimir Putin,* trans. Catherine A. Fitzpatrick (New York: Public Affairs, 2000), quoted in Hanna Zimnitskaya, *A State within a State: the Case of Chechnya* (Saint Paul, MN: Macalester College, International Studies Honors Projects, Spring 2012), 40, https://digitalcommons.macalester.edu/cgi/viewcontent.cgi?article=1014&context=intlstudies_honors.

9. "This Day in History, October 23, 2002: Hostage crisis in Moscow theater," History.com, last modified October 26, 2020, https://www.history.com/this-day-in-history/hostage-crisis-in-moscow-theater.

10. "This Day in History, September 01, 2004: Chechen separatists storm Russian school," History.com, last modified August 28, 2019, https://www.history.com/this-day-in-history/chechen-separatists-storm-russian-school.

11. Весело живём! [We Live Merrily], "Vladimir Putin: Ramzan Kadyrov is like a son to me," YouTube video, 1:34, August 2, 2016, https://www.youtube.com/watch?v=HEl4Mt1CtkQ.

12. The Akhmad Kadyrov Mosque photo is published under the Creative Commons Attribution 4.0 International license by Vyacheslav Argenberg. https://commons.wikimedia.org/w/index.php?curid=94799249.

13. Marlène Laruelle, "Kadyrovism: Hardline Islam as a Tool of the Kremlin?" *Russie.Nei.Visions,* no. 99 (March 2017): 14, https://www.ifri.org/sites/default/files/atoms/files/rnv99_m._laruelle_kadyrovism_en_2017.pdf.

14. "Ramzan Kadyrov: Putin's key Chechen ally," *BBC News,* 21 May 2020, https://www.bbc.com/news/world-europe-31794742.

15. Ibid.

16. Martin Breitmaier, *Ramzan Kadyrov: Insecure Strongman?* (European Union Institute for Security Studies, 26 February 2016), 2, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2010%20Kadyrov.pdf.

17. Julie Wilhelmsen, "Inside Russia's Imperial Relations: The Social Constitution of Putin-Kadyrov Patronage," *Slavic Review* 77, no. 4 (Winter 2018): 919–936, https://www.cambridge.org/core/journals/slavic-review/article/inside-russias-imperial-relations-the-social-constitution-of-putinkadyrov-patronage/FA38D6E2093711CD76250D5152FF7CED/core-reader.

18. Ivan Nechepurenko, "FSB Officers Go on Strike After Release of Chechen Cops, Report Says," *Moscow Times,* March 24, 2013, https://www.themoscowtimes.com/2013/03/24/fsb-officers-go-on-strike-after-release-of-chechen-cops-report-says-a22672.

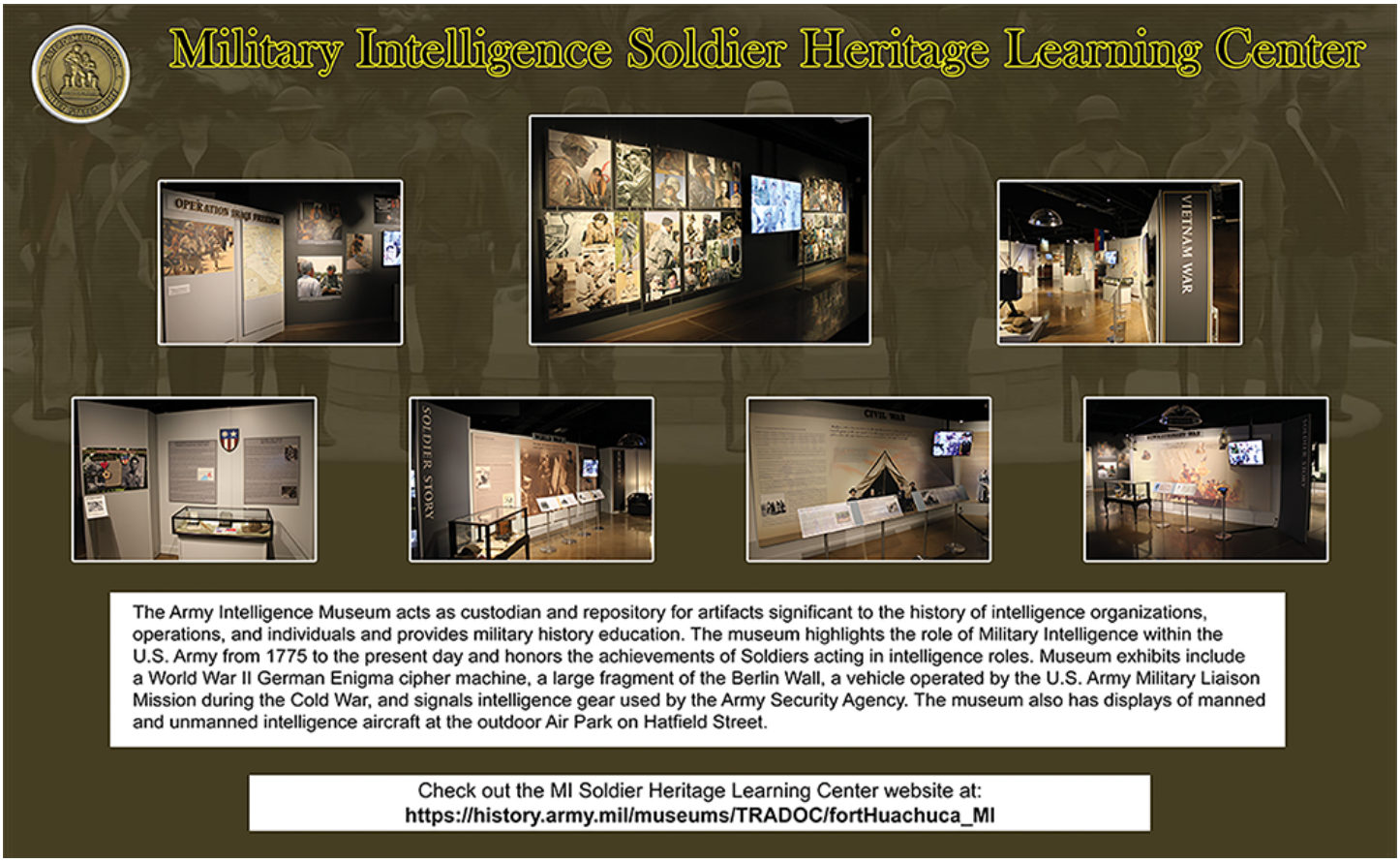
19. Timothy L. Thomas, *Kremlin Kontrol: Russia's Political-Military Reality* (Fort Leavenworth, KS: Foreign Military Studies Office, 2017), 9, https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-books/197266.

20. Laruelle, "Kadyrovism: Hardline Islam," 14.

21. Thomas, *Kremlin Kontrol,* 19.

22. Valery Dzutsati, "Creation of Russian National Guard Could Affect Kremlin Policies in the North Caucasus," *Eurasia Daily Monitor* 13, no. 75 (April 18, 2016), https://jamestown.org/program/creation-of-russian-national-guard-could-affect-kremlin-policies-in-the-north-caucasus-2/.

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



Transition to the Counterintelligence and Human Intelligence Requirements, Reporting, and Operations Management Environment (CHROME)

by Ms. Aline G. Sutton

Introduction

The U.S. Army Intelligence and Security Command (INSCOM) G-35 Collection Management (CM) executes the Army's operational counterintelligence (CI) and human intelligence (HUMINT) collection management responsibilities in support of Army priorities established by the Deputy Chief of Staff G-2, Intelligence, and Deputy Chief of Staff G-3/5/7, Operations, Plans, and Training, in accordance with AR 10-87, *Army Commands, Army Service Component Commands, and Direct Reporting Units*. The INSCOM G-35 CM serves as the Army proponent of the CI and HUMINT collection management architecture in support of information technology systems that execute Army CI and HUMINT collection requirements, operations management, and source administration functions.

Development of CHROME

In fiscal year (FY) 2012, the Defense Intelligence Agency (DIA) Directorate of Operations initiated the retirement of two legacy CI/HUMINT tools—HUMINT Online Tasking and Reporting (HOTR) and Source Operations Management Module—to execute the development of the CI and HUMINT Requirements, Reporting, and Operations Management Environment (CHROME). HOTR is on track to retire on or around the first quarter of FY 2022.

Since then, the Army G-2X Counterintelligence, Human Intelligence, Security and Disclosure Directorate, known as DAMI-CD, and the INSCOM G-35 CM represented Army end-user requirements in the development of the CHROME tool. The INSCOM G-35 CM supports CHROME-based functional control boards, in-process acceptance testing, user studies, and system reviews. Additionally, INSCOM collection requirements managers pioneered the use of CHROME by publishing their evaluations exclusively via the CHROME Collection Requirements Management (CRM) widget since FY 2017.

CHROME is an interoperable, synchronized information technology architecture that will accelerate workflow, increase efficiency, and broaden intelligence sharing within the Department of Defense (DoD) and across the intelligence community. CHROME was developed on both the SECRET Internet Protocol Router (SIPR) and the Joint Worldwide Intelligence Communications System (JWICS) networks. It provides access to all Collection Operations Management (COM), CRM, and Source Operations Management (SOM) widgets. It also provides access to CHROME CI programs, which include Force Protection Detachment, Supply Chain Risk Management, Technical Surveillance Countermeasures, Defense Critical Infrastructure Protect, Foreign Visits, and CI Name Checks/Records Check widgets, as well as the search engine CORE-Discovery, under one single logon capability.

The INSCOM G-35 CM is the lead for the support and planning of all collection elements operating under Army Executor Authorities and Army Production Centers transitioning to CHROME. The INSCOM G-35 CM led the Army functionality test of CHROME tools, which took place in the first quarter of FY 2021. The CHROME functionality test served as an exercise to ensure the CHROME widgets and system are able to execute CRM, COM, and SOM functions aligned with Army end-users' duty descriptions, user roles, and classification criteria, and feed into intelligence community repositories. The INSCOM G-35 CM is equipping Army units with the information necessary for a seamless and successful transition by providing basic considerations needed for users to transition from HOTR to CHROME.

What CHROME Users Will Need

CHROME general users will need to have—

1. SIPR access.
2. SIPR token. (A SIPR token/certificate is required to log in to CHROME.)
3. Field reporter number.
4. Public key infrastructure (PKI) information that is registered in DIAS at https://dias.dia.smil.mil.
5. A registered account at https://chrome.dse.dia.smil.mil/owf/. When registering, users should ensure they identify their organizational unit under *Agency. Once registered, all CHROME users have automatic access to CORE-Discovery.

CHROME collectors, collection managers, and analysts will need to follow steps 1 through 5 for general users (shown above). Additionally—

6. Collection managers must know the name of their CHROME executive administrator. The CHROME executive administrator is likely their organization's HOTR organizational coordinator. The CHROME executive administrator will assign the collection managers' roles and permissions under their organization's hierarchy.
7. Collection managers must build the workflow for their organization. Collection managers will need to identify administrative functional managers.
8. Collectors and analysts must contact their organization's collection manager to assign their roles and permissions (COM and CRM) in CHROME once they have access to CHROME. Military intelligence brigades-theater and Army Service component commands executing CI and HUMINT collection under DoD/combatant command (CCMD) executor authorities will fall under their respective CHROME CCMD hierarchy.

CHROME Education

CHROME education is available via JWICS on the DIA Academy website. CHROME end-user manuals and user training videos are available under the Documents tab on the official SIPR CHROME help desk located on I-Space (SIPR) and R-Space (JWICS).

For information on the CHROME transition, contact the CHROME INSCOM CM executive administrators by SIPRNet email usarmy.belvoir.inscom.list.ag2x-osd-cm1@mail.smil.mil, or call 703-706-1660, 703-706-1082, or 703-706-1759.

Ms. Aline Sutton is the U.S. Army Intelligence and Security Command G-35 Collection Management Chief. She has an extensive background in collection management information technologies and systems and in training, enforcement, resourcing, and strategic planning. She is a subject matter expert in counterintelligence (CI) and human intelligence (HUMINT) collection operations management, collection requirements management, and the CI and HUMINT Collection Management Architecture, with over 15 years' experience in CI and HUMINT collection management systems and tools.

Doctrinal Proficiency and Doctrinal Assistance

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

- Answer -

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

Want to be in the doctrinal know?

USAICoE doctrine maintains an email notification list to announce —

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

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

Awards For Excellence in Military Intelligence

Due to the coronavirus disease 2019 restrictions in June 2020, the awards ceremony for the 2020 MI Corps Awards was postponed. Conditions permitting, the following four awardees will be honored during a combined 2020/2021 awards ceremony currently planned for 25 June 2021.

Captain Kevin N. Hoerold
2020 Recipient of the
Lieutenant General Sidney T. Weinstein Award
For Excellence in Military Intelligence

The Military Intelligence (MI) Corps created the Lieutenant General 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 Kevin Hoerold graduated from Norwich University in 2013 as a distinguished military graduate and received a commission as a second lieutenant in military intelligence (MI). After completing the MI Basic Officer Leader Course, he was assigned as the assistant intelligence officer for 1st Battalion, 503rd Infantry (Airborne), 173rd Infantry Brigade Combat Team (A), at Caserma Ederle, Vicenza, Italy. In 2014, he participated in the initial deployment of United States forces to the Baltic States, serving as the senior intelligence officer in Latvia.

From 2015 to 2017, CPT Hoerold served as assistant intelligence officer for 1st Battalion, 75th Ranger Regiment, at Hunter Army Airfield, Savannah, Georgia. Deploying twice as a senior targeting officer in a joint special operations task force, he enabled direct action raids and other kinetic operations across Afghanistan. His efforts and results were recognized by the highest levels of the national security apparatus, prompting his selection for immediate continued service in the 75th Ranger Regiment.

After graduating from the MI Captains Career Course in 2018, CPT Hoerold was assigned as the senior intelligence officer of the 1st Battalion, 75th Ranger Regiment. On his third deployment to Afghanistan, he served as J-2 for a joint special operations task force. His efforts culminated in the collapse of an Islamic State contingent in western Afghanistan and the removal of the most senior members of ISIS in the Khorasan Region.

On his fourth and fifth combat deployments to Afghanistan, CPT Hoerold led a team of more than 100 joint and interagency partners to directly enable the removal of more than 1,600 enemy combatants and dozens of high-value individuals. Most significantly, his ability to lead his joint intelligence team, while incorporating international partner agencies, resulted in the mitigation of multiple threats to the United States. He built a network that enabled cross-agency communication and provided the cornerstone for the U.S. Government as it managed peace negotiations with the Taliban.

CPT Hoerold is currently the MI company commander in the Regimental Military Intelligence Battalion of the 75th Ranger Regiment.

CPT Hoerold's awards and decorations include the Bronze Star Medal, Meritorious Service Medal, Joint Service Commendation Medal with "C" Device, Combat Action Badge, Senior Parachutist Badge, and Ranger Tab.

Chief Warrant Officer 2 Evan Beeson
2020 Recipient of the
Chief Warrant Officer 5 Rex Williams Award
For Excellence in Military Intelligence

The Military Intelligence (MI) Corps established the Chief Warrant Officer 5 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 Evan Beeson is a native of Birmingham, Alabama. In 2002, he enlisted in the U.S. Army as a military occupational specialty (MOS) 96R (Ground Surveillance Systems Operator). Five years later, he reclassified to MOS 33W (now 35T) (Military Intelligence [MI] Systems Maintainer and Integrator). As a staff sergeant, he led the 719th MI Battalion to win the Army Award for Maintenance Excellence for fiscal year 2012.

In 2014, SSG Beeson was appointed to the rank of warrant officer as a MOS 353T (MI Systems Maintenance and Integration Technician). The following year, he was assigned to the 303rd MI Battalion and deployed to Afghanistan in support of Operation Resolute Support where he was the primary Intelligence and Electronic Warfare (IEW) technician for Task Force Observe, Detect, Identify, and Neutralize (ODIN). His duties included signals intelligence prime mission equipment readiness for three RC-12X Guardrail Common Sensor (GRCS) aircraft, nine associated Datalink antennas, and three Operational Ground Station (OGS) data transport systems on three sites manned by eight MOS 35T personnel. Despite having no formal OGS architecture training, he enabled Task Force ODIN to conduct its first multi-aircraft Communications High Accuracy Airborne Location System sorties in Afghanistan and the first airborne relay sorties in 5 years. He was also instrumental in deploying the Remote Tactical Common Datalink relay at Forward Operating Base Lightning, increasing GRCS theater coverage by 20 percent and enabling more than 200 aerial missions that provided critical signals intelligence support to a new region.

After an assignment with the 163rd MI Battalion, CW2 Beeson became the IEW maintenance technician for the 297th MI Battalion, 513th MI Brigade (Theater), in June 2019. He has servicing responsibility for more than 400 Distributed Common Ground System components and collection sensors spread through the Army Central Command area of responsibility. He created the brigade's first IEW Sustained Readiness Model training initiative and fully integrated the Global Combat Support System (GCSS) into IEW sustainment efforts. His initiative significantly increased awareness, decreased misinformation regarding system readiness, and provided instant feedback to commanders. He trained 18 MOS 35Ts in his section on GCSS and its integration with sustainment and logistics channels to enable unity of effort. A graduate of the Digital Intelligence Systems Master Gunner (DISMG) Course, he also serves as a DISMG instructor.

CW2 Beeson's awards and decorations include the Meritorious Service Medal (2 Oak Leaf Clusters), Army Commendation Medal (5 Oak Leaf Clusters), Army Achievement Medal (6 Oak Leaf Clusters), Good Conduct Medal (5 awards), numerous service ribbons, two NCO Professional Development Ribbons, Combat Action Badge, Air Assault Badge, and Knowlton Award.

Sergeant Antatenique Avila
2020 Recipient of the
Command Sergeant Major Doug Russell Award
For Excellence in Military Intelligence

The Command Sergeant Major Doug Russell Award was created in 2001 in honor of an esteemed noncommissioned officer (NCO) who personified the integrity, moral courage, and loyalty espoused in the NCO Creed. CSM 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 Military Intelligence Corps.

SGT Antatenique Avila was born and raised in Leadville, Colorado, where she graduated from Battle Mountain High School in 2012. She received two bachelor of arts degrees, in English and in psychology, from Colorado State University-Pueblo in 2016. Shortly after graduating, she enlisted in the U.S. Army as a military occupational specialty (MOS) 35N (Signals Intelligence [SIGINT] Analyst). Following basic training in Fort Sill, Oklahoma, she completed 6 months of Advanced Individual Training (AIT) at Goodfellow Air Force Base, Texas. During AIT, she volunteered for Airborne School and earned her Parachutist Badge. In September 2017, she was assigned to Delta Company, 307th Airborne Engineer Battalion, 3rd Brigade Combat Team, 82nd Airborne Division, Fort Bragg, North Carolina.

After receiving her promotion status in October 2018, Avila attended the Basic Leader Course, during which time she competed in the Iron Warrior Competition. She also supported three battalion-level and one brigade-level joint forcible entry operations and was the first paratrooper in U.S. Forces Command to conduct a static-line jump with the new HPACK SIGINT system and rucksack, both weighing more than 70 pounds. SGT Avila's efforts were instrumental in developing the standard operating procedure for HPACK airborne employment. In January 2019, she began an intense and demanding series of MOS training, completing 10 SIGINT courses in just over 6 months. This training prepared her and her platoon for their deployment in support of Operation Freedom's Sentinel in Afghanistan. She was promoted to sergeant in June 2019, 4 months before her 3-year time-in-service mark.

In Afghanistan, SGT Avila serves as the noncommissioned officer in charge (NCOIC) for SIGINT operations for 5-73 Cavalry Squadron Task Force Panther Recon at Camp Dwyer and as a senior cryptologic analyst in the Train, Advise, Assist Command-South. She also oversees the daily duties of eight contracted linguists. As a threat reporting analyst, she analyzed thousands of lines of analytical data in support of collection and analysis priorities, enabling the CJ2 SIGINT section to successfully execute more kinetic strikes in 4 months than the previous leadership executed in 18 months. Her efforts led to the removal of 10 high-value individuals, the dissemination of threat indicators and warnings, and the creation of hundreds of target development packets. Additionally, as a Level II Army Combat Fitness Test (ACFT) NCOIC, SGT Avila helped instruct and certify more than 115 graders and officers in charge/NCOICs downrange, preparing all Army units throughout the Combined Joint Operations Area-Afghanistan for the implementation of the new ACFT in fiscal year 2021.

SGT Avila's awards and decorations include the National Defense Service Medal, Afghanistan Campaign Medal, Global War on Terrorism Service Medal, Army Service Ribbon, two Certificates of Appreciation, and Parachutist Badge. She is pursuing a civilian master of professional studies in cybersecurity analytics and operations.

Mr. William J. Grimshaw
2020 Recipient of the
Ms. Dorothe K. Matlack Award
For Excellence in Military Intelligence

In 2018, the Military Intelligence (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.

Mr. William Grimshaw enlisted in the U.S. Army in 2003 as an all-source intelligence analyst. He began supporting U.S. Army counterintelligence in 2004 as a contracted all-source analyst and joined the U.S. Army Intelligence and Security Command (INSCOM) as a Department of Army Civilian counterintelligence special agent in 2006. He served as an analyst, staff officer, and project officer for strategic projects and deployed to Afghanistan in 2009 in support of the International Security Assistance Force.

Mr. Grimshaw joined the 310th Military Intelligence Battalion in October 2015 and served in roles of progressive responsibility, including team leader, branch chief, and operations officer. He was responsible for teams comprised of Soldiers, Civilians, and contractor staff of diverse backgrounds and expertise, conducting counterintelligence collection and reporting in support of priority Army, Department of Defense (DoD), and intelligence community requirements. His teams' reporting made significant contributions to the force protection of Army and DoD personnel in contingency areas and the protection of sensitive Army information, personnel, systems, and facilities worldwide and generated positive feedback from all echelons of DoD.

Mr. Grimshaw recently concluded 19 months of service as Director of Operations for an office conducting counterintelligence collection and reporting. In addition to maintaining daily operations supporting the Army and a wide range of combatant commands and defense agencies, he provided the technical expertise that enabled a transformation of the organization to meet the vision of the INSCOM commanding general and drive new capabilities on behalf of the U.S. Army. Mr. Grimshaw oversaw the successful planning, staffing, and initial implementation of new mission authorities, task organization, specialized equipment, and personnel. He maintained continuity of operations and leadership through a period of substantial personnel turnover and navigated the organization through significant areas of lacking or outdated policy guidance. He recently reported to his next assignment with the Army Deputy Chief of Staff for Intelligence, G-2.

Mr. Grimshaw successfully completed advanced government and commercial intelligence, counterintelligence, management, and information security training courses. The DoD and the former National Counterintelligence Executive recognized him for his individual and team achievements. He holds a bachelor of science in foreign service from Georgetown University.

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

by Ms. Beth Leeder

Training Is a Journey, Not a Destination

The U.S. Army Training and Doctrine Command (TRADOC) Commanding General, GEN Paul E. Funk II, has a list of 40 "Funk's Fundamentals," and number 38 on that list is "Training is a journey, not a destination." Nowhere in the Army is this more evident than with the Army Reserve and the National Guard. This Training Readiness column will explore the journey involved in training our Army reservists.

One Army School System

TRADOC Regulation 350-18, *The Army School System (TASS),* and AR 350-1, *Army Training and Leader Development,* direct that in-service reclassification (military occupational specialty [MOS]-transition) must use Reserve Component schools when a Total Army Training System course is available. By using existing training infrastructure and resources, the One Army School System (OASS) provides for efficient institutional training across all Army training institutions. It eliminates the need for mobile training teams and requires that certain courses be phased and scheduled back-to-back at select training institutions.

The OASS enables Soldiers to receive standardized training across all three components using the same program of instruction, including the Noncommissioned Officers Academy. It optimizes the institutional training capacity and allows active duty enlisted Soldiers to attend National Guard and Army Reserve schools to obtain their MOS-transition qualifications and professional military education training. The training encourages attendees to gain a better understanding of the mission sets across all three components. An added benefit is the reduction in temporary duty costs and all components are represented.

The Commanding General of the U.S. Army Intelligence Center of Excellence (USAICoE), as the military intelligence (MI) proponent, has responsibility for the oversight of intelligence institutional training in various locations. These consist of Army National Guard training at the 4th MI Battalion, 640th Regional Training Institute at Camp Williams, Utah; and the 1st MI Battalion, 122nd Regional Training Institute, at Camp Clay, Georgia. The USAICoE oversight also includes the Army Reserve training at the 4th MI Brigade, 102nd Training Division, co-located at Fort Huachuca, Arizona, under the OASS. The Army's goal is course standardization and equivalency regardless of which component teaches the course. The USAICoE Deputy Commanding General for the Army Reserve oversees Reserve Component training by chairing the Reserve Component quarterly training reviews. The Reserve Component Branch within the Training Development and Integration Division, Directorate of Training, is responsible for ensuring standardization of the training curriculum at the three Reserve Component training locations. Currently, LTC Angel Parish is the branch chief, and she is supported by three Soldiers. Additionally, the branch supports the Reserve Component MI Captains Career Course (MICCC) at USAICoE.

The Courses

USAICoE courses that the National Guard and Army Reserve currently teach include—

- Intelligence Analyst 35F10 and 35F Advanced Leader Course (ALC).
- Geospatial Intelligence Imagery Analyst 35G10 and ALC.
- Counterintelligence Agent 35L10 and ALC.
- Human Intelligence Collector 35M10 and ALC.
- Signals Intelligence (SIGINT) Analyst 35N ALC.
- SIGINT Voice Interceptor 35P ALC.
- Noncommissioned Officer Senior Leader Course (SLC).

The 4th MI Brigade, 102nd Training Division, supports 35F, 35N, 35G, 35M, 35L, and SLC. The Camp Williams Regional Training Institute supports 35M, 35F, 35L, 35P, and SLC. The Camp Clay Regional Training Institute supports 35F and 35M courses. The 304th MI Battalion at Fort Huachuca conducts the Reserve Component MICCC instruction.

All USAICoE courseware is within one version of active Army material, with updates occurring once a year. The Reserve Component branch works with the active courses throughout the training development process to determine how to condense the active duty course length to fit the reserve model. USAICoE's Quality Assurance Office inspects each Reserve Component training site every 3 years using the same Army accreditation standards that apply to USAICoE. The quarterly training reviews allow the three training sites to update the proponent on the unit's instructor certification status summary, list upcoming key events, highlight recent successes, and identify issues that need the proponent's assistance.

Time Issues and the Validation Process

There are unique challenges to training our reservists, one of which is time—time to train and time to get the curriculum to the reserve schoolhouses. The basic model you are probably most familiar with for reservist training is 2 days per month and 2 weeks per year. This is known as the battle assembly weekend or drill, and 2 weeks of annual training that is spent working on the operational mission set of the unit. The Army Reserve will usually fill up the weekend with required Army training, such as the AR 350-1 and mission essential task list training. If the unit is mobilizing or deploying, the training will focus more on the unit mission, but the Army training must still be completed. The OASS MOS-transition and Noncommissioned Officer Professional Development System courses are developed in phases that allow Army Reserve and National Guard Soldiers to complete the training in chunks. The only guideline is that they have to complete all the phases within 19 months of the initial start date. This is not always an easy thing to do. For example, the 35M10 active course is 93 days/770 hours, whereas the Reserve Component MOS-transition course is 66 days/660 hours and is taught in two phases. In order to fit the Reserve Component training timeline, the Intelligence Soldier Field Craft (think, Field Training Exercise) was removed from the reserve course and the repetitions of practical exercises were reduced. The essential training, including assessments and terminal and enabling learning objectives, remains the same. Additionally, a training week in the Reserve Component is 6 days at 10 hours per day, and the Active Component trains 5 days at 8 hours per day.

The other time issue pertains to the validation process. After the Reserve Component Branch completes training development work on the Reserve Component curriculum, the National Guard Bureau and the U.S. Army Reserve Command must review/concur with the resulting program of instruction. They have 60 days to complete their review and provide memorandums of concurrence or nonconcurrence. These memorandums are included in the documents submitted to TRADOC Headquarters for validation.

The program of instruction identifies the Reserve Component course resources (for example, equipment and instructor-to-student ratios). Concurrences from the National Guard Bureau and U.S. Army Reserve Command are an acknowledgment of the funding that needs to be in the Program Objective Memorandum. If a resource is increased, it will not be available for use until the execution of the Program Objective Memorandum, i.e., 3 years from validation of the program of instruction.

Finally, students face some unique training readiness challenges. It is important for Reserve Component and National Guard units to proactively prepare students to attend training. Units can do this by ensuring that the paperwork has been submitted for the security clearance level students will need. Units can also identify those students who require extra help with writing and send them to https://libicoe.army.mil to take advantage of the writing self-development courses. Additionally, they can stay current on training prerequisites and requirements. For example, beginning next year, MOS 35M (Human Intelligence Collector) students must attend the Defense Language Institute before starting their 35M training.

Conclusion

The OASS is the essence of one team, one fight. The mission of the Reserve Component branch at Fort Huachuca is to ensure that the Army Reserve, National Guard, and regular Army MI Soldiers have the same training across the board to maintain the highest standards in training and education and produce MI Corps professionals capable of maintaining information superiority to win the Nation's wars.

Intelligence, Information, Cyber, Electronic Warfare, and Space in the New World Order

by Mr. Chet Brown, Chief, Lessons Learned Branch

Birds of a Feather Flock Together

Animals provide us with a host of lessons learned. My favorite is from a passage in Rudyard Kipling's *The Jungle Book,* "For the strength of the pack is the wolf, and the strength of the wolf is the pack,"[1] displayed on a challenge coin bestowed on me by a now retired all-source intelligence technician chief warrant officer. Every wolf has a role in ensuring the pack's success, and each role is different. These diverse roles deliver a united effort that applies to the Army's newest formation—the Intelligence, Information, Cyber, Electronic Warfare, and Space (I2CEWS) battalion. We do more when operating together than we are able to do alone. This is exemplified by the various roles Soldiers perform when operating in a squad. Each Soldier is a wolf—loyal, committed, and deadly. However, history reveals that in the modern era, wolves cannot survive, much less thrive, without the support and intervention of other creatures that are not wolves.

Leaders prepare their subordinates to operate in their stead, accepting that every individual is replaceable but the function they perform is not. Every military occupation is essential and interdependent with every other occupational specialty in achieving tactical mission success. This is also true of the I2CEWS formations.

The separate fields of intelligence, information, cyber (signal), electronic warfare (EW), and space are employed individually within cylinders of excellence in support of various functions. Similar to the individual wolf, the power of differing individual enablers is multiplied when employed together in the I2CEWS battalion pack. Allow me one more quote, a proverb this time, to underscore the synergy realized by the comprehensive and collaborative employment of the I2CEWS capabilities in multi-domain operations within large-scale combat operations: "If you want to go fast, go alone. If you want to go far, go together."[2]

Ambiguous Boundaries

Ambiguous boundaries exist between planning, preparing, training, and conducting each separate I2CEWS function. Where does military intelligence (MI) stop and cyber begin? When does information become intelligence? Who coordinates Army Space support to operations for the other I2CEWS elements? The answers are neither clearly delineated nor specified in a single authoritative doctrinal reference. The U.S. Army Cyber Center of Excellence (USACCoE) is the proponent for signal, cyber, and EW. MI used to have proponency for EW, fielding organizations in which MI Soldiers performed EW operations. The U.S. Army Intelligence Center of Excellence (USAICoE) is the

proponent for intelligence, which includes the signals intelligence (SIGINT) collection discipline. While I'm not old enough to have served as an "Old Crow" in the Army Security Agency, I was an "EWok" performing both SIGINT and EW in an EW platoon, Company C, 109th MI Battalion (Combat Electronic Warfare Intelligence [CEWI]), 9th Infantry Division (Motorized).[3]

ATP 3-19.94, *Techniques for the Multi-Domain Task Force*

This new Army techniques publication (ATP) is under development by the U.S. Army Fires Center of Excellence. The purpose of ATP 3-19.94 is to describe the role, organization, and capabilities of the Multi-Domain Task Force (MDTF). It will primarily focus its discussions on the non-prescriptive ways the commander and staff will perform the missions, functions, tasks, and roles of each warfighting function in support of the MDTF. Included in the discussions is the I2CEWS Battalion. The Fires Center of Excellence expects to conclude critical exercises, ensure the publication nests with FM 3-0, *Operations,* and incorporate all feedback into a final draft of the ATP in late summer/early fall 2021.

While "EWok" was intended as a pejorative nickname the unit ground surveillance platoon members bestowed upon the SIGINT Soldiers, the SIGINT Soldiers embraced it as a recognition of the tactical field craft and operational skills needed to survive combating a numerically superior enemy. The EWoks operated both SIGINT and EW systems when training on the portion of Joint Base Lewis-McChord, Washington, formerly known as Fort Lewis. Practical application of both SIGINT and EW was routine during battalion-sized force-on-force exercises at the training center in Yakima, Washington, and while operating as a brigade-sized opposing force against a U.S. light infantry division's certification exercise at Fort Hunter-Liggett, California. A key lesson learned was the laws of physics dictated that the EWoks could do either SIGINT or EW, but never both at the same time. Well-camouflaged, effectively emplaced SIGINT system passive operations were immediately compromised when the jamming of enemy communications commenced. SIGINT elements were able to mitigate transforming from a passive to an active signature when using radio transmissions to report on enemy activity. Mitigation measures included using terrain-masking and field-expedient directional antennas (built and rehearsed during home station training), and employing brevity codes in very short transmissions. Unfortunately, the initiation of EW operations increased the electromagnetic signature a hundredfold. Like their *Star Wars* namesakes, the Charlie Company "EWoks" felt more secure operating as denizens of the misty, dense ferns and pines surrounding Rogers Drop Zone, performing only SIGINT missions, rather than in the dry, sparsely vegetated environments of Yakima and Hunter-Liggett where an enemy can easily detect, identify, and engage EW systems.

I Can See Clearly Now the Rain Has Gone[4]

I'm sure it's still raining at Joint Base Lewis-McChord. However, the Cyber, EW, Fires, Intelligence, and Space Centers of Excellence Lessons Learned elements are working together to clear away some of the fog and mist obscuring the authoritative and proponent lanes of the differing I2CEWS functions. Some of you may be wondering how Fires entered this discussion because it is not even in the I2CEWS acronym. The answer lies in something a general officer said when making a plea for MI personnel to revise their situational understanding and purpose: "Intelligence supports fires; fires drives maneuver." When I first heard the general's comment, I thought, "Nope. That's wrong." Luckily, I kept my mouth shut at the time but sought confirmation from several others immediately after the Leader Professional Development session. "Did he really say that? Does he not know that *intelligence drives operations?*" It took me a while to appreciate the intent behind the general's statement. The general was identifying and describing an actual paradigm shift to us. What he said tied to the purpose of the (then) newly established MDTF formation. Reading (and re-reading) FM 3-0, various MDTF concept writings, exercise after-action reports, and our own firsthand lesson learned observations reveals the initially unappreciated wisdom of the general's statement. The general's clarion call of the reordered priority of MI Soldier support addresses the antiaccess and area denial (also known as A2AD) conditions we will face across multi-domain operations within large-scale combat operations. The MDTF has matured since the general's comment. In addition to refining tactics, techniques, and procedures of the various elements, the MDTF gained an I2CEWS battalion. "Don't even think about calling it a CEWI battalion" was the advice of multiple capability developers when discussing the emerging formation.[5]

Like most people, I initially resist change. Take away my M-1911 pistol and give me an M-9 pistol in its place? No, thank you. Now I hear we're moving back to the venerable .45 ACP. Eliminate my rifle's capability to fire full auto by limiting me to burst? Doesn't seem smart to take away a capability that might be needed. Oh, full auto is back? Good. Put an EW jammer on the same platform as SIGINT collection. We tried that before, and I wasn't too keen on being one of the Soldiers on the team tasked to perform both functions at the tactical level. With an assumed (urban myth?) large-scale combat operations life expectancy of 7 seconds after switching from listening to jamming, no one was happier

than the tactical-level EWoks when the U.S. Navy and U.S. Air Force assumed airborne jamming in support of ground operations. Let the communist artillery formations try to take out a grid square when the jammer is moving at hundreds of miles an hour at thousands of feet over the battlefield. Not to mention that the power of a turbofan engine running an EW transmitter greatly exceeds what a ground vehicle slave cable or generator can provide. Even if we were to change the meaning of the letter C from *combat* to *cyber*, CEWI is out, and I2CEWS is in.

U.S. Air Force photo

A General Dynamics EF-111A Raven at the National Museum of the U.S. Air Force in Dayton, Ohio. The EF-111A Raven, known affectionately as Fat Tails and Spark Varks (the F-111 is known as the Aardvark), served as tactical electronic jamming aircraft in the 1980s and 1990s.

We've Been Saying It Wrong All Along

What other terms must we revise to reflect the new world order? I made a mistake. I meant to say new *word* order, not new world order. The technological advances that necessitated multi-domain operations and led to the creation of I2CEWS also drive a change to the Army's axiom of "shoot, move, communicate." We've heard this phrase a bajillion times in our careers. Say it with vigor: *"shoot, move, communicate!"* How many of you just recited the double-time cadence in your head, ending with the obligatory "bang-bang." It's okay, I did it. We've been saying "shoot, move, communicate" in the wrong order. Our profession has corrected inaccurate word order for other Army slogans or mnemonics. Initially, I didn't like the change from OCOKA to OAKOC.[6] However, rearranging the letters in the order of tactical importance makes sense. The same reasoning applies to shoot, move, communicate. This isn't my idea. The credit belongs to my colleague Mr. Rick San Miguel, the USACCoE Lessons Learned government lead. He recommends the reordering of shoot, move, communicate to better align with the manner in which we will conduct multi-domain operations. The revision also corresponds to each of the phases and across all domains of unified land operations. While the order in which we currently sing the cadence is more rhythmic, the new word order provides a more logical sequence of the traditional exuberant exclamation "communicate, move, shoot…bang-bang!" I hear the reluctant acceptance of *communicate* being the first operation, but there is probably still some resistance to the order of move and shoot. Bear with me as I explain.

Communicate. We (the Army) are an orders-based profession and culture. We don't unilaterally decide to initiate combat operations. To do so would be illegal as well as putting the cart before the horse. Every operation begins with some type of an order. After receiving an initial order, we continue operations as directed upon receipt of other orders (WARNO, FRAGO,[7] etc.) or take appropriate action (within the commander's intent) in the absence of orders. It's logical then to declare that "communicating" is the first task in implementing an action. Regardless of which method a leader employs (for example, verbal, text, graphic, or visual), communicating the order will always be the first action.

Move. Once our leaders tell us to begin, we have to go somewhere to do it. Whether we physically move units across the physical domains or enter a few keystrokes to navigate within cyberspace, we move to operate within the boundaries of the associated domains. Only after we arrive at our area of operations can we can begin shooting. This may involve putting steel on target or firing electrons across physical or information dimensions.

Shoot. In the midst of these recent changes to the way we operate, a key principle remains intact: the first engagement is always the reconnaissance/counterreconnaissance (recon/counterrecon) fight. Reconnaissance forces seek to gain information on their adversaries, and correspondingly, adversaries seek to thwart us from collecting and communicating information or intelligence. Sometimes the "fight" portion of recon/counterrecon engagement involves the physical effects of munitions, smoke, or decoys. Other times it may involve communications deception, EW, or information

operations (including misinformation or disinformation). The modern multi-domain operations engagement shoot function could involve a trigger, a lanyard, a keypad, a dial, or all simultaneously. This is only a slight shift from legacy Cold War tactics and techniques in which forces used electrons in communicating, moving, and to a limited extent, "shooting" electrons in electronic countermeasures (jamming). Current and future engagements will see differing types of shooting in each of the domains in all phases of operations. The modern and future multi-domain operations recon/counterrecon fight will involve cyber, EW, and information effects, with the last category attaining a level of importance unheralded until now.

Information Convergence and Information Dominance

Information Advantage Enables Decision Dominance

Gaining and maintaining the initiative during competition, crisis, and armed conflict largely depends on a commander's ability to attain an Information Advantage. Maintaining this advantage contributes to decision dominance by enabling superior situational awareness by sensing, understanding, deciding, and acting faster and more effectively than an adversary. How does the Army effectively employ doctrine that enables capabilities, techniques, and activities across all dimensions of the operational environment to gain and maintain the Information Advantage that enables Decision Dominance?[8]

As the Army refines a conceptual framework that is the foundation for information advantage, the USAICoE Lessons Learned team wonders who is ensuring that lessons and best practices are discovered and applied to Army doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF–P)? Each of the Army's six warfighting functions depends upon, and assumes, we will have an information advantage over our adversaries.

Which one of the I2CEWS force modernization or branch proponents (AR 5-22, *The Army Force Modernization Proponent System*) ensures we are discovering, validating, and integrating pertinent lessons and best practices? Is there a central coordinating authority across the multiple domains and proponents? At the Army and centers of excellence level, the answer is yes. The Center for Army Lessons Learned ensures the cross-function, multiple center of excellence, or branch proponent integration of lessons learned requiring action within DOTMLPF–P.

Lessons Learned Support for I2CEWS Soldiers

The Army's current lessons learned enterprise lacks a comprehensive unified I2CEWS ***Soldier-level*** lessons learned exchange venue. Differing I2CEWS proponent organizations unilaterally discover, validate, integrate, and assess lessons learned from MDTF and I2CEWS training and exercises. Each of the I2CEWS lessons learned proponents routinely shares lessons and best practices with each other, but these exchanges rarely make it down to the Soldiers in the operating force. To address this short-term challenge, one action taken by the Cyber, Intelligence, Fires, and Space Centers of Excellence was to establish an online forum to identify, discuss, and exchange I2CEWS lessons learned and best practices with Soldiers and leaders conducting I2CEWS operations.

I2CEWS Lessons Learned Forum

USAICoE volunteered one of its monthly MI Lessons Learned Forums to serve as the inaugural I2CEWS Lessons Learned Forum. This was an easy decision for us because the forum's purpose nests within the fiscal year (FY) 2021 training guidance priorities specified by Desert 6, USAICoE Commanding General MG Anthony R. Hale:

- Objective 1: Build Leaders.
- Objective 2: Drive Change.
- Objective 3: Inform.

The premier I2CEWS Lessons Learned Forum on 18 February 2021 leveraged the intent specified in objective 2 of the FY 2021 training guidance—to drive change "through efforts which are inclusive and collaborative, sharing of best practices with other [centers of excellence] COEs, and ensuring we look externally across the Army."[9]

We developed and conducted the first I2CEWS Lessons Learned Forum to capitalize on these assumptions:

- Rapidly sharing I2CEWS lessons learned information provides an information advantage and supports decision dominance for I2CEWS and MDTF training, planning, preparation, and readiness.
- Increased I2CEWS and MDTF Soldier readiness supports multi-domain operations.
- I2CEWS lessons learned exchanges support a culture of learning and Army readiness by helping to build leaders, drive change, and inform those preparing to conduct multi-domain operations.

Time for the I2CEWS Herd to Be Heard

We consciously strive to keep the lesson and best practice exchanges limited to current conditions and I2CEWS lessons learned from the past several years. While we have identified and integrated EW lessons from the era of CEWI battalions and the past several years of MDTF involvement in warfighter exercises, our focus is on what I2CEWS

U.S. Army photo illustration

The Army is looking to incorporate the Electronic Warfare Planning and Management Tool in the military decision-making process.

Soldiers are learning and applying today. Our first set of firsthand I2CEWS operator lessons learned originates with the I2CEWS battalion's MI company commander. The commander has compiled lessons and best practices from the initial MDTF exercise to the present. These lessons and best practices form the centerpiece of the first I2CEWS Lessons Learned Forum. To participate, contact your respective branch or proponent organizational lesson manager to receive participation instructions. We look forward to the opportunity for the I2CEWS herd to be heard.

Endotes

1. Rudyard Kipling, *The Jungle Book* (London: Macmillan, 1894).

2. The source of this saying is unclear. Some believe it may be an African proverb.

3. The term Ewok comes from the *Star Wars* trilogy. Ewoks first appeared in the 1983 film *Return of the Jedi* and are a fictional species of small, furry mammaloid bipeds. They inhabit the forest moon of Endor and live in various arboreal huts and other simple dwellings. Wikipedia, s.v. "Ewok," last modified 28 January 2021, 05:08, https://en.wikipedia.org/wiki/Ewok#Return_of_the_Jedi.

4. Johnny Nash, "I Can See Clearly Now," *I Can See Clearly Now,* Epic, originally released in 1972.

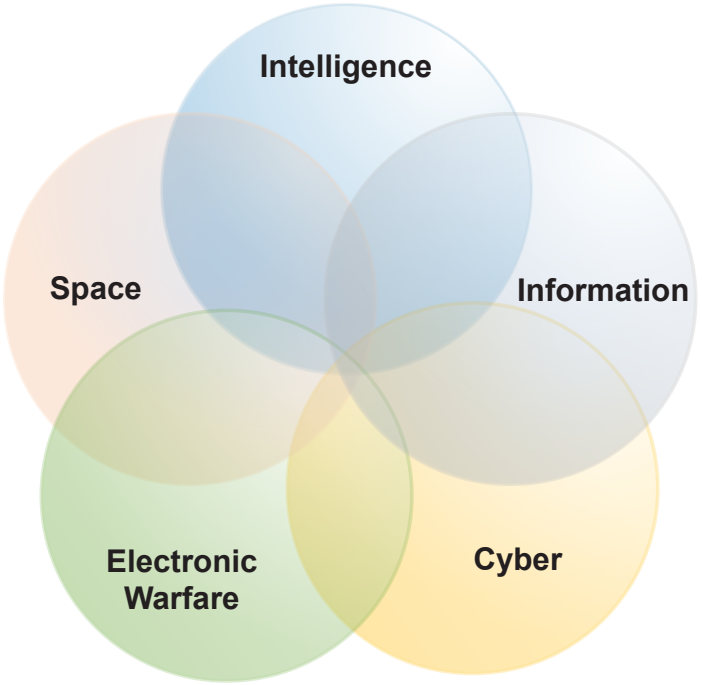
5. The combat electronic warfare and intelligence, or CEWI, battalion dates back to 1976. The first of these was the 522nd Military Intelligence (MI) (CEWI) Battalion, formed at Fort Hood, TX, in 1976 and assigned to the 2nd Armored Division. Ruth Quinn, "522nd MI (CEWI) Battalion passes tactical intelligence test. April 7, 1977," U.S. Army Worldwide News, April 4, 2014, https://www.army.mil/article/123363/522nd_mi_cewi_battalion_passes_tactical_intelligence_test_april_7_1977.

6. The acronym OCOKA means observation and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach. "OCOKA Military Terrain Analysis," *Vicksburg National Military Park: Cultural Landscape Report* (Atlanta, GA: National Park Service, 2009), 242. OAKOC stands for observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, cover and concealment. Department of the Army, FM 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 27 February 2008 [obsolete]), 5-6.

7. Warning order and fragmentary order.

8. Department of the Army, *White Paper on Information Advantage and Decision Dominance* (working paper, U.S. Army Cyber Center of Excellence, Fort Gordon, GA, 2021).

9. Department of the Army, *U.S. Army Intelligence Center of Excellence (USAICoE) Training Guidance for Fiscal Year 2021 (FY21),* memorandum (22 January 2021).



by Mr. Kevin B. Gorski

China's sense of time beats to an altogether different rhythm from America's.

—Henry Kissinger

Introduction

In the future competitive continuum, the United States will face challenges from many nations into and beyond 2035. Of greatest concern is the need not only to recognize but also to envision the future adversarial potential of the People's Republic of China (PRC) and its ongoing significant national and military modernization efforts.

Under the current Chinese President, Xi Jinping, the PRC is implementing the great rejuvenation using Xi's slogan of *fuxing zhi lu*[1] (which roughly means "the road to renewal"). Included are national pride and the goal of demonstrating a "world class" military by December 2049, the 100th anniversary of the PRC.

Background

Chinese history is witness to centuries of strife and discord. The Qing dynasty is known for its initial prosperity and tumultuous final years, lasting from the mid-17th century until it was overthrown in 1912 after the Xinhai Revolution. The Republic of China, established in 1912, lasted until 1949 when Mao Zedong founded the PRC. Since Mao, the PRC embarked on a path to establish China as a global power in the 21st century, and the Chinese leaders and strategists are engaged in the "Hundred-Year Marathon,"[2] from 1949 to 2049. This strategy is a modernization effort across all aspects of the Chinese society, economy, and military that is intended to replace the United States and other world powers as the globally dominant nation by 2035.

PRC Leaders' Strategies over the Last 70 years

- **Mao Zedong (1949 to 1976)**—Created the "People's War" guiding principle for the People's Liberation Army (PLA), which focused on three strategies: imminent war, major war, and nuclear war.
- **Deng Xiaoping (1978 to 1989)**—Focused on "peace and development," including a PLA prepared to conduct "local war under modern conditions" of speed, mobility, and lethality.
- **Jiang Zemin (1989 to 2002)**—Assessed modern warfare after the first Gulf War and called for a "revolution in military affairs" based on the realization China was "ill-prepared" to address a Taiwan scenario.
- **Hu Jintao (2002 to 2012)**—Updated the Chinese military strategic guidance to "local war under modern, high-tech conditions," emphasizing joint cooperation and a move toward technology and the integration of "system-of-systems operations" referenced in the PLA Academy of Military Science document published in 2010.
- **Xi Jinping (2012 to present)**—In 2015, placed the PLA on a defining modernization effort across all branches of military operations, directing the PLA to win "informatized[3] local wars" and emphasizing "informational" (electromagnetic, space, cyberspace, and cognitive) and maritime domains, later including the air domain.[4] Subsequently, China's State Council Information Office published *China's Military Strategy,* driving the great national rejuvenation and the need for a strong military.

National Rejuvenation

PRC President Xi and Chinese Communist Party leaders are executing "national rejuvenation," targeting Chinese social stability, economic prosperity, and technology gains

that will ensure China dominates global affairs. The strategies direct the PLA to modernize, expand from regional concerns to a global response capable force, and dominate information, cyberspace, and space by 2049:

- **Military-Civil Fusion:** The result of the Military-Civil Fusion development strategy is a completely self-reliant defense industry.
- **One Belt, One Road:** The One Belt, One Road strategy, also known as the Belt and Road Initiative, employs foreign and economic policies to expand global transportation and trade links to improve China's economy and access to essential resources and technology.
- **Polar Silk Road:** Over the past decade, Chinese presence in the Arctic has steadily increased, centered on research and exploitation. There have been disputes in the "near-Arctic State," enforced by icebreaker vessels, the presence of trained military personnel, and the deployment of an extended integrated air defense capability.
- **Global Affairs:** PRC foreign policy will expand bilateral and multilateral military exercises and achieve an overseas presence that allows for enhanced relations with nations and their militaries.
- **Non-War Military Activities:** The period from 2021 to 2035 will emphasize humanitarian assistance and disaster relief, maintaining internal security, and maritime rights in the South and East China Seas. Additionally, PRC official writings describe aspects of Non-War Military Activities that advocate global PLA expansion—or a means to implement multi-domain operations, emphasizing recent advances in antiaccess and area denial capabilities.

Photo credit: jiulong by CC SA 2.0

China's People's Liberation Army flag raising parade in Kunming, China, December 29, 2007.

Conclusion

By 2049, the outcome of the national rejuvenation is a modern self-reliant defense industry, a world-class and globally responsive military force, and a national strategy capable of exerting dominance across multiple domains. In order to achieve this global goal, the current Chinese scientists' ideas and concepts will need to complete a transition as early as 2035 to 2040 of a modern military that is heavily reliant on advanced technology while still boosting significantly high numbers of available manpower. Ultimately, the future military will include the integration of advanced computing and artificial intelligence with robotics, advanced weapons, and biotechnological human enhancement, as well as the inclusion of new lunar materials to enhance armor, energy, and communication networks.

Epigraph

Henry Kissinger, "Face To Face With China," *Newsweek,* April 15, 2001, https://www.newsweek.com/face-face-china-150011.

Endnotes

1. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company, 2015).

2. Ibid. The Hundred-Year Marathon is a term coined by author Michael Pillsbury to describe China's strategy to supplant the United States as the world's dominant power. It is also the title of one of his books.

3. "Informatized" is the correct translation. It describes a process that involves acquiring, transmitting, processing, and using information to conduct joint military warfare.

4. Edmund J. Burke, Kristen Gunness, Cortez A. Cooper III, and Mark Cozad, *People's Liberation Army Operational Concepts* (Santa Monica, CA: RAND Corporation, 2020), 4–5, https://www.rand.org/pubs/research_reports/RRA394-1.html.

Moments in MI History

How Did We Get Here?
The U.S. Army Intelligence School Moves to Fort Huachuca (Part 1 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.
- Readying the New Home.

October–December 2021 issue

- 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 Story Begins at Fort Holabird

Post-World War II training for Army intelligence was scattered across the United States. Signals intelligence was the purview of the Army Security Agency (ASA), headquartered at Arlington Hall Station, Virginia, and with training at the ASA School at Fort Devens, Massachusetts. Combat intelligence training for officers and enlisted members began in 1946 in the Intelligence Division, Army General School, at Fort Riley, Kansas. These courses focused on training personnel for S-2 and G-2 staff positions at battalion, regiment, and division. Finally, Fort Holabird, a World War I–era quartermaster depot, became the location of the Army's Counter Intelligence Corps School as early as 1945. All three schools had roots in the lessons of World War II, when the necessity for professionally competent officers and enlisted personnel in all intelligence disciplines became clear.

In the 1950s, courses in field operations intelligence, geographic area studies, and industrial security were added to the curriculum at the Counter Intelligence Corps School at Fort Holabird. As the scope of intelligence training expanded at the Maryland post, MG Arthur Trudeau, the Assistant Chief of Staff for Intelligence (ACSI), who oversaw the Army's

U.S. Army photo

Students arrive for class at the Counter Intelligence Corps School, ca. late 1940s.

intelligence training efforts, directed the establishment of the U.S. Army Intelligence School there. Consequently, on 1 May 1955, all intelligence training courses moved from Fort Riley to Fort Holabird, and the Counter Intelligence Corps School was officially redesignated the U.S. Army Intelligence School (USAINTS).[1]

This consolidation of intelligence training, collocated with the Central Records Facility and the Army Photographic Interpretation Center, made Fort Holabird the closest thing to a "home" for Army intelligence at the time. However, signals intelligence training continued at Fort Devens, and beginning in 1957, the Combat Surveillance and Target Acquisition Training Command at Fort Huachuca conducted the Army's ground and aerial surveillance training. USAINTS and the ASA School were the responsibility of the ACSI until an Army-wide reorganization, on 1 July 1962, transferred responsibility for all training at Army Service schools to the U.S. Army Continental Army Command (CONARC).[2]

USAINTS continued to grow throughout the 1960s. By the time ground forces were committed to the Vietnam War in 1965, USAINTS staff were conducting 31 different resident courses for officers, warrant officers, enlisted members, and civilians and managing a robust nonresident instruction program for U.S. Army Reserve forces. Meeting the Army's intelligence personnel requirements for the war, however, was severely straining the installation.

Notes on the Army Intelligence Center

U.S. Army photo

Headquarters of the U.S. Army Intelligence School at Fort Holabird shortly after its redesignation.

In 1954, MG Arthur Trudeau had proposed a concept to GEN Charles L. Bolte, Vice Chief of Staff of the Army, to create an Army Intelligence Center (AIC) at Fort Holabird, Maryland, under the ACSI. The Chief of the AIC would be responsible for all intelligence training and personnel processes (active and reserve); the Central Records Facility at Fort Holabird; the new Army Photo Interpretation Center to be activated at Fort Holabird; the Army Security Center at Fort Meade, Maryland; and the Censorship School at Lowry Field, Colorado. The Chief of the AIC would also handle the organization and command of certain lettered intelligence detachments, strategic intelligence detachments, and Counter Intelligence Corps and military intelligence detachments already assigned to the ACSI. The AIC would also conduct research and development for intelligence equipment, write intelligence doctrine, and handle all G-2 operational and staff functions that could feasibly be removed from the Pentagon to a "G-2 Rear Echelon" at the AIC. This concept was approved and became effective in accordance with Department of the Army, General Order No. 65, on 1 September 1954, but it was never fully realized. Consequently, the AIC was discontinued in October 1965.

The Combat Surveillance and Target Acquisition Training Command

The Combat Surveillance and Target Acquisition Training Command (CSTATC) was established at Fort Huachuca, Arizona, on 1 December 1957. It taught surveillance technicians how to operate and maintain new families of sophisticated electronic equipment in the fields of radar and infrared. Initial training focused on ground surveillance radar and aerial surveillance drones and eventually included manned aerial surveillance systems, beginning with the U-23 aircraft equipped with the Army's first side-looking radar, the AN/APQ-85. The OV-1 Mohawk later replaced the U-23. Unattended ground sensors training was added in 1968. CSTATC was renamed the Combat Surveillance School in 1963 and then the Combat Surveillance and Electronic Warfare School in 1968.

What's Wrong with Fort Holabird?

Facilities at Fort Holabird were initially intended to meet only the needs of the Counter Intelligence Corps School, but the establishment of USAINTS in 1955 taxed the school's footprint. Almost immediately, the Army began looking for a new location for the school but without success. By the time the need for expanded facilities became critical, Fort Holabird's deficiencies in academic capacity, location, and quality of life were glaring.

In 1964, USAINTS graduated 3,530 students, but the annual throughput began increasing thereafter. From 4,970 graduates in 1965, the school's throughput nearly doubled to 8,258 in 1966 and increased again to 9,656 in 1968.

U.S. Army photo

This aerial view of Fort Holabird in the 1950s illustrates the lack of available field training space. The U.S. Army Intelligence School headquarters building is located in the center of the photograph.

While the student load increased for already established courses, the Army also levied new requirements on USAINTS for several noncommissioned officer courses, as well as tactical intelligence officer and Southeast Asia orientation courses. To meet this increased training capacity in a limited number of classrooms, USAINTS ran double shifts of classes, training 12 hours per day, 6 days per week.

In addition to limited classroom space, Fort Holabird had no outdoor training ranges. Students traveled to Fort Howard, Maryland, 10 miles distant, for field training exercises, which were limited in quantity and duration.

Despite the construction of a mock Vietnamese village at Fort Howard, the paucity of field training was evident to commanders in Vietnam, who complained their intelligence personnel were unprepared for their duties in country. This lack of training ranges was also cited as a reason why USAINTS could not develop and execute a critically needed MI Officer Basic Course. Instead, newly commissioned MI lieutenants had to attend the Infantry Officer Basic Course at Fort Benning, Georgia.

The limitations on space extended to living quarters as well. Enlisted student quarters had been reduced to the Army's minimum allowable 40 square feet of sleeping space, and some students were quartered in the gym. No on-post quarters existed for officers, who were given an allowance for off-post housing, costing the Army $1.8 million annually. Additionally, the mess halls could accommodate only 1,000 students at a time, requiring staggered and truncated mealtimes.

Unfortunately, all available space on Fort Holabird was already being used, leaving little opportunity to expand within the installation boundaries. Likewise, hemmed in by the industrial areas of Baltimore, Fort Holabird had no possibility of expanding outside its boundaries. Even if space was available, Department of Defense policy at that time prohibited any construction within metropolitan areas.

Living and training conditions suffered from more than just space limitations. The majority of the school buildings were World War II–era railroad warehouses converted for academic use, and one was a partially condemned 1894 brewery. The lack of air conditioning required that windows remained open, and the outdoor air and noise pollution contributed to dirty working conditions and interfered with class instruction.

By all accounts, Fort Holabird was not conducive to training the Army's intelligence specialists. In February 1967, a board chaired by MG Frank W. Norris, an artillery officer serving as the Director of Plans in the Office of the Deputy

U.S. Army photo

One of U.S. Army Intelligence School primary classroom buildings, Allen Hall, named after 1LT Eldon L. Allen, a counterintelligence agent killed during World War II.

Chief of Staff for Personnel, took an in-depth look at the Army's intelligence effort. The Norris Board recommended, and the Army Chief of Staff approved, that another study was warranted to find a suitable location where USAINTS could be collocated with the ASA Training Center and School (formerly the ASA School). From June through September, CONARC conducted on-site surveys of facilities at Fort Devens; Fort Riley; Fort Huachuca; Fort McClellan, Alabama; Fort Monmouth, New Jersey; Fort Meade, Maryland; Fort Bliss, Texas; Fort Gordon, Georgia; Fort Lee, Virginia; Governors Island, New York; Fort Leonard Wood, Missouri; and Fort Jackson, South Carolina. Meanwhile, ASA considered the option of moving USAINTS to Fort Devens. Published on 26 September 1967, CONARC's feasibility study indicated that none of these options proved ideal at providing "the necessary combination of academic, administration, logistical, and field training areas needed to support the school."[3] Many of the East Coast options were further hampered by the Department of Defense's construction prohibition. The impetus to move USAINTS remained high, however.

U.S. Army photo

MG Joseph McChristian, Assistant Chief of Staff, Intelligence, August 1968 to April 1971.

MG Joseph McChristian and the Intelligence Center Concept

In early 1968, many of the Army's Service schools embraced the CONARC "Center Team Concept," which collocated schools with their combat development agencies to ensure an integration of experience, knowledge, and capabilities. In August 1968, a proponent of this Center Team Concept arrived in the Pentagon as the ACSI and began formulating an even more extensive "Intelligence Center Concept."

The new ACSI, MG Joseph McChristian, had enlisted in the U.S. Army in 1933 and rose to his two-star rank during 38 years of service. Most recently, he had finished a tour in South Vietnam as GEN William C. Westmoreland's J-2 for the Military Assistance Command–Vietnam (MACV), where he essentially stood up the intelligence structure that supported MACV throughout the war. MG McChristian firmly believed "that there is no staff function more important to a decision maker than intelligence." He had an unparalleled understanding of the shortcomings of Army intelligence, stating it "needed badly a qualitative improvement in its performance."[4]

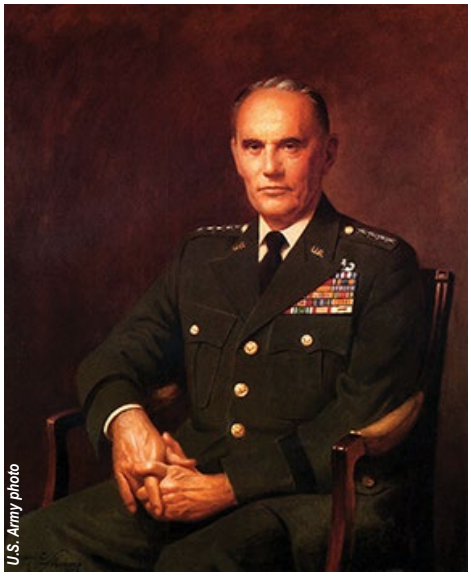
MG McChristian's vision was to create a "home" for intelligence, like the artillery center at Fort Sill, Oklahoma, or the infantry center at Fort Benning, a "central base for further development and growth of highly professional Military Intelligence personnel with esprit equal to that of the other distinguished branches of the Army."[5] It would be a place where intelligence personnel could return to work, train, and exchange ideas—a place where new doctrine, concepts, and techniques could be rapidly developed and integrated. "My concept is basically this: A home where all intelligence schools, all intelligence units, and all intelligence activities of the Army that are not required to be located someplace else, are established for the first time in our history where they can work together, and find out how one can help the other; because it is team work, you do not do intelligence in compartments. They must help each other on the battlefield."[6]

MG McChristian envisioned an intelligence center at which up to 21,000 personnel could be stationed to "centralize the Army's planning and operational control of intelligence collection and exploitation activities and permit

U.S. Army photo

Headquarters of the U.S. Army Combat Surveillance School in 1963.

the production of all-source capability studies to satisfy the Army's Intelligence requirements."[7] Further, the center would combine USAINTS, the Combat Surveillance School, and the ASA Training Center and School into one school system, supported by combat troops for realistic training. His ideal intelligence center would need good classrooms, plenty of airspace and training space, and an uncluttered electromagnetic spectrum.


U.S. Army photo

GEN Bruce Palmer Jr., Vice Chief of Staff of the Army, August 1968 to June 1972.

In March 1969, MG McChristian had an opportunity to visit Fort Huachuca en route to a speaking engagement on the West Coast. Knowing the Combat Surveillance School was there, he said, "I wanted to see it and know something about it." After conducting "a very thorough reconnaissance" of the post, he returned to the Pentagon and told Vice Chief of Staff of the Army GEN Bruce Palmer Jr. that he "considered Fort Huachuca a good candidate for an Intelligence Center, provided that the whole post be turned over." [8]

At that time, the Army's Strategic Communications Command (today's Network Enterprise Technology Command, known as NETCOM) had headquarters there, and MG McChristian recognized that water availability could not support both that command and the large intelligence center he envisioned. GEN Palmer directed MG McChristian to refine his Intelligence Center Concept to determine the exact composition of the center, personnel strength, and square-footage requirements for classrooms, barracks, officer quarters, administrative facilities, and field training ranges.

About the same time, the Army initiated a Long-Range Stationing Study Group (LRSSG) under the chairmanship of MG Linton S. Boatwright, an artillery officer who had previously served in World War II, Korea, and Vietnam and was currently the Deputy Chief of Staff for Personnel's Director of Individual Training. The LRSSG's mission was to update the Army's previous stationing study taking into account what the post-Vietnam Army would require. Part of that mission was also to find a suitable location for the Intelligence Center. In a convergence of MG McChristian's study (referred to as the ACSI Study) and the LRSSG, MG McChristian provided his detailed requirements to MG Boatwright, who then told MG McChristian which sites the LRSSG determined could fit those requirements. Taking the list of nearly 30 sites, MG McChristian personally visited the most reasonable selections and narrowed his candidates to two: Fort Riley and Fort Huachuca. Meanwhile, the Secretary of Defense directed a base realignment and closure package that included shuttering Fort Holabird. The need to find a new home for military intelligence became more urgent.

Endnotes

1. In accordance with Department of the Army, General Order No. 20, Section III (Washington, DC, 11 March 1955).

2. This reorganization coincided with the establishment of the Army Intelligence and Security Branch in the Regular Army. It was redesignated the Military Intelligence Branch in 1967.

3. Department of the Army, *Feasibility Study of Relocating the United States Army Intelligence School* (26 September 1967), 6-8.

4. *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. 14-15 (10 May 1972) (statement of MG Joseph McChristian, U.S. Army, Retired).

5. MG Joseph McChristian, "Presentation to Command Sergeants Major" (November 1969), 6.

6. *Testimony before Armed Services Subcomm.* 17 (statement of MG McChristian).

7. McChristian "Presentation to Command Sergeants Major," 2.

8. *Testimony before Armed Services Subcomm.* 18-19 (statement of MG McChristian).

Next time in this 2021 series:

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

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 2,000 and 4,000 words, double-spaced with normal margins without embedded graphics.
- We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- Although MIPB targets quarterly themes, you do not need to write your article specifically to a theme. We publish non-theme articles in most issues.
- Please do not include any personally identifiable information (PII) in your article or biography.
- Please do not submit an article to MIPB while it is being considered for publication elsewhere; nor should articles be submitted to MIPB that have been previously published in another publication or that are already available on the internet.
- All submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for reprint upon request.

What we need from you:

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

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

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

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

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

PIN:209478-000