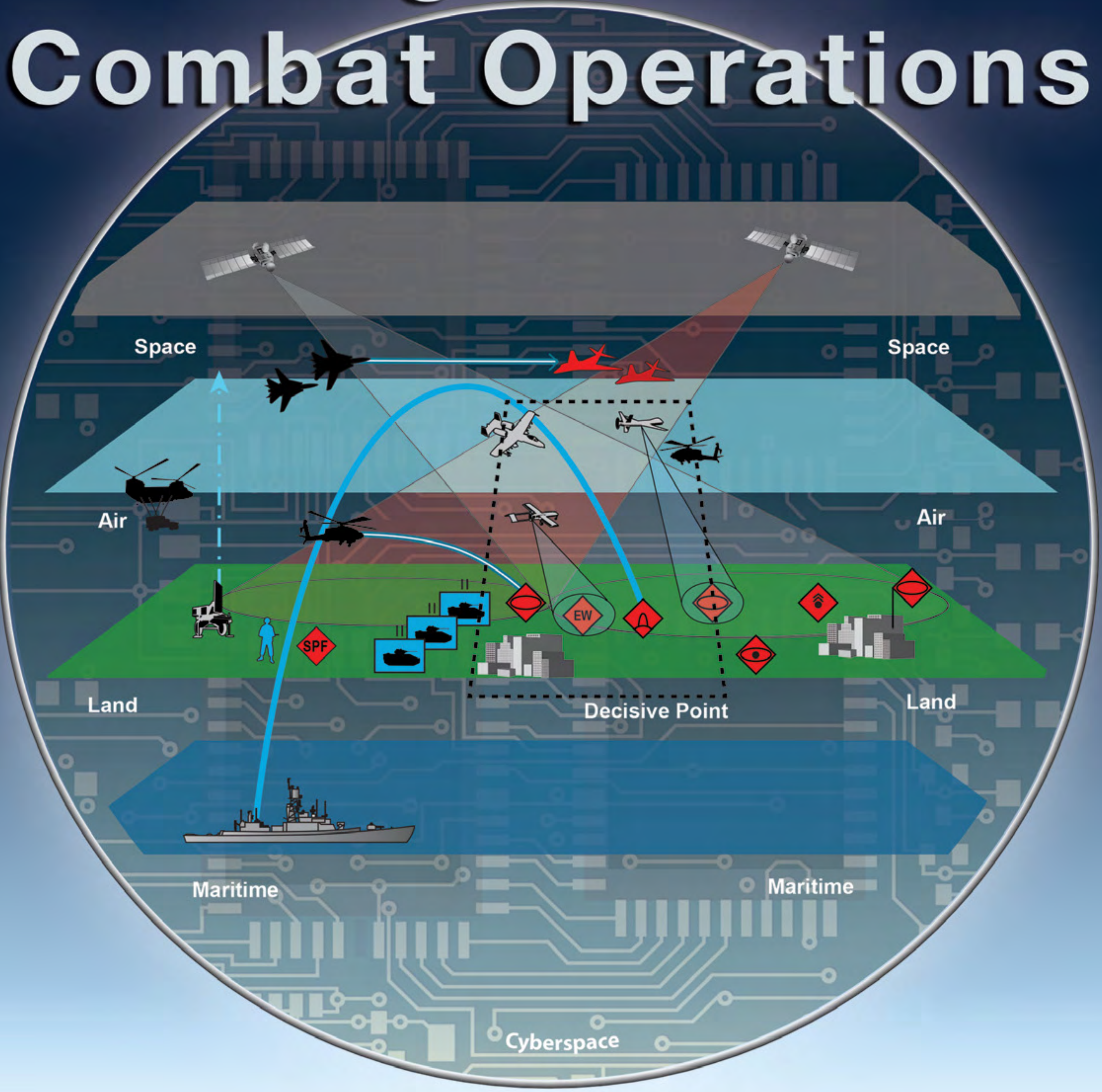
MI Professional Bulletin
January - March 2019
PB 34-19-1

Intelligence in Large-Scale Combat Operations



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

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

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

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

Commanding General
MG Robert P. Walters, Jr.

Chief of Staff
COL Douglas R. Woodall

Chief Warrant Officer, MI Corps
CW5 David J. Bassili

Command Sergeant Major, MI Corps
CSM Warren K. Robinson

STAFF:

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

Associate Editor
Maria T. Eichmann

Design and Layout
Emma R. Morris

Cover Design
Emma R. Morris

Military Staff
CPT Emily R. Morrison

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

By order of the Secretary of the Army:

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

Official:

GERALD B. O'KEEFE
Administrative Assistant
to the Secretary of the Army
1831101

From the Editor

The following themes and deadlines are established:

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

October–December 2019, *Intelligence in Echelons Above Corps.* This issue will discuss aspects of intelligence support and operations at Echelons Above Corps. Deadline for article submission is 1 July 2019.

January–March 2020, *Intelligence Preparation of the Battlefield.* The intent of this issue is to take a holistic look at IPB and the input provided by all staff sections to conduct mission analysis. Deadline for article submission is 28 September 2019.

April–June 2020, *Intelligence Analysis.* This issue will focus on the various aspects of intelligence analysis and their importance to operations. Deadline for article submission is 19 December 2019.

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

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

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 2019
PB 34-19-1
Volume 45 Number 1

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

Intelligence in Large-Scale Combat Operations

FEATURES

DEPARTMENTS

Always Out Front

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

The future of our Army is dynamic. We must train and be ready to compete and win anywhere in the world. Over the last few years, U.S. forces excelled in counterinsurgency and counterterrorism operations in Iraq and Afghanistan. During that time, our peer threats were watching our operations and developing their capabilities to counter our forces in future conflict. To help address these increased adversary capabilities, this quarter's *Military Intelligence Professional Bulletin* theme is intelligence support to large-scale combat operations. Large-scale combat operations are characterized by "complexity, chaos, fear, violence, fatigue, and uncertainty".[1] The fluid and chaotic nature of large-scale combat operations causes the highest degree of friction and stress on the intelligence warfighting function. Threat forces will attempt to counter friendly collection capabilities by using integrated air defense systems, long-range fires, counterreconnaissance, cyberspace and electronic warfare operations, camouflage and concealment, and deception. It is imperative that our warfighting function understand how we support these operations with the full weight and power of our intellect, tools, and processes throughout the conflict continuum. As intelligence professionals, we must create situational understanding, pulling information from all agencies, governments, and partners to ensure decision makers have the information required to drive operations and make informed decisions.

Readiness Through Training

"Training is the foundation for successful operations. Effective training must be commander driven, rigorous, realistic, and to the standard and conditions that units are expected to fight. Realistic training with limited time and resources demands that commanders focus their unit training efforts to maximize repetitions under varying conditions to build proficiency."[2]

As we train for future conflicts, our priority must shift from counterinsurgency-focused problem sets to large-scale combat operations and achieving a position of relative advantage. To win during large-scale combat operations, we must analyze our enemy's capabilities to determine whom and what we are facing. Weather and terrain are important considerations to determine how the threat and our forces will shoot, maneuver, and communicate. That is why we at the U.S. Army Intelligence Center of Excellence have emphasized the importance of conducting tactical intelligence training. Specifically, we have begun training these skills across the ranks, ensuring that our Soldiers, warrant officers, and officers are able to confidently deploy with any unit preparing for combat. Our intelligence professionals and future leaders will be ready to provide their commanders with the necessary intelligence and recommendations to defeat the enemy. All across Fort Huachuca, training has been revamped to replicate real-world situations with the intent to provide units with tactically and technically proficient Soldiers. One important example of providing realistic training is the capabilities resident in the Intelligence and Electronic Warfare Tactical Proficiency Trainer.

Foundations in Doctrine

In ADP 2-0, *Intelligence*, our team developed a publication that aligns with FM 3-0, ADP 3-0, and ADRP 3-0, *Operations*. ADP 2-0 (published September 2018) explains that during large-scale combat operations we must fight for intelligence and "strive to identify or open windows of opportunity across domains."[3] FM 3-0, ADP 3-0, and ADRP 3-0 each highlight necessary actions expected from the intelligence warfighting function, stating that "the side that best understands an operational environment, that learns and adapts more rapidly, and that acts more quickly, is most likely to win."[4] Our intelligence Soldiers provide the information necessary to analyze the operational variables listed in the memory aid PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time). They process, exploit, and disseminate information to provide a better understanding of the operational environment, which allows maneuver units to succeed in close combat. We are also helping the commander and staff *Develop the Situation Through Action*. Intelligence professionals continuously conduct intelligence operations and perform analysis to satisfy priority intelligence requirements.

The Challenge

Throughout this issue, we will examine intelligence support from theater, corps, division, and brigade perspectives. We will explore how the intelligence warfighting function supports lethality for the fires warfighting function and the importance of the intelligence warfighting function in preparing for and executing a successful combat training center rotation. We will gain insights on how a peer threat uses intelligence to support their combat operations. Lastly, we will look at how refocusing on the basic techniques and principles of information collection planning and collection management helps us gain an advantage and allows our commanders to be at the right place and time, and in the right posture to close with and destroy the enemy.

I challenge each of you, as members of the Military Intelligence Corps, to learn, embrace, and support Army operations and intelligence doctrine as we continue to develop strategies that will allow us to win our Nation's wars. We are sure to win the trust of our commanders and the confidence of the staff by thoroughly understanding the enemy and ourselves within the context of large-scale combat operations.

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.

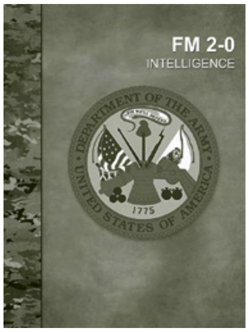
2. Department of the Army, Army Doctrine Publication (ADP) 3-0, *Operations* (Washington, DC: U.S. GPO, 6 October 2017), 5.

3. Department of the Army, ADP 2-0, *Intelligence* (Washington, DC: U.S. GPO, 4 September 2018), 5-1.

4. Department of the Army, ADP 3-0, 2.

Always Out Front!

Large-Scale Combat Operations: An Excerpt from FM 2-0



Introduction

The Army must reorient on large-scale ground combat while simultaneously conducting other types of operations worldwide to prevent peer threats from gaining positions of strategic advantage. Many of the considerations necessary to achieve military success in the current operational environment remain fundamentally unchanged, but what has changed is important. Army forces cannot focus solely on large-scale ground combat operations at the expense of the other missions, but they also cannot afford to be unprepared for large-scale combat operations in an increasingly unstable world. Being prepared for large-scale ground combat generates credible deterrence and contributes to worldwide stability. The future requires the lethal theater armies, corps, divisions, and brigades necessary to conduct operations with the right mix of forces necessary to execute tactical tasks to achieve operations and strategic goals.

FM 2-0 provides doctrine for how Army forces, as a part of a joint team and in conjunction with unified action partners, develop intelligence to support operations. It describes intelligence and intelligence operations using current Army capabilities and formations in today's operational environment. Intelligence is critical in a complex operational environment against a peer threat.

Intelligence drives operations and operations enable intelligence. Commanders and staffs need timely, accurate, relevant, and predictive intelligence to understand threat characteristics, goals and objectives, and courses of action to successfully execute offensive and defensive tasks in large-scale combat operations. Precise intelligence is also critical to target threat capabilities at the right time and place and to open windows of opportunity across domains, particularly during large-scale combat operations. Commanders and staffs must have detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute unified land operations.

Endnote

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

CSM FORUM

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

One of the key things leaders need to concern themselves with is training our Soldiers for the role of intelligence in large-scale combat operations. We do not have to throw away more than 16 years of combat experience. Soldiers of all ranks have done outstanding work in support of our Nation, while spending time away from their families. However, we cannot allow ourselves to think the next potential fight is going to be the same as the one our Soldiers have faced for most of the time they have been in the Army.

Intelligence professionals need to understand how the operational environment has changed. Conducting large-scale combat operations will not be the same as fighting in a counterterrorism/counterinsurgency environment. It is essential that we prepare to combat adversaries that are our peer or near peer in technologies in multiple domains. This will require looking at each domain simultaneously to ensure we plan, coordinate, and synchronize our efforts for maximum effect.

Many of our Soldiers are conducting real-world missions on a daily basis. It is necessary to maintain focus on current requirements, but it is negligent not to train our Soldiers on warrior tasks and battle drills and other military occupational specialty (MOS) tasks required in combat. Senior leaders understand this is not always easy. The Secretary of the Army has all but eliminated Army-required training that does not increase the lethality of our Soldiers. Leaders down to the junior level should conduct training management and set aside time to ensure our Soldiers get the training they require to execute the Army's mission of fighting and winning our Nation's wars.

We need to look at the tasks we must train our Soldiers to execute to standard. Increasing Soldier lethality is one of the top priorities of our Army today. Large-scale combat operations will place our intelligence Soldiers in situations they are not accustomed to, regardless of the number of deployments they have. The physical fitness of our Soldiers will be increasingly important to meet the demands of an expeditionary force on the battlefield. Shoot, move, and communicate are skills every Soldier must be proficient in, but there are other simple things to brush up on. The potential of not living on forward operating bases or hardstand camps is likely. Setting up tents, determining daily load plans, jumping the tactical operations center, and dealing with basic fieldcraft and sanitation are areas in which many of our Soldiers are not proficient.

Next, we need to look at the most effective approach to train the MOS tasks required in large-scale combat operations. Studying the new FM 2-0, *Intelligence*, is a good place to start to understand how we will fight for intelligence during large-scale combat operations. The critical task list for each MOS should focus our noncommissioned officers on training individual tasks. We must ensure the critical task list focuses on those tasks Soldiers will execute on the battlefield. Each unit may not have all the required equipment to train and certify Soldiers on all intelligence tasks. Leaders may have to communicate outside their organization to coordinate for equipment to ensure our Soldiers get the training they deserve.

It is important that leaders be very deliberate in finding and allocating time to train our Soldiers to conduct large-scale combat operations and increase their lethality against the peer and near-peer threat. The key will be to train and equip our junior leaders to think and operate in this way. The good news is our younger generation is more than capable of conceptualization and multitasking, which makes them invaluable in multi-domain operations. The future is unknown, but we have the tools to build agile, adaptable leaders prepared to fight for intelligence.

Always Out Front!

Technical Perspective

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

As our Army returns the focus to large-scale combat operations against peer threats, military intelligence warrant officer technical leadership remains a critical capability for mission success. In most military intelligence formations today, only a handful of folks are likely to bear the "scars of experience" (wrinkles and gray hair) earned preparing to confront a peer threat (the former Soviet Union). To overcome this gap, a plethora of new technology, formations, doctrine, and concepts bombard emails, video teleconferencing, and teleconferences almost daily. In an operational environment where we are contested in all domains, change comes rapidly and we all must be prepared to react positively to it. One concept or idea however that doesn't change for the intelligence warfighting function still rings true today: *"Know thy self, know thy enemy. A thousand battles, a thousand victories…" Sun Tzu*.

While the likelihood of a scenario involving Darkhorse (11th Armored Cavalry Regiment) once again defending the Fulda Gap seems unlikely, the detailed understanding of threat doctrine, organization, capabilities, and vulnerabilities remains the cornerstone of winning in ground combat. As discussed in FM 3-0, *Operations*, and FM 2-0, *Intelligence*, fighting for intelligence is the norm our tactical formations should expect. Being contested in all domains complicates our ability to gain a critical understanding of where lead regimental reconnaissance assets are, the depth and distance between battle positions in an area defense, or the location of the Zoopark-1 counterfire radar. This forces us to develop that understanding through multiple "sets and reps" of noncommissioned officer led and warrant officer/officer managed intelligence training that prepares us to "predict" likely threat courses of action with limited information in a given situation, in any terrain, and in any weather conditions, or put simply, mastering intelligence preparation of the battlefield.

Unfortunately, it is not enough to master threat understanding. As intelligence professionals, we must all master operational doctrine and become experts in employing our intelligence capabilities within the operational framework. Prior to modularity, our formations at brigade combat team and below had very limited ground collection capability, notwithstanding the ground surveillance radar. Our terrestrial layer collection platforms ought to be fought like weapons systems. If we're not practicing maneuver in nonpermissive environments, our likelihood of survival diminishes swiftly. If we're not personally involved in the maintenance of our systems, or understanding the logistical requirements to sustain operations, we're fooling ourselves if we think we'll be successful on the battlefield. These are the norms we must return to, and warrant officers play a critical role in shaping the training requirements and the environments in which critical training must occur.

To truly understand what intelligence support to large-scale combat operations means for the intelligence warfighting function, we have to look at it from the scope of multi-domain operations. Meaning, we cannot focus solely on the tasks associated with armed conflict, but must also focus on those tasks occurring during the shaping and preventing roles. Building readiness for armed conflict is certainly critical, but as intelligence professionals our role during shaping and preventing is as equally critical to winning in armed conflict. Our operational-level intelligence formations, along with limited tactical echelon support, must build the maneuver commander's and their formations' foundational understanding of the operational environments they will potentially operate in and provide combatant commanders critical understanding through indications and warning of adversarial intentions to undermine or usurp U.S. interests in a given country or region. Once again, intelligence preparation of the battlefield and/or intelligence preparation of the operational environment is the mechanism to build that understanding—it is merely a different focus during the shaping and preventing roles. Operationally, several areas encompass some of the functions and roles that our intelligence professionals at the operational level perform to build readiness for armed conflict during shaping and preventing:

- ✦ Establishing relationships that lead to future placement and access with host nation security and military organizations.
- ✦ Training and developing those same partner organizations.
- ✦ Developing a deep understanding of the electromagnetic spectrum in a country or region.

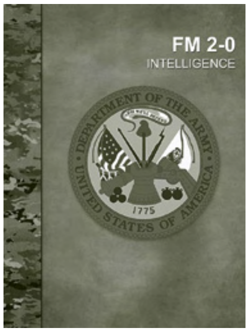
- Developing detailed order of battle understanding.
- Identifying gaps and developing requirements to satisfy those gaps.
- Developing cultural understanding.

As warrant officers, you lead most of those teams and have the task of balancing daily operational requirements while ensuring the foundational depth of understanding continues.

The greatest challenge now is not losing the years of experience gained during counterinsurgency operations; those skills and knowledge are still critically important to successful multi-domain operations. The world is adding more rocks (large-scale combat operations and multi-domain operations) to your rucksack, and I am confident our cohort is up to the challenge. Thank you for all that you do each and every day for our Army.

Always Out Front!

Fighting for Intelligence During Large-Scale Combat Operations: An Excerpt from FM 2-0



The Challenge

Producing intelligence and executing information collection differ significantly based on the Army strategic role. For example, intelligence operations conducted during shaping operations differ drastically from intelligence operations conducted during large-scale combat operations.

Of the four Army strategic roles (shape, prevent, conduct large-scale ground combat, and consolidate gains), the intelligence warfighting function is most challenged to meet the vast number of large-scale combat operation requirements. Large-scale combat operations are intense, lethal, and brutal—creating conditions, such as complexity, chaos, fear, violence, fatigue, and uncertainty. Battlefields will include noncombatants crowded in and around dense urban areas. To further complicate operations, enemies will employ conventional and unconventional tactics, terrorism, criminal activities, and information warfare. Activities in the information environment will often be inseparable from ground operations. The fluid and chaotic nature of large-scale combat operations will cause the greatest degree of fog, friction, and stress on the intelligence warfighting function.

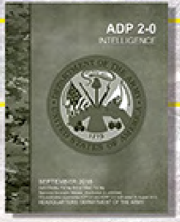
When fighting a peer threat during large-scale combat operations, units must be prepared to fight for intelligence against enemy formations, a range of sophisticated threat capabilities, and many unknown conditions within the operational environment. The challenges to information collection include IADSs, long-range fires, counterreconnaissance, cyberspace and EW operations, and camouflage, concealment, and deception.

Key aspects of fighting for intelligence to support operations include the following:

- Commanders drive intelligence.
- Effective staff integration is crucial.
- Effective intelligence requires a comprehensive intelligence architecture.
- A thoroughly developed and flexible information collection plan is critical.
- A successful information collection plan begins with identifying the right requirements for reconnaissance, surveillance, security operations, and intelligence operations.
- Together, commanders, staffs, and subordinate units strive and constantly adjust to develop and execute a layered and aggressive information collection plan.

Endnote

Department of the Army, Field Manual 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, 6 July 2018), 6-1.



ADP 2-0 Update

by Ms. Terri M. Lobdell

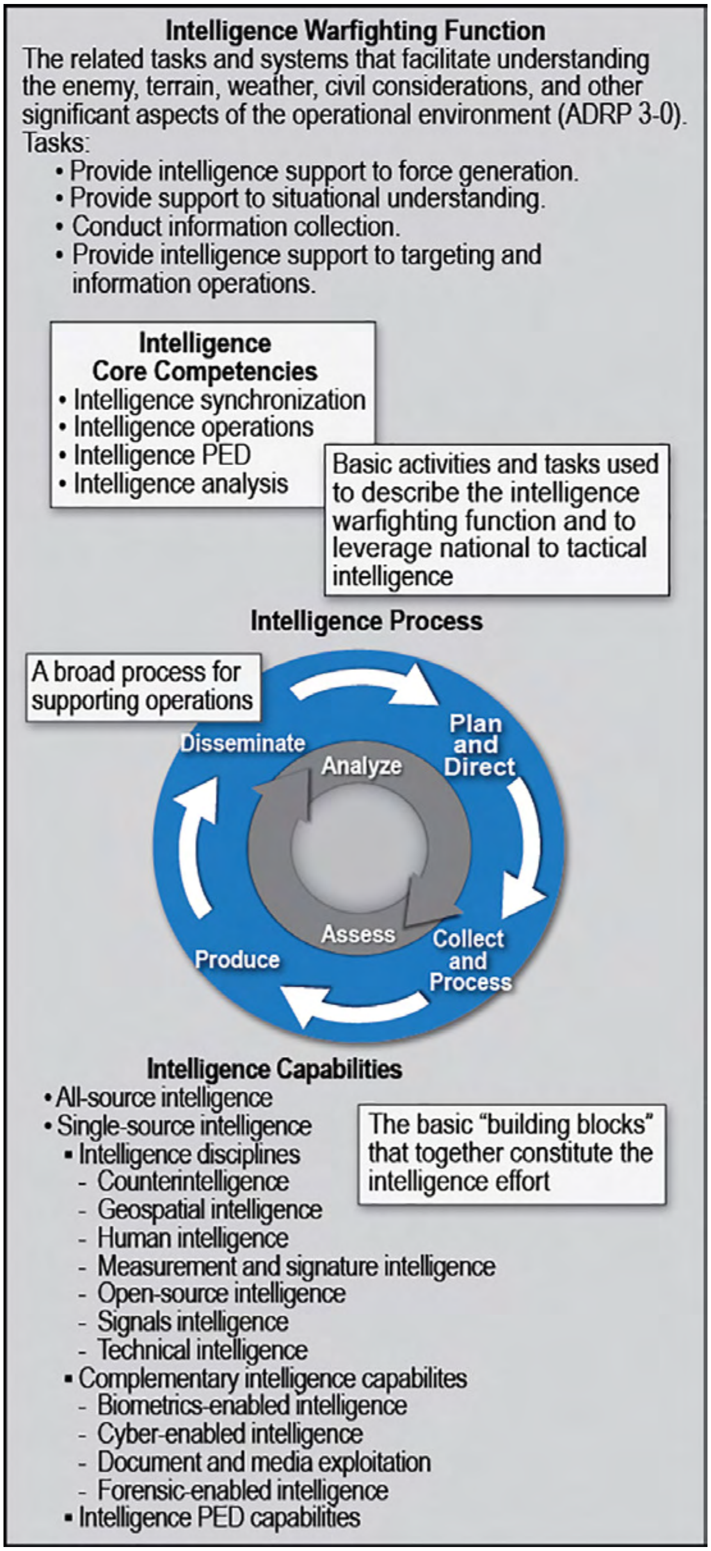
On 4 September 2018, the Army released ADP 2-0, *Intelligence*. This version updates and combines the August 2012 versions of ADP 2-0 and ADRP 2-0 into one publication. GEN Townsend, U.S. Army Training and Doctrine Command Commanding General, directed all Army proponents to eventually combine their Army doctrine publications and Army doctrine reference publications. The U.S. Army Intelligence Center of Excellence is the first center of excellence to publish its combined Army doctrine publication.

What Is New

ADP 2-0 marks a significant departure from previous intelligence doctrine. The publication was deliberately developed to reset Army intelligence doctrine to nest with FM 3-0, *Operations*, while simultaneously improving clarity and maintaining time-tested fundamental intelligence concepts—the intelligence warfighting function, the intelligence process, all-source intelligence, and single-source intelligence, including the intelligence disciplines and complementary intelligence capabilities.

ADP 2-0 is to be used in conjunction with FM 2-0, *Intelligence* (6 July 2018), to help focus the intelligence warfighting function on the new challenges associated with peer threats, multi-domain operations, and the conduct of large-scale combat operations. The following includes some of the key changes to ADP 2-0:

- ✦ Discusses the requirement for precise intelligence to identify and take advantage of *windows of opportunity* in *multi-domain operations*.
- ✦ Introduces *processing, exploitation, and dissemination (PED)* as a term.
- ✦ Introduces *intelligence PED* as an intelligence core competency to address how "the intelligence warfighting function processes collected data and information, performs an initial analysis (exploitation), and provides information in a useable form for further analysis."[1]
- ✦ Replaces the term *intelligence enterprise* with *national to tactical intelligence* to better articulate those capabilities (U.S. intelligence professionals, sensors, systems, federated organizations, information, and processes



Intelligence Warfighting Function

The related tasks and systems that facilitate understanding the enemy, terrain, weather, civil considerations, and other significant aspects of the operational environment (ADRP 3-0).

Tasks:

- Provide intelligence support to force generation.
- Provide support to situational understanding.
- Conduct information collection.
- Provide intelligence support to targeting and information operations.

Intelligence Core Competencies

- Intelligence synchronization
- Intelligence operations
- Intelligence PED
- Intelligence analysis

Basic activities and tasks used to describe the intelligence warfighting function and to leverage national to tactical intelligence

Intelligence Process

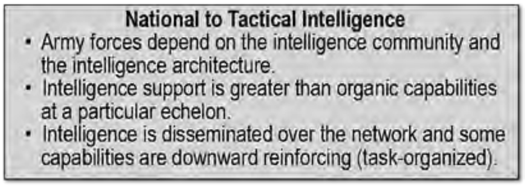
A broad process for supporting operations

Intelligence Capabilities

- All-source intelligence
- Single-source intelligence
  - Intelligence disciplines
    - Counterintelligence
    - Geospatial intelligence
    - Human intelligence
    - Measurement and signature intelligence
    - Open-source intelligence
    - Signals intelligence
    - Technical intelligence
  - Complementary intelligence capabilites
    - Biometrics-enabled intelligence
    - Cyber-enabled intelligence
    - Document and media exploitation
    - Forensic-enabled intelligence
  - Intelligence PED capabilities

The basic "building blocks" that together constitute the intelligence effort supported by a network-enabled architecture) to which the commander has access.

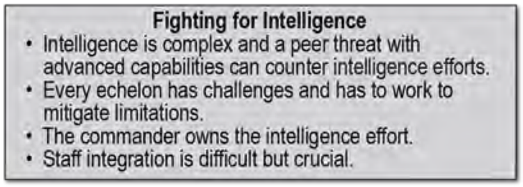
- Discusses *setting the theater* for intelligence in Army forces across all echelons of a deployed force in theater. Intelligence staffs and military intelligence units must carefully transition intelligence capabilities and activities to support all engagements and operations as the Army moves from shape to prevent to prevail in large-scale ground combat and to consolidate gains.


National to Tactical Intelligence

- Army forces depend on the intelligence community and the intelligence architecture.
- Intelligence support is greater than organic capabilities at a particular echelon.
- Intelligence is disseminated over the network and some capabilities are downward reinforcing (task-organized).

- Recognizes that, because of network/broadcast dissemination, each echelon has more intelligence capabilities than simply organic capabilities. "The basic intelligence support provided by the G-2/S-2 and intelligence staff at each echelon is the same. What differs is the size, composition, and number of supporting capabilities for the intelligence staff; access to higher-level information and intelligence; number and complexity of the requirements; and time available to answer those requirements."[2]

ADP 2-0 culminates with an in-depth discussion of fighting for intelligence. *Fighting for intelligence* is the challenge of ensuring an effective intelligence effort during large-scale combat operations. Intelligence is never perfect, information collection is never easy, and a single collection capability is never persistent and accurate enough to provide all the answers. "The following aspects of fighting for intelligence are critical:


Fighting for Intelligence

- Intelligence is complex and a peer threat with advanced capabilities can counter intelligence efforts.
- Every echelon has challenges and has to work to mitigate limitations.
- The commander owns the intelligence effort.
- Staff integration is difficult but crucial.

- Effective intelligence requires developing an effective intelligence architecture well before large-scale combat operations.
- The commander must own the intelligence effort.
- The commander and staff—
  - Must forge an effective relationship and excel in staff integration.
  - Must understand intelligence limitations, especially collection gaps, at their echelon and overcome or mitigate those limitations through effective information collection.
  - At times, may have to conduct combat operations or find creative solutions to enable information collection.
- The unit must adjust the information collection plan, adapt to threat counter-collection measures, and maintain a layered and aggressive information collection effort."[3]

"Despite a thorough understanding of intelligence fundamentals and a proficient staff, an effective intelligence effort is not assured. Large-scale combat operations are characterized by complexity, chaos, fear, violence, fatigue, and uncertainty. The fluid and chaotic nature of large-scale combat operations causes the greatest degree of fog, friction, and stress on the intelligence warfighting function. Threat forces will attempt to counter friendly collection capabilities by using integrated air defense systems, long-range fires, counterreconnaissance, cyberspace and electronic warfare operations, camouflage and concealment, and deception."[4]

Your Doctrinal Challenges

As an avid supporter of doctrine, MG Robert Walters, Jr., Commanding General of the U.S. Army Intelligence Center of Excellence, expects all intelligence professionals to read and understand intelligence doctrine and to know how it supports Army operations, particularly ADP 2-0. ADP 2-0 serves as the intelligence doctrinal foundation for our Army, as it provides the intellectual structure of intelligence support in complex operational environments and a framework to support unified land operations across the range of military operations. It is incumbent on all intelligence professionals to understand their foundational doctrine and how to use it to effectively support the commander.

ADP 2-0 is available on Intelligence Knowledge Network at https://ikn.army.mil/apps/IKNWMS/Home/WebSite/MILITARY_DOCTRINE_CAC2, on the Army Publishing Directorate website at https://armypubs.army.mil/, and on the Central Army Registry at https://atiam.train.army.mil/catalog/dashboard.

Endnotes

[1] Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (Washington, DC: U.S. Government Publishing Office, 4 September 2018), 2-5.

[2] Ibid., 2-9.

[3] Ibid., vii.

[4] Ibid.

Best Practices for Communications, Common Operational Pictures, and Command Post Jumps

by Major Jared N. Ferguson, Captain Jeff W. Linzey, and Captain Casey L. Coyle

Introduction

At all echelons, the intelligence warfighting function serves to contribute to the commander's visualization and understanding. In fixed facilities, this can be challenging—even with unhampered access to high-bandwidth internet and permanently emplaced systems on all classification levels of networks, radios, and phones. However, when taking the intelligence warfighting function into a tactical environment, the challenges increase, and they compound further when jumping the command post.

Knowing the options of the tactical environment and carefully considering them allows informed and deliberate planning. As a result, decision makers will have a better understanding of whether and when to jump the command post and can combine shared ownership of their actions before, during, and after jumping command posts. This will facilitate near-seamless transitions and provide the continuity of intelligence support to commanders during large-scale combat operations.

As a means of informing deliberate planning, let us examine the tactics, techniques, and procedures identified as best practices through the lens of the Joint Multinational Readiness Center (JMRC). We will highlight the coordination necessary in order to provide continuous intelligence support during transitions between main command posts and tactical command posts. A similar transition occurs when intelligence responsibilities pass to other capable entities, such as the brigade intelligence support element (BISE).

> **Combat Training Center Best Practice**
>
> Commanders determine the roles and responsibilities of mission command nodes and identify intelligence requirements. Then they man, train, and equip them and practice before the fight.

Notable impacts exist when jumping the command post, ranging from incomplete access to information to diminished communication capabilities with which to disseminate assessments. While intelligence should always be concise, there is no need to be frugal with bandwidth requirements when systems are firing on all cylinders and a robust architecture is enabling a high-volume throughput.

Command Posts' Roles and Responsibilities

Established and clearly understood roles and responsibilities is a theme that will be developed at length throughout this article, but it starts with understanding the purpose and function of a command post. According to FM 6-0, *Commander and Staff Organization and Operation*, **"A *command post* is a unit headquarters where the commander and staff perform their activities,"** essentially a hub for mission command that enables the staff to work in support of the commander's visualization and situational understanding. "Each [command post] CP performs specific functions by design as well as tasks the commander assigns," which include but are not limited to maintaining the common operational picture (COP); running estimates; managing the fight; coordinating with higher, lower, and adjacent units; and otherwise functioning as a one-stop-shop for commander visualization and situational understanding.[1] (Note: For the duration of this article, "COP" refers to common graphics and position location information, including common intelligence pictures.)

> **Combat Training Center Best Practice**
>
> Establish, vet, practice, and actively use a tactical operations center standard operating procedure. (1) Do periodicity and conditions-based reporting (every hour, upon contact, and upon observation); (2) Format and have a PACE plan for each type of report: "Given [XYZ] condition, send with format [ABC]."

After a unit establishes its command post, many available units enable different types of connectivity. These include network access at different classification levels, detailed and nested digital COPs, supported Distributed Common Ground System-Army (DCGS–A) Brains, and fully connected intelligence elements at echelon, such as the company intelligence support team, BISE, or analysis and control element. The ability to create this kind of intelligence architecture does not in itself limit the ability to move quickly, but attention and care must be put into planning, preparing, and executing deliberate transitions, which in this context are “intelligence handovers” between assorted command posts to provide continuity until the architecture is reestablished.

Main command posts and tactical command posts have different doctrinal functions, aside from the commander-directed duties. The staff should steep themselves in doctrine, which should include FM 6-0. The field manual identifies key differences among the duties and responsibilities of the varying command posts. **“The *main command post* is a facility containing the majority of the staff designed to control current operations, conduct detailed analysis, and plan future operations.”**[2] Meanwhile, **“the *tactical command post* is a facility containing a tailored portion of a unit headquarters designed to control portions of an operation for a limited time.”**[3] The tactical command post relies on the main command post for planning, detailed analysis, and coordination. The field manual then transitions to identify that “when organizing the CP, commanders must consider effectiveness and survivability. However, effectiveness considerations may compete with survivability considerations, making it difficult to optimize either. Commanders balance survivability and effectiveness considerations when organizing CPs.”[4]

Many factors affect the commander’s decision; the more commanders can decide and codify through previous exercises and repetitions, the less they need to consider anew. They can defer to the deliberate planning conducted before the high-intensity conflict. That leaves them free to make only subtle changes during the fight based on the operational variables of mission, enemy, terrain and weather, troops and support available–time available and civil considerations (METT–TC). Deliberate planning, whether conducted before or as time allows during the conflict, includes consideration of the factors of effectiveness and survivability. The U.S. Army identifies the subcategories of effectiveness as design and layout, standardization, continuity and deployability, capacity, connectivity, and range. The Army similarly divides survivability into dispersion, size, redundancy, and mobility.

Combat training center observations suggest that deliberate planning should also include the following criteria when cobbling together the set of systems that will comprise the primary, alternate, contingency, and emergency (PACE) means of communication. Units can address them differently but should not overlook even one.

Combat Training Center Best Practice

Consider the following additional criteria when determining the command post and architecture composition and PACE plan:

- Availability (includes maintenance status).
- Reliability (consistency of setup or occurrence of issues).
- Cost (and to whom: unit, headquarters and headquarters company, urgent operational needs, “Big Army,” and others).
- Size.
- Weight.
- Ease (expertise or training required to set up).
- Speed of setup.
- External requirements (i.e., who else has to help?).
- Redundancy.
- Throughput (bandwidth-enabled).
- Signature and emissions (noise, light, and electronic warfare).
- Vulnerability and security (hackable or destroyable).

According to the JMRC’s senior intelligence officer and the five-paragraph operation order structure, units must operationalize paragraph 5 (command and signal) to address paragraph 3 (execution) in order to defeat paragraph 1 (situation) and achieve paragraph 2 (mission) (all with the help of paragraph 4 [sustainment]). One would be hard-pressed to say that any warfighting function operates in a vacuum. In fact, each warfighting function relies heavily on the others to enhance commander visualization and situational understanding, ultimately informing the commander’s application of combat power.

Combat Training Center Best Practice

Preplan transitions that link the PACE means of communication with phases of the operation. This nests and enables the concept of operations while accounting for the threat environment.

Intelligence Architecture: More Than One Way

Intelligence architecture is not a fixed, rigid flowchart. It describes how data, information, and knowledge flow across the enterprise, and there are a number of ways to make that happen. Within the intelligence community, the term “intelligence architecture” is often met with consternation; any follow-on topics are assumed too complex and therefore are summarily dismissed. A simplified frame of reference for intelligence architecture is a PACE plan for intelligence communication—the means to share processing, exploitation, and dissemination; data; analysis; assessments; and other intelligence production.

According to doctrine and the modified table of organization and equipment, different units and echelons have specific organic assets for establishing network architectures. But who owns the architecture? Intelligence architecture typically rides on a network architecture backbone; therefore, it is necessary to gain an understanding of the options that the S-6/G-6/J-6 and signal community have available. We will examine what those options look like and each option's pros and cons with respect to the tactical fight.

When a unit differentiates its PACE plan by end-user system, it clarifies what communications platforms to use. For example, regardless of military occupational specialty, a radio-telephone operator in the main command post can look at the PACE plan, look at the systems in front of him or her, and know what to use. The downside of setting a PACE plan by end-user system is that the unit often fails to consider the method of transport. Voice over Secure Internet Protocol (SVoIP) phones and SECRET Internet Protocol Router (SIPR) email rely on the same backbone; if the PACE means of communication is SIPR chat, SVoIP, SIPR email, and frequency modulation, the unit may immediately find itself on its emergency communications platform the moment the satellite transportable terminal goes down. That would be true regardless of whether it is self-imposed or due to enemy activity, and three of the four PACE means would immediately be non-mission capable.

Multiple pieces of equipment can work on different waveforms. This has the potential to confuse the end user because the PACE plan may not specify which mode should be used. To successfully plan PACE by platform, S-6 personnel must know each of the warfighting functions' desired PACE plan in order to deconflict the potential overreliance on any one waveform.

Combat Training Center Best Practice

Equipment for PACE Plan Comprising One From Each Column

PACE by Platform Options

Primary	Alternate	Contingency	Emergency
SINGARS (20K w/pa)	AN/PRC-154	154A (2K)	Runner
AN/PRC-117 (20K w/pa)	AN/PRC-117 (LOS SAT)	DTCS (LOS SAT)	Flags
AN/PRC-148 (7K)	AN/PRC-152 (LOS SAT)	GRRIPs (LOS SAT)	Cellphone
AN/PRC-152 (7K)	JCR/FBCB2		
SVoIP (Upper T/I)	CPOF (Upper T/I)		
SIPR Email (Upper T/I)			
DCGS–A (Upper T/I)			

The electromagnetic spectrum is the range of all possible frequencies of electromagnetic radiation. The term *waveform* refers to the shape and form of a signal, such as the wave, moving in a physical medium or an abstract representation. It is important to understand that the electromagnetic spectrum is divided into waveforms: high frequency, very high frequency, ultrahigh frequency, and L, S, C, X, Ku, K, and Ka bands.

Setting the PACE means of communication by waveform eliminates the potential single point of failure between different communication platforms. Units then have a primary means of waveform connectivity, such as a satellite transportable terminal, and potentially an alternate, such as Tampa equipment. Both of these can enable SIPR connectivity. The S-6 feeds operation order development, specifically Annex H (Priority of Establishment of Mission Command Systems), which dictates the primary system to provide the given waveform capability.

Combat Training Center Best Practice

Waveform PACE Comprising One From Each Column

PACE by Waveform Options

Primary	Alternate	Contingency	Emergency
VHF	UHF (Band I)	HF	UHF (Band III)
EHF			

The downside of a PACE plan by waveform is that end users and non-signal Soldiers might not know which systems operate on each waveform. To use waveform-PACE successfully, a shared understanding must exist within the organization about which end-user devices operate on which waveforms.

When talking in terms of waveform, it is common to use the electromagnetic spectrum. When specificity is needed, it is best to use the modulation within the spectrum. Modulation can be thought of as a subcategory. Generally, lower tactical internet communication platforms provide their own transport or backbone. Upper tactical internet communication platforms tend to "piggyback" on transport systems such as the Secure Mobile Anti-Jam Reliable Tactical Terminal and Joint Network Nodes. The unit modified table of organization and equipment dictates which transport systems are assigned per unit.

Also worth mentioning are the intelligence-specific systems and capabilities, such as those that the TROJAN equipment provides or those that reside on the military intelligence domain. The TROJAN series of equipment provides an organic intelligence asset in the form of a satellite antenna mounted on a high-mobility multipurpose wheeled vehicle and shelter-housed racks of networking equipment. This allows a portable, self-contained means of establishing not only the upper tactical internet but also access to the military intelligence domain on SIPR and the Joint Worldwide Intelligence Communications System, with national-level intelligence access as well, to support signals intelligence. Furthermore, the TROJAN serves to eliminate a command post's network architecture as a single point of failure for military intelligence systems.

Using the TROJAN, intelligence sections establish an intelligence architecture riding on a backbone of the TROJAN Data Network, as opposed to the Warfighter Information Network-Tactical (WIN–T) typically fielded within a brigade combat team. Modernization efforts intend to accommodate all warfighting function requirements via ubiquitous and redundant WIN–T systems; however, current capabilities fall short of providing on-the-move network connectivity or the anti-jamming and anti-scintillation capabilities desired of future network architectures.

Anytime a unit relies on tactical SIPR for connectivity within national to tactical intelligence, it needs to request firewall exemptions to access strategic SIPR. This applies across exercises and real-world operations, allowing support from higher echelons, theater intelligence brigades, and others within the intelligence community working on the strategic SIPR.

Within the WIN–T suite of communication technologies, the Global Broadcast Service enables intelligence cells to have a stand-alone capacity for receiving high-bandwidth data. When the S-2 section is trained and ready to implement its Global Broadcast Service capability, the section can support full motion video downlinks, high-resolution graphics, and the receipt of additional data sources (as well as the all-time favorites—MSNBC, Fox News, and CNN!). Although the Global Broadcast Service provides critical capabilities in the absence of other shared resources, these capabilities notably provide only one-way communication. They are not a means to transmit.

If the PACE plan uses different equipment with an array of vulnerabilities and resiliency, redundant communication capabilities enable coordination despite any number of enemy actions targeting command and control nodes. The unit should choose an assortment of capabilities. These can include multiple radio networks, trailer-mounted satellite antennas, small satellite antennas, mounted and/or dismounted position location information systems like the Joint Capabilities Release, Blue Force Tracking, Force XXI Battle Command Brigade and Below, Integrated Tactical Network, or Nett Warrior, and physical means like the ever-reliable "runner." Along with the myriad categories of primary systems, units should also maintain their supporting and enhancing antennas and related devices in order to maximize the range and effective use of the available systems.

The system of systems that a unit chooses affects the timelines for setup and teardown. This timeline, combined with the distance and duration of moving the command post, affects how long the command post will be out of the fight and unable to provide intelligence support. This relates to some of the requirements for before, during, and after jumping command posts, which will be discussed later in the article.

Units must invest in time and resources to ensure Soldiers can set up and maintain the upper tactical internet. A unit's dedication to communication enables it to quickly set up, tear down, move, and re-establish using any number of systems. Because intelligence sections often rely on the network backbone, it is imperative that intelligence Soldiers know the network architecture and equipment. The extent of that knowledge affects how robust the intelligence architecture will be and how the available bandwidth affects its overall data throughput. The signal section bears the burden of establishing the network, but the onus of the other components of intelligence architecture falls on the intelligence warfighting function, specifically the intelligence and electronic warfare sections. One of the means to account for this knowledge is institutional learning like that provided in the noncommissioned officer and officer education systems and additional schools like the Battle Staff Course.

Intelligence personnel can set up military intelligence systems at the same time the signal Soldiers establish the network. Within that framework, DCGS–A is the program of record and the heart of a robust intelligence architecture. There tends to be overreliance on the limited population of 35Ts (Military Intelligence Systems Maintainers/Integrators) within units as many military intelligence Soldiers may be unable or unwilling to take responsibility for their own primary weapons systems.

Before discussing other pieces of intelligence architecture, let us examine some tactics, techniques, and procedures and practices that maximize a unit's flexibility and mobility while maintaining DCGS–A in the tactical fight. The BISE provides some unique capabilities that complement the intelligence and communications architecture within a brigade. There is also an extensive communication capability within the multifunction platoon. However, the limiting factor for these capabilities is often the lack of knowledge or overreliance on national to tactical intelligence. A recurring trend during JMRC rotations is that brigade S-2s do not know the totality of functions, equipment, capabilities, personnel, and resources they have at their disposal.

Furthermore, some legacy mindsets carry over from counterinsurgency operations, such as particular uses of national technical means of collection, and the types of national to tactical intelligence used in the U.S. Central Command's area of responsibility over the past decade. It would be better to internalize the nuances of decisive action fights with peer threats and use assets within the span of control of the brigade combat team, or at least the supporting division.

Combat Training Center Best Practice

Brigade combat teams use organic collection assets with particular emphasis on scouts, cavalry elements, and other ground-based collection assets.

At the outset of any mission set or rotation, the S-2 section and military intelligence company must conduct a detailed mission analysis that specifically addresses a communication infrastructure for national to tactical intelligence. The S-2s and S-6s should address three areas in this portion of mission analysis:

- First, determine the sort of communication platforms suitable for every form of traffic. Digital platforms are obviously better for passing graphics, compared to voice platforms, which are better for synchronizing.
- Second, establish a robust, redundant, and resilient PACE plan. Units need digital and analog PACE plans. Relying on one or the other often leads to failure. Additionally, attempting to force information over an unsuitable medium will result in frustration and missed opportunities. All too often, units post time-sensitive information in accordance with their digital PACE plan but fail to confirm receipt of the targetable information by the proposed action-arm. Analog development of similar information may find its mark but conflicts with issues of timely dissemination.
- Third, address priorities of work. Which communications platform must be operational first, and which should be second? Although many systems can be established simultaneously, several require the expertise of a limited population. This must be clearly defined, lest the 35Ts be ineffective.

Many brigades have experimented with different configurations of their BISE and S-2 sections with varying degrees of success. One common theme is a split-BISE. This option has some advantages with respect to survivability but also has shortcomings regarding troops to task and redundancy of capability. To be effective, both elements must have a similar communications capability and enough Soldiers from each discipline to perform BISE functions at each location. Lastly, each section must have a clear mission and intent, detailed standard operating procedures for production, and a checklist to enable battle handovers.

Combat Training Center Best Practice

Clearly define roles, responsibilities, and deliberate placement of intelligence elements akin to considerations of command posts.

Within the pool of military intelligence talent and capabilities, Digital Intelligence Systems Master Gunners (DISMGs) can help bridge gaps and generate options. DISMGs maximize the intelligence architecture and provide both situational awareness and know-how to the S-2 because they are specifically trained on managing digital systems. They have additional training and skills that allow them to advise how to create and maximize intelligence architectures. Their insights are paramount when planning to adjust the architecture and critical when forced into unplanned adjustments to the architecture (whether imposed by adversaries, adverse conditions, maintenance, or user errors). DISMGs also receive training on DCGS–A, which is useful when 35Ts are already stretched so thin.

Combat Training Center Best Practice

Identify DISMGs as intelligence section master trainers.

Because there are many ways to establish the upper tactical internet, almost no bounds exist as to the detail, size, or scope of digital products that can be shared. Real-time integration via Command Post of the Future and similarly synched systems becomes possible. Intelligence sections can send and receive ultrahigh definition images; stream video for processing, exploitation, and dissemination; and use other high-bandwidth means of furthering commander visualization and situational understanding. Units do not plan to fail—they fail to plan, at least with respect to an informed and deliberate PACE means of communication.

Common Operational Pictures, Common Intelligence Pictures, and the Not-So-Common

Related to the capabilities inherent within the different command nodes, the primacy of analog or digital affects what is required to maintain the COP and/or common intelligence picture, and it plays a significant role in sustained and uninterrupted intelligence support.

Commanders have many reasons to prioritize digital or analog production, but they are virtually all influenced by the speed, consistency, and ease of establishing the upper tactical internet. Digital COPs have the ability to layer data and incorporate graphics more seamlessly than do analog products, but they require the systems on which they reside. Another substantial consideration is how fast they can be updated; few COP updates are quicker than the S-2 grabbing a red marker, taking a few steps, and annotating updated enemy battle positions in response to an important incoming report.

Bearing in mind the difficulty in establishing the means to maintain a digital COP, many commanders opt for both analog and digital COPs; nevertheless, one of them typically has primacy. The tactical operations center's standard operating procedure should specify which is to be updated first. There is necessarily a cost comparison between the speed, ease, and dependability of an analog COP, and the detail and depth of a digital COP. Assorted best practices for each become salient while observing combat training center rotations.

Time and resource constraints relegate or enable one to create a hasty or deliberate COP. Although nondoctrinal, this is a relevant framework for considering the detail that goes into the COP; if time is available, it is beneficial to develop the best and most concise picture to maximize commander visualization and understanding. All too often, S-2s and G-2s are initially pressed for time but neglect to go back and add detail and depth whenever they have an opportunity.

Some aspects of COPs apply to both analog and digital. Standard operating procedures should address the templates, formats, and PACE plans for sending updates and accounting for differences in available systems among subordinate, adjacent, and higher units. Additionally, developing the information early enough so that it may be useful to recipients requires intentional, early investment in product refinement during the military decision-making process and rapid decision-making and synchronization process, and when the information is available to update running estimates. Situational templates and event templates need to be available early enough to inform and shape the development of operational graphics and the unit's plan. It is necessary to communicate substantial changes to the assessments clearly, so that graphics can remain common across the formation.

Considerations unique to using analog COPs include whether additional staffers are available to make copies of overlays. In the alternative, the subordinate units may need to generate their own copies using "runners."

Combat Training Center Best Practice

Use night shift staff and drivers of key personnel to make analog copies; this minimizes the impact on current operations and others during high operating tempo.

Another consideration unique to analog products is whether to maintain enemy information as an overlay to the main COP or within a separate Red COP. The tactical operations center's ergonomics necessarily influence some of the aspects bearing on this decision. Depending on the accessibility of the main COP, availability becomes a concern. Because the S-2 has direct control of the Red COP, he or she has immediate access to annotate known and assessed locations and other enemy data, which ultimately allows the staff to multitask. The downside of a separate Red COP is the difficulty in comparing operational plans with assessed enemy courses of action. For this reason, finding a means to use the Red COP as an overlay, or generating overlay copies of the Red COP, enables both the plans cell and additional military decision-making process/rapid decision-making and synchronization process.

To the credit of digital COPs, and something that must be mitigated when using analog COPs, is the extent to which reporting may be an update to an already plotted element, and the need to deconflict this otherwise duplicative information. DCGS–A functions to correlate new collection against known entities within the Tactical Entities Database, and it provides updated geolocation data. Decisions about whether to add enemy graphics to the Red COP, or to erase or move existing enemy information, must be deliberate.

While analog production has the greatest potential for expedient adjustments to the main COP, a significant number of opportunities for human error and "fat-fingering" also exist with respect to unit locations and logging all reports. Digital COPs offer the potential for automation from collection to depiction and, at the very least, allow copy-and-paste functions, which mitigates some of the opportunities for human error that are present in analog COPs.

By their very nature, digital COPs depend on the architecture that supports them. Because they tie into data streams and can access large amounts of information, a different degree of knowledge management is required. Beyond determinations about the Five Ws for recording information, knowledge managers must take additional care regarding the access and rights to manipulate the COP. Whether using assorted software packages like the DCGS–A suite, Command Post of the Future, or Joint Capabilities Release, it may be necessary to limit rights and access to prevent others from deleting, corrupting, or confusing the COP, thereby making it inefficient.

Knowledge management needs to be deliberate and unit-specific at echelon. Units can gain power and efficiency when everyone in the unit has write-privileges and can contribute. For example, if the frontline units observe enemy activity across 10 different locations simultaneously, and all have the access and training required to update the digital COP, knowledge management can be done without any middlemen or delay. Conversely, if everyone has rights but not sufficient training, those same individuals, in an attempt to help, might cause confusion or add significant delays to information and knowledge communicated via the COP. Furthermore, if the unit fails to control access, the COP could fall into enemy hands, and they might use deception operations or delete it wholesale.

There is something to be said for consolidating control of the COP within the staff sections best suited to bring the information together and make assessments. Whether, and to what extent, COP management diffuses across the staff, or whether only the battle captain and the S-2 have privileges, is up to the unit. Given the task organization, time constraints, and levels of risk deemed acceptable after other considerations discussed, a best practice for a primary and alternate for each of the Red and Blue COPs is to have extensive training in managing the COP, with as many additional personnel as feasible.

Determinations of primacy between analog and digital COPs significantly affect the ability to transition intelligence support responsibilities between nodes because analog updates must be made at each node. A single node can maintain a digital COP and update the information available to all outstations in near real time. For this reason, digital COPs have a greater tendency to be "common," while reliance on analog COPs is prone to every command post having a different, "non-common" operational picture. Command posts and intelligence elements potentially prioritize information disparately, leading them to record, depict, and analyze different information.

Intelligence Before, During, and After Command Post Jumps

Deliberate consideration within the military decision-making process and wargaming provides insights to the communications and mission command capabilities that a main command post provides, while also identifying likely enemy activity associated with potential, preplanned locations. This leads to a commander's assessment of risk and decisions regarding when and where to jump the main command post.

Combat Training Center Best Practice

Where should command posts be located?

- Close enough to have communications until the next preplanned move.
- Somewhere safe and secure (defensible terrain and active security plan).
    - o Away from natural lines of drift and observation.
    - o Away from other unit locations that might give away their position.

Before the Jump. The first step leading up to jumping the command post is determining whether the command post ought to be jumped. This begins early in the planning phase and is clarified during the military decision-making process. When considering various factors of effectiveness and survivability, the staff should include recommended criteria and/or times indicated in the concept of operations to determine whether the main command post should jump—all of which is incorporated in the decision support matrix. If the commander does not use formal decision support matrixes, or decides main command post jumps do not warrant additions to the decision support matrix, the staff should develop a separate, internal main command post decision support matrix or similar product. This triggers staff discussion about jumping the command post, provides forewarning about likely upcoming main command post jumps, and otherwise increases readiness by reducing the main command post's need to react to jumping the command post.

Combat Training Center Best Practice

Preplan command post jumps and identify the criteria that drive them.

The staff should conduct thorough coordination before the command post jump, and they should arm the commander to make an informed decision whether and when to jump. The earlier discussion regarding network architecture plays a large role in the feasibility of jumping the command post, and each consideration in determining the architecture also becomes a consideration for whether, when, and where to jump the command post. The transition plan should clearly delineate the roles and responsibilities of each command post, including the extent to which intelligence support responsibilities shift to alternative nodes during the command post jump. Units should use clear standard operating procedures to establish redundant capabilities across differing nodes.

Intelligence personnel should coordinate with the operations command sergeant major and signal officer regarding the reasons and triggers for jumping the command post. Early planning can allow time to generate potential command post locations and allow the S-2 and S-6 to vet the locations for suitability and survivability, determining whether they are viable and vulnerable. The S-2 should consider the threat situation affecting the command post in the current location and set of conditions, and the threat during the transition. Transition assessments should include route security and vulnerability to all forms of contact, not the least of which is visual observation, which often precedes other forms of contact on the command post during or after the jump. The signature of the command post with respect to its size, concealability, and emissions, such as noise, light, and electronic warfare, also plays a large role in the overall vulnerability.

Meanwhile, the S-6 should conduct a line of sight analysis to confirm or deny whether the PACE means of communication can be established and the longevity of the communications structure in the new location. The commander should consider how long the proposed command post location would enable good communications with which to manage the fight before having to jump again.

Part of having defined roles and responsibilities includes specific actions in support of command post jumps. Sections must conduct intelligence handovers to allow continuous support and they should be codified. This requires the respective nodes of intelligence support to notify and acknowledge the shift in responsibilities, pass the running estimates, if not already communicated, and relay additional updates and considerations not accounted for within the standard operating procedure.

Combat Training Center Best Practice

Deliberate intelligence handovers are codified in the standard operating procedure. Conditions are met before breaking down the main command post, to include sharing current assessment, control of ongoing collection management, and anticipated enemy contact.

During the Jump. Even after the intelligence element with the jumping command post transitions its general intelligence support requirements, it needs to maintain as much situational awareness as possible in order to inform the convoy of any threats in the area and provide input to the command post until it can reestablish and resume control of the fight. Contemporaneous with the command post reacquiring the reins, the intelligence section similarly resumes the position to provide primary intelligence support. The jumping intelligence element strives to receive information and assess the enemy situation, but doing so may require a separate PACE plan for the duration of the jump, or at least moving to a different part of the PACE plan until the command post is reestablished. Lastly, the quicker the command post jumps, the more it mitigates the effects of degraded communications on intelligence support to the unit.

Depending on talent management, development within the section, and capacity of other intelligence professionals across the organization, the transitions among command posts and intelligence nodes may have minimal effect on the overall intelligence support; however, a potential for degraded support exists and should be considered when making manning determinations, both at the outset and as changes are required.

Every element of intelligence personnel has some capacity to contribute to plans, future operations, current operations, and/or battle tracking. Depending on the available manpower and individual skills, commanders or S-2s may make different decisions to determine which nodes to use, how many personnel are at each node, and who is at each node to ensure the right mix of personalities, capabilities, and command post operations.

After the Jump. Similar to the considerations that necessitate alacrity when moving the command post, the unit needs to set up their systems swiftly. For the command post personnel to be quick and efficient, they should regularly practice at home station and in exercises. If the organization develops proficiency, it can resume primary roles and responsibilities within the command post in a fraction of the time it takes unpracticed units to jump the command post.

After gaining access to current information channels, another intelligence handover should happen—the reverse of what was done when the primary passed the responsibilities to the alternate. The S-2 should then reassess the situation and incorporate information and assessments from the intelligence handover. Once this is completed, the S-2 can reassume primacy for intelligence functions.

Conclusion

Across the Army, leaders are high-caliber, smart individuals, but command post transitions tend not to be part of their schema for important, pre-operation planning. Deliberate and informed preparation facilitates reliable and resilient communications to maximize capacity throughout the fight. Using this connectivity allows greater use of digital COPs and wargaming. The use of analog production better enables the staff to contribute to commander visualization and situational understanding. Command post jumps, while largely affected by communications and COPs, require consideration of other factors as well. Jumping the command post should not be taken lightly, and a deliberate and informed staff is best able to support the commander's decision on whether and when to jump. When that decision is made in the affirmative, knowing the options and conducting thoughtful planning lets the unit minimize negative impact, expedite the process, and bring about near-seamless transitions.

Endnotes

[1] Department of the Army, Field Manual 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. Government Publishing Office, 5 May 2014), 1-1. Change 1 was issued on 11 May 2015. Change 2 was issued on 22 April 2016.

[2] Ibid.

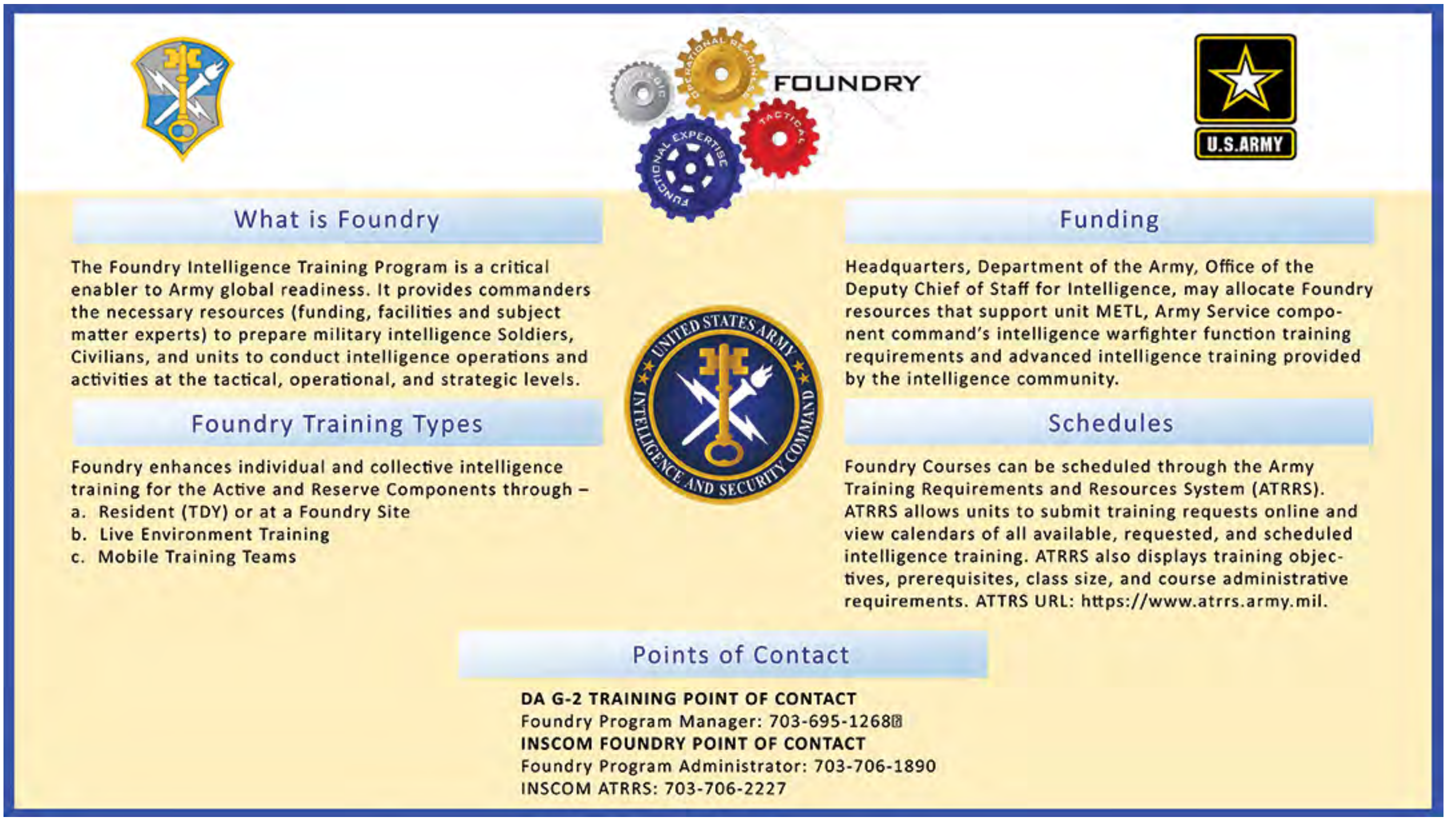
[3] Ibid., 1-2.

[4] Ibid., 1-3.

MAJ Jared N. Ferguson is the brigade intelligence trainer for the Joint Multinational Readiness Center (JMRC) at U.S. Army Garrison, Hohenfels, Germany. He has observed, coached, and trained ten U.S. and North Atlantic Treaty Organization brigades and three division intelligence sections. He commissioned as an infantry officer in 2004 with a bachelor's degree in history, later completed a master's degree in international relations, and received a graduate certificate in security assistance. Positions that MAJ Ferguson held while in the infantry include platoon leader, executive officer, and commanding officer. After transitioning to military intelligence, he served as a brigade S-2X, battalion S-2, brigade assistant S-2, and brigade S-2. His deployments include Afghanistan and Iraq.

CPT Jeff W. Linzey is the battalion intelligence trainer for the Timberwolves Team at JMRC, Hohenfels, Germany. He commissioned in 2008 through the Reserve Officers Training Corps, California State University at Fullerton. His prior assignments include Task Force Deputy J-2 (AFG), unmanned aircraft system platoon leader, battalion S-2, Army Service component command analyst and team chief, Deputy J-2 (TCD), and commanding officer. CPT Linzey has a bachelor's degree in English and a juris doctorate.

CPT Casey L. Coyle is the signal and mission command observer, coach, and trainer for the Timberwolves Team at JMRC, Hohenfels, Germany. Before his assignment to JMRC, he participated in five combat training center rotations divided between the National Training Center and the Joint Readiness Training Center. Additionally, CPT Coyle is Mission Command Digital Master Gunner certified. He served as the 6th Squadron, 1st Cavalry Regiment S-6 for 18 months in 1st Stryker Brigade Combat Team, 1st Armored Division at Fort Bliss, TX. While deployed in Afghanistan, CPT Coyle was the G-6 for the Train Advise Assist Command Southeast in Gardez province.


FOUNDRY
STRATEGIC
OPERATIONAL READINESS
TACTICAL
FUNCTIONAL EXPERTISE
U.S. ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND

What is Foundry

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

Foundry Training Types

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

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

Funding

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

Schedules

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

Points of Contact

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

Targeting in Large-Scale Combat Operations

by Major Robin W. VanDeusen and Major Wesley N. Knight

Introduction

As professional U.S. Army officers, we conceptually understand that "intelligence drives operations." We understand that in order to eliminate enemy forces, we must first find them; however, identifying a near-peer adversary during combat operations is not easy. This challenging task leads many units to have difficulty translating conceptual understanding of the enemy into detailed action. The focus of this article is to share common observations of the link between intelligence collection and fire support at the National Training Center. This link helps provide the necessary detail to support targeting. More importantly, we seek to display how units can effectively strengthen that link to increase their ability to shape the battlefield for their maneuver commanders.

Enable the Intelligence Section to Provide Necessary Support

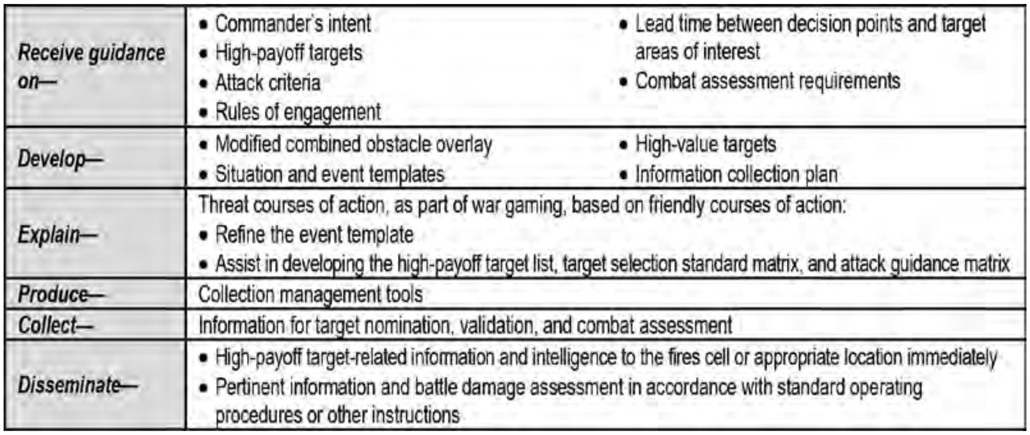
For a brigade that receives a mission and begins the military decision-making process (MDMP), FM 2-0, *Intelligence*, clearly lays out certain actions that will help enable the intelligence section to provide necessary support to MDMP and to the brigade's targeting cycle. However, many units do not execute these actions as a matter of routine standard operating procedure. A few examples worth noting are that during the MDMP's Step 1 (Receipt of Mission),[1] some units do not actively "use intelligence reach to collect updated or additional enemy, terrain and weather, and civil considerations data."[2] They request this data later in the process, when they actually need to have it available for integration into their overall analysis. Terrain and weather will not only influence how the enemy will fight but will also affect the employment of airborne and human sensors. Additionally, as units transition between operations, staff sections must keep their running estimates up to date. The S-2 section is no different. Although the S-2 captures a majority of their running estimate in the intelligence preparation of the battlefield, they must account for important considerations such as the status of unmanned aircraft systems or other collection assets and communication status with higher and subordinate echelons. This information feeds directly to the S-2 planners and S-2 targeting personnel so that they can conduct mission analysis (and more specifically intelligence preparation of the battlefield) with the latest available information in a constantly changing environment.

FM 6-0, *Commander and Staff Organization and Operations*, states, "Since no amount of subsequent planning can solve an insufficiently understood problem, mission analysis is the most important step in the MDMP."[3] This statement further emphasizes the importance of intelligence preparation of the battlefield that allows the intelligence professional not only to influence the quality of the overall maneuver plan but also to enable effective targeting by the fires, aviation, and maneuver. The brigade begins developing the key products for supporting targeting during mission analysis, refines those products during course of action (COA) development, and synchronizes those products with the maneuver and fires plans during COA analysis.

Key Products that Support Targeting

FM 2-0, *Intelligence*, describes the key products required to support targeting, but some of the nuances of these requirements are unclear. In addition to listing "modified combined obstacle overlay," the "develop" section of FM 2-0's table 2-3, shown on the next page, lists as required products—

- situation and event templates,
- high-value targets, and
- information collection plan.[4]



Receive guidance on—	• Commander's intent • High-payoff targets • Attack criteria • Rules of engagement	• Lead time between decision points and target areas of interest • Combat assessment requirements
Develop—	• Modified combined obstacle overlay • Situation and event templates	• High-value targets • Information collection plan
Explain—	Threat courses of action, as part of war gaming, based on friendly courses of action: • Refine the event template • Assist in developing the high-payoff target list, target selection standard matrix, and attack guidance matrix	
Produce—	Collection management tools	
Collect—	Information for target nomination, validation, and combat assessment	
Disseminate—	• High-payoff target-related information and intelligence to the fires cell or appropriate location immediately • Pertinent information and battle damage assessment in accordance with standard operating procedures or other instructions	

Intelligence Support to Targeting[5]

However, the "explain" section of table 2-3 lacks the necessary specificity that intelligence sections may overlook or misunderstand while supporting targeting. In an attempt to provide the necessary clarity, we will focus on the three products previously listed in terms of required outputs of those products and their interaction with brigade-level targeting.

Situation Template and High-Value Targets. Beginning with the situation template, the product should contain all the normal requirements such as mission, task/purpose, and general orientation on the overlay. The S-2 needs to emphasize the enemy high-value target list and the ways those targets will conduct operations in the coming fight. An example of a high-value target list could be the enemy exploitation force. This mix would appear as 10 T-90 battle tanks and 18 BMPs (*Boyevaya Mashina Pekhoty,* or infantry fighting vehicles) and serve as the enemy commander's decisive operation. Now that the briefer has identified the element, he must explain the exploitation force in time and space.

Event Template. In order to aid the briefer and visually display the enemy in time and space, the S-2 must use the event template. The event template depicts the amount of time an enemy will take to move from one point along its avenue of approach until it reaches its objective. It is important that the event template use time phase lines or incremental timing points. This graphical depiction of enemy maneuver with associated times provides the necessary information to the rest of the staff to begin requisitioning detection and delivery assets for finite windows of time.

Information Collection Plan. This depiction of enemy movement in time and space now leads to the last required product—the information collection plan. The first step in developing the information collection plan is placing named areas of interests (NAIs) over key weapon systems and/or locations where enemy COAs may differ in order to answer priority intelligence requirements (PIRs) or support targeting. The S-2 uses NAIs to answer PIRs focused on confirming or denying the enemy's COA. Doctrinally, PIRs are a type of commander's critical information requirement that are "identified by the commander as being critical to facilitating timely decision making."[6] Information collection assets, in the form of human sensors, like the brigade cavalry squadron, and as airborne intelligence, surveillance, and reconnaissance (ISR) platforms, will collect according to these NAIs based on the commander's PIR. From a targeting perspective, using the Army's decide, detect, deliver, and assess methodology, all detect assets are also tied to the commander's PIR, which we will discuss later.

Once the collection manager places the NAIs on the overlay, the collection manager starts aligning assets based on capability and availability to observing these NAIs, creating the information collection synchronization matrix. The graphical depiction of NAIs and arraying of assets in time against those NAIs serves as the foundation for the information collection plan. Returning once again to our example of the enemy exploitation force, the collection manager will add NAIs over the templated location and key chokepoints or intersections along the anticipated route of march.

Proper Target Value Analysis

Once the unit identifies key enemy high-value targets and appropriately aligns a collection plan against those targets, they transition to seeing if they need to add the high-value targets to the high-payoff target list. Often, units overlook the importance of proper target value analysis (TVA) in understanding how elements on the high-value target list will fight and in understanding their vulnerabilities. ATP 3-60, *Targeting*, describes TVA as a responsibility of the G-2 at the division level, but doctrine does not clearly assign responsibility for TVA at the brigade level, which often results in no or incomplete TVA. TVA should be a shared effort between the brigade's targeting officer and the S-2 emphasizing, "detailed analysis of enemy doctrine, tactics, equipment, organizations, and expected behavior for a selected COA."[7] This analysis will aid the staff in better understanding how to develop the necessary guidance to attack high-value targets, as well as understanding their importance to the friendly commander's COA. This aids in determining which targets are high pay-off targets during COA development. By definition, a high-payoff target is "a target whose loss to the enemy will significantly contribute to the success of the friendly course of action."[8] The S-2 and targeting officer must consider time available in their TVA and have to apply a certain degree of judgment to ensure they are conducting analysis on the proper high-value target sets that the brigade can affect in near-term, upcoming operations (usually in the next 24 to 48 hours).

During COA analysis, or wargaming, the brigade staff finalizes synchronization of the information collection plan with other aspects of the enemy's actions (including suspected reactions to friendly actions), and the maneuver, fires, and airspace plans. They confirm the draft brigade high-payoff target list created during COA development now that they are able to visualize in time and space what target sets friendly elements must destroy in order for the maneuver commander to achieve victory. With this understanding, they confirm that templated NAIs and target areas of interest (TAIs) make sense according to likely friendly and enemy actions. Moreover, they also confirm that lethal and nonlethal delivery assets planned during COA development remain properly aligned in time and space to achieve the commander's desired effects. Proper TVA from earlier in the process will also inform the brigade staff as it develops target selection standards and attack guidance for those targets on the high-payoff target list.

Figure 1 shows the enemy exploitation force from the example. In the figure, the brigade would establish NAIs to confirm or deny the enemy route of march along multiple avenues of approach. When the brigade detects the enemy in NAI 2, via ground moving target indicator, this triggers cross-cueing from the brigade's Shadow unmanned aircraft system to confirm that it is indeed the exploitation force. When the Shadow sees the enemy exploitation force cross NAI 4, this provides confirmation that the exploitation force is committed to the southern route, COA 2. When the exploitation force crosses NAI 6, this triggers a call for fire from cannon artillery on TAI 2. The time it takes the enemy to move from NAI 4 to TAI 2 will be the planned amount of time required by the field artillery to process and deliver the call for fire on TAI 2.

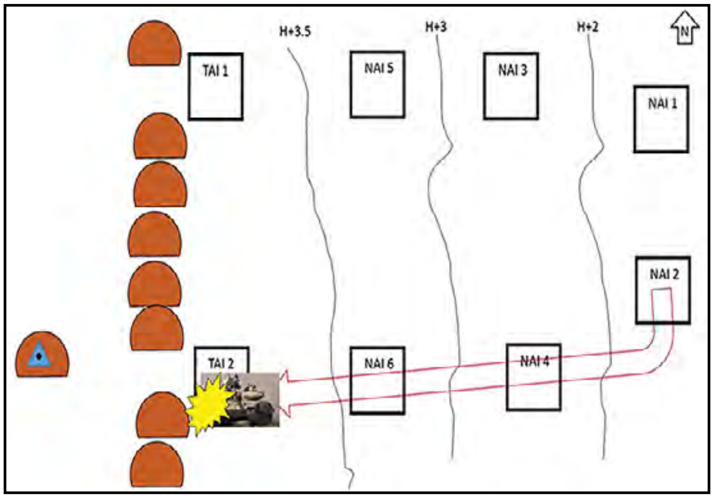


Figure 1. Enemy Exploitation Force

In this example, the brigade uses the terrain and threat analysis conducted by the S-2 to determine the location of a TAI in a chokepoint along the enemy's most likely avenue of approach, making attack by organic cannon artillery more feasible. During the TVA, the brigade used its TVA to determine that the exploitation force would have to slow or stop before the attack for the brigade to achieve effects with cannon artillery. Using the attack guidance matrix derived from the TVA, the brigade combat team determined it would need to fire all 18 cannons with 12 rounds each of dual-purpose improved conventional munitions to neutralize the exploitation force in accordance with the commander's intent. Additionally, during COA development and COA analysis, as part of the information collection plan, the brigade assigned a human observer to an observation post overlooking the TAI.

As the final aspect of the information collection plan, the brigade must also align an asset to assess the results of the engagement. In this example, the observation post can accomplish this task. If we destroy 10 percent of the exploitation force (one T-90/two BMPs), the S-2 can assess that the brigade neutralized the enemy exploitation force, and the enemy will now commit its reserve. However, if nine T-90s remain, this target may require re-attack with cannon, re-attack by dynamic re-tasking of other available assets, or some other pertinent decision that the brigade commander will make.

High-Payoff Target Lists

Although some may see the discussion of PIR and targeting as separate topics, a clear linkage exists. We already understand the stated doctrinal relationship between NAIs, PIRs, and decision points in that NAIs should link to specific PIRs that subsequently link to specific decision points for the commander. However, doctrine does not clearly delineate the relationship between decision points and high-payoff targets. Since all brigade detection assets are assigned task and purpose in accordance with the PIR, the relationship between commander's decision points and high-payoff targets logically follows. Often, brigades do not focus their high-payoff target list according to what the commander needs for mission success. This results in broad high-payoff target lists that lack the required focus and analysis. A good measure of effectiveness that we suggest to ensure brigades focus their high-payoff target list is to confirm that the destruction of brigade high-payoff targets links directly back to brigade decision points. This does not mean the brigade cannot attack targets of opportunity throughout the battle, but it does focus brigade assets on those targets deemed vital to the success of the friendly commander's mission. We can see an example of this high-payoff target linkage to a decision point in our earlier exploitation force example. Once we complete the decide, detect, deliver, and assess methodology and we neutralize the exploitation force, logically this would lead the commander to transition from a defensive posture to the counterattack phase of the operation.

Importance of the Intelligence Collection/Fires Rehearsal

Thus far, this article has focused on the critical planning steps involved in effectively linking intelligence and fires to achieve effective targeting. We would be remiss if we did not mention the importance of rehearsals as the last step in the process to ensure execution success. The intelligence collection/fires rehearsal is where all the pieces in the example above come together. Ideally, the intelligence collection/fires rehearsal is not a wargame. The critical synchronization already occurred in the wargame. The rehearsal is to ensure all parties have a common understanding of how the brigade intends to attack high-payoff targets throughout the depth of the brigade's area of operations. Although a proper information collection/fires rehearsal will also cover essential considerations for brigade targets such as smoke and obscuration, that is outside the scope of this article. For our purposes, the information collection/fires rehearsal must clearly delineate the brigade's deep and close fights through a clear understanding of the coordinated fire and intelligence handover lines and the triggers that will cause them to shift.

Moreover, we must discuss the relationship of intelligence sensors to delivery assets (sensor to shooter) and the approach to assess that target set in detail. For example, in the exploitation force example, the information collection manager should discuss the collection plan in time and space according to what PIR the brigade will be collecting on with the Shadow. The information collection manager will then explain how the detection of eight T-90s and ten BMPs in NAI 4 confirms enemy COA 2 and answers PIR 1 ("Where will the enemy exploitation force attack?"). Then, when the enemy crosses into NAI 6, the information collection manager will explain how the Shadow operator communicates via Transverse Chat to the brigade's intelligence current operations and immediately relays this information to the brigade fires cell, triggering them to inform the observation post to call for fire on TAI 2. The observation post then simulates a radio transmission of that call for fire all the way to the cannons, which then fire the mission. Then the observation post will simulate a radio transmission ending the call for fire and relaying the battle damage assessment for the mission. The brigade fires cell then states the criteria to re-attack or to dynamically re-task other assets; or it may indicate whether the lack of enemy battle damage will initiate a commander decision point, such as committing the reserve. The staff should then re-rehearse the plan—considering various friction points such as having to use alternate or contingency communications methods, alternate observers, and alternate delivery assets.

Don't Chase the Shiny Object

It is also important to note that the brigade must resist the temptation to "chase the shiny object"; it must keep its collection plan focused on the brigade's deep fight. During recent counterinsurgency operations, units tended to allocate all ISR resources to wherever maneuver units found themselves in a "troops in contact (TIC) situation." In the decisive action fight, everyone is in a "TIC." The brigade does not have the resources to look at everything and must adhere to the brigade commander's collection plan. Likewise, brigade assets cannot range anything in the division's deep area; therefore, it does not make sense to attempt to collect in the division's deep area. The brigade should leverage the division to provide critical information, such as information needed for transitions, from its deep area.

Conclusion

The process of linking a sensor to a shooter and achieving intelligence and fires integration is not a complex concept, but rather it is a simple one. The practice of properly planning, rehearsing, and executing is hard. Although the process may be hard, it is not impossible—it can be achieved by following doctrine and the unit's stated standard operating procedure. The simplified process is deciding upon which enemy to place lethal or nonlethal effects, detecting that enemy, using a delivery system to achieve those effects, and, finally, assessing the results. To achieve success, those planning sensor-to-shooter operations must move beyond conceptual planning and delve into the science of detailed planning. Attention to detail in planning and rehearsals pays significant dividends when the fires and intelligence warfighting functions are able to link their efforts to shape the brigade fight for the brigade commander.

Endnotes

[1] Department of the Army, Field Manual (FM) 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. Government Publishing

Office [GPO], 5 May 2014), 9-3. Change 1 was issued on 11 May 2015. Change 2 was issued on 22 April 2016.

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

3. Department of the Army, FM 6-0, 9-6.

4. Department of the Army, FM 2-0, 2-11.

5. Ibid.

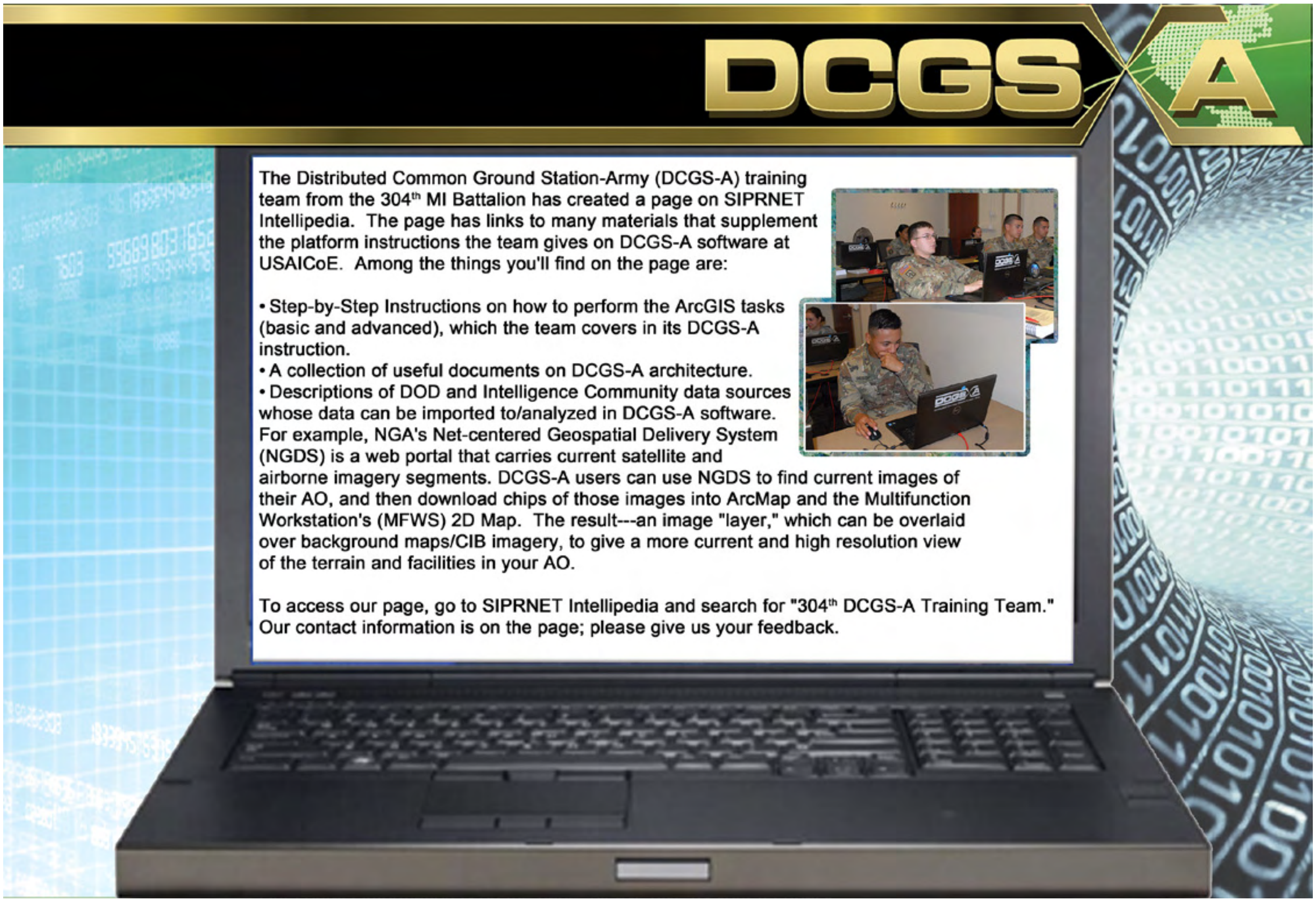
6. Joint Chiefs of Staff, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: U.S. GPO, 17 January 2017), III-13. Change 1 was issued on 22 October 2018.

7. Department of the Army, Army Techniques Publication 3-60, *Targeting* (Washington, DC: U.S. GPO, 7 May 2015), 2-3.

8. Joint Chiefs of Staff, JP 3-60, *Joint Targeting* (Washington, DC: U.S. GPO, 28 September 2018), I-10.

MAJ Rob VanDeusen is currently the brigade combat team fire support officer observer-coach-trainer at the National Training Center, Fort Irwin, CA. Previous assignments include field artillery battalion S-3 observer-coach-trainer and Strike Director, Combined Joint Operations Center-Baghdad, 101st Airborne Division. He has a bachelor of science in sociology from the U.S. Military Academy and a master of arts in management from Webster University.

MAJ Wesley Knight is currently the senior brigade combat team S-2 observer-coach-trainer at the National Training Center, Fort Irwin, CA. Previous assignments include 1st Stryker Brigade Combat Team, 1st Armored Division, S-2; and 1st Armored Division G-5 intelligence planner. He has a bachelor of science in political science from the U.S. Military Academy, a master of arts in national security and strategic studies from the Naval War College, and a master of military art and science from the School of Advanced Military Studies, U.S. Army Command and General Staff College.

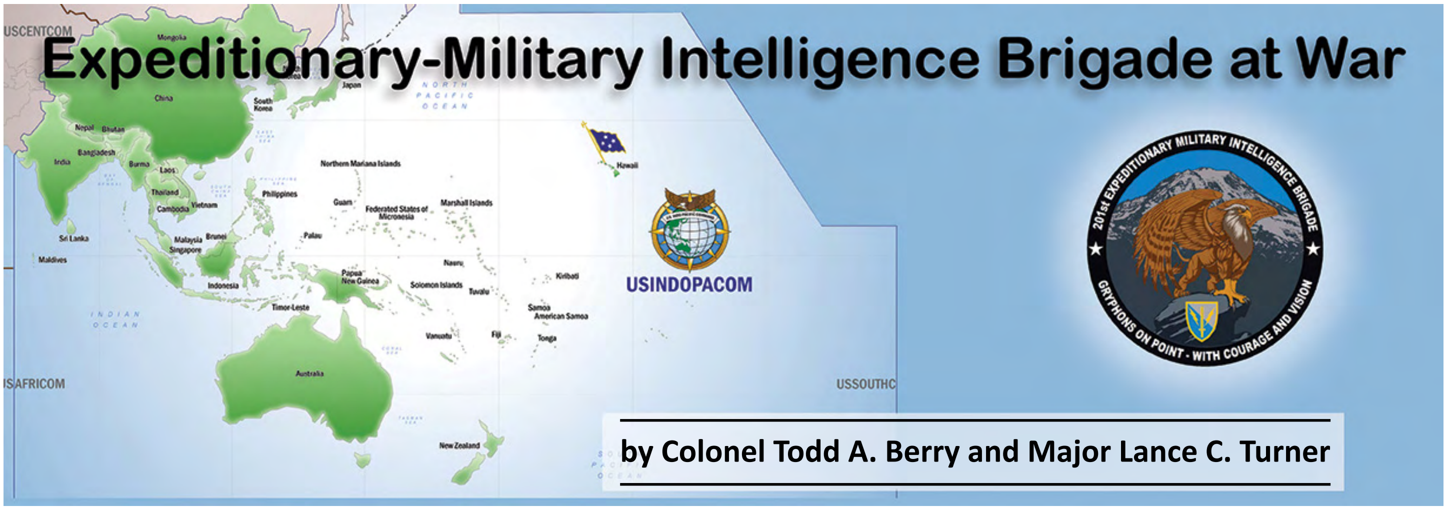


The Distributed Common Ground Station-Army (DCGS-A) training team from the 304th MI Battalion has created a page on SIPRNET Intellipedia. The page has links to many materials that supplement the platform instructions the team gives on DCGS-A software at USAICoE. Among the things you'll find on the page are:

- Step-by-Step Instructions on how to perform the ArcGIS tasks (basic and advanced), which the team covers in its DCGS-A instruction.
- A collection of useful documents on DCGS-A architecture.
- Descriptions of DOD and Intelligence Community data sources whose data can be imported to/analyzed in DCGS-A software. For example, NGA's Net-centered Geospatial Delivery System (NGDS) is a web portal that carries current satellite and airborne imagery segments. DCGS-A users can use NGDS to find current images of their AO, and then download chips of those images into ArcMap and the Multifunction Workstation's (MFWS) 2D Map. The result---an image "layer," which can be overlaid over background maps/CIB imagery, to give a more current and high resolution view of the terrain and facilities in your AO.

To access our page, go to SIPRNET Intellipedia and search for "304th DCGS-A Training Team." Our contact information is on the page; please give us your feedback.

Expeditionary-Military Intelligence Brigade at War


USCENTCOM
USINDOPACOM
USAFRICOM
USSOUTHCOM
NORTH PACIFIC OCEAN
INDIAN OCEAN
201st EXPEDITIONARY MILITARY INTELLIGENCE BRIGADE
GRYPHONS ON POINT - WITH COURAGE AND VISION

by Colonel Todd A. Berry and Major Lance C. Turner

Introduction

As the U.S. Army transforms the scope and breadth of its missions, military leaders may be left pondering, "How does the Army adequately shift its intelligence priorities from counterinsurgency operations and/or decisive action training environment to large-scale combat operations?" This article provides some possible solutions based on changes that the 201st Expeditionary-Military Intelligence Brigade (E–MIB) made to support its intelligence priorities for large-scale combat operations.

This article describes how leaders at the 201st E–MIB successfully shifted their training and readiness focus from the battlefield surveillance brigade to the E–MIB, and from the Central Command (CENTCOM) area of responsibility to the Indo-Pacific Command (INDOPACOM) area of responsibility. It will discuss the intelligence priorities and planning considerations required to redirect mission priorities from a counterinsurgency-centric fight to austere large-scale combat operations. This article includes insight into how the E–MIB integrates and supports the corps' shaping fight. It highlights significant learning points, such as the realization that while both theaters require the same basic planning considerations, the environment in which Soldiers and equipment operate may pose significant new challenges and may require entirely different training to ensure success. It also discusses environmental impacts that require learning new techniques for the area of responsibility to ensure a maximum state of readiness for intelligence teams and intelligence systems in the new theater.

Recent Evolution at the 201st Expeditionary-Military Intelligence Brigade

In mid-2017, the 201st E–MIB started its evolution from a counterinsurgency-focused unit to a large-scale combat operations–focused unit. The brigade deployed to Iraq and Afghanistan continuously for over a decade, first as a military intelligence brigade, then as a battlefield surveillance brigade, and later as an E–MIB. During deployments, the unit primarily gathered intelligence in an operational environment focused on counterinsurgency. In the summer of 2017, the brigade transitioned to a direct reporting unit subordinate to America's First Corps (I Corps) and concentrated on near-peer threats, primarily in the Pacific. The brigade also continued employing some of its skilled Soldiers and intelligence systems into the CENTCOM area of responsibility, while operating in a fairly stable threat environment, using a hardwired and stable intelligence architecture.

As a direct reporting unit to I Corps, the E–MIB has shifted its focus to near-peer threats in an unfamiliar operational environment, including a new focus on large-scale combat operations. The brigade and battalion commanders assumed the new role of chief of intelligence, surveillance, and reconnaissance (ISR) for both the corps and division commanders. The E–MIB commenced these changes with mild trepidation because the INDOPACOM area of responsibility comprises a vastly different terrain, weather, and threat, certainly different from the ongoing CENTCOM missions the brigade continued to conduct. Additionally, intelligence and communications architectures were initially limited. With these differences in mind, the unit adapted and overcame by creating new tactics, techniques, and procedures (TTPs), and revitalizing older methods of collection and exploitation.

As the training focus shifted, the 201st E–MIB's intelligence teams reorganized to better train and fight in an environment most units had never experienced. Two decades of constant rotations to CENTCOM had created a pattern of training, deploying, and fighting specific to one theater. Thus, the brigade revamped its training plan to prepare Soldiers to fight large-scale combat operations. Human intelligence efforts were reprioritized away from military source operations and toward traditional interrogation training to increase Soldiers' proficiency and meet theater requirements. The unit task organization was restructured to support the employment of expeditionary collection in a mobile and degraded environment. Multifunctional teams, comprised of both human intelligence and signals intelligence Soldiers, adjusted training to mimic individual and collective operations, depending on the phase and location of the operation, supporting brigade combat teams and below, as well as the corps' support area command post, while ISR operations supported corps and division echelons. These changes forced the creation of a new set of standard operating procedures. The standard operating procedures refinements were made for support to the corps, coalition forces land component command, and joint task force echelons. The E–MIB learned to fight as a decentralized unit, supporting multiple echelons within the area of operations. Additionally, the E–MIB learned how to remove the processing, exploitation, and dissemination architecture from the forward lines, and support from rear or home station locations as needed. This allowed constant analysis of the fight from the rear and front, creating redundant means for the commander to visualize the battle.

Figure 1 shows the E–MIB's concept of employment for large-scale combat operations. It outlines the task organization of an E–MIB and its direct support to corps, division, and brigade combat teams, as well as the support to the security area command post.

Integration of Multinational Partners

In addition to integrating intelligence assets, units tackled the integration of multinational partners into command posts. This required incorporating the operation of different networks to increase shared knowledge of the environment. Initially, this created unforeseen challenges. Multiple networks forced the units to double their workstations within the command post, restricting space within each cell, and degrading the capacity of network dataflow. Further, intelligence sharing over multiple networks created delayed response times for reports through various networks, often creating new responsibilities for Soldiers. From these challenges, the E–MIB learned the benefit of integrating liaison officers with multinational partners. The liaison officers mitigated the reliance on systems and built stronger relationships with partnered nations. To mitigate the lack of intelligence sharing, the brigade reached out and began sharing its needs and TTPs with the other E–MIBs.

Shared network usage presented another problem. Initially, there was a misconception about the usage of shared networks between the U.S. and coalition forces, leading to inaccurate planning assumptions. Other units were not using the networks to the extent that the E–MIB initially anticipated. When Soldiers attempted to retrieve intelligence information, it was lacking. These challenges affected shared knowledge across the networks, and forced Soldiers and leaders to engage their counterparts face-to-face throughout the operation.

Improving Organic Communications

A third issue was the lack of an adequate modified table of organization and equipment to allow for organic communications across the environment without reliance on another unit. Teams and Soldiers needed the means to deploy, collect, and fight at the lowest echelon, sometimes

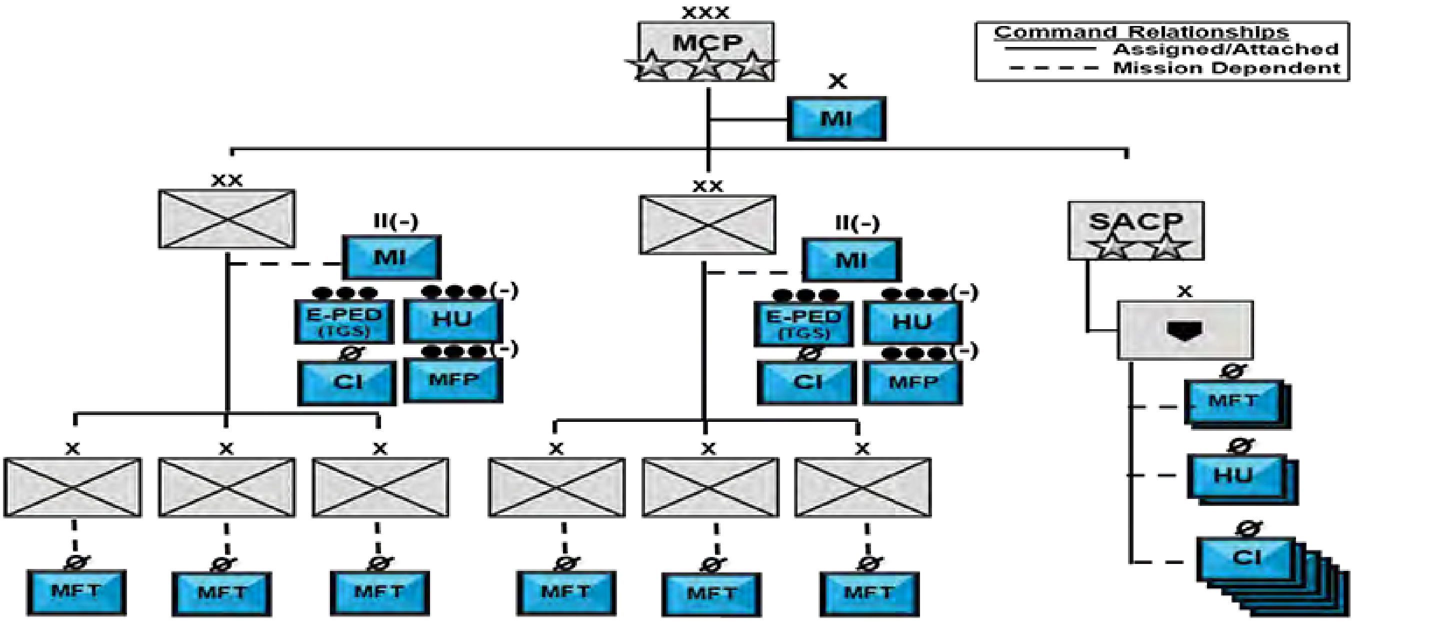


Figure 1. Task Organization of an E–MIB

Photo by SSG Keith Anderson

Soldiers from the 109th Expeditionary Military Intelligence Battalion, 201st Expeditionary MI Brigade, from Joint Base Lewis-McChord, collaborate on multi-disciplined intelligence collection, surveillance, and reconnaissance operations during Warfighter 19-01 at Schofield Barracks, Hawaii.

as a singleton, in order to be effective in theater. As the brigade began resolving its problems, it began to capture the solutions to these friction points by building unclassified standard operating procedures, TTPs, and other products. The brigade made all of its products available on the Nonsecure Internet Protocol Router Network to maintain continuity from one team to the next and to promote sharing among the intelligence community and its partners. This unclassified base product could then be modified for use on any network.

Live Environment Training to Increase Readiness

The E–MIB sent Soldiers and teams to different theaters to train on theater-specific standard operating procedures and TTPs and to collect information to increase situational awareness. One training opportunity that arose was the increase in live environment training. Live environment training events shed light on equipment shortages and highlight opportunities to increase readiness within a theater before combat operations. Live environment training became an enduring training practice. Units began to rotate multiple Soldiers in and out of theaters, replicating a mini-reception, staging, onward movement, and integration (RSOI), intelligence architecture simulation, and early stages of testing collection methods.

When live environment training events highlighted team shortfalls, specifically when tied to collection systems, the E–MIB began informing the intelligence community of critical shortfalls within its current programs of record and proposing potential solutions to the community. By identifying these shortfalls, these issues drove units to submit augmentation to their tables of distribution and allowances and/or request operational needs statements for mitigation.

Because of the ability to identify these real-world problems before deployment operations, live environment training rotations have become invaluable to the E–MIB. The benefits of sending signals intelligence, human intelligence, and counterintelligence Soldiers into theater to conduct intelligence operations with the military intelligence brigade-theater cannot be overstated. Thirty-, sixty-, and ninety-day rotations are vital to understanding how to connect into the theater's architecture and how to collect in the operational environment. This leads to a much clearer picture of how to fight in a particular theater and how to train for that fight.

During a recent live environment training opportunity in the Pacific in 2017, the E–MIB learned that connection issues added weeks to the reception and staging phases of RSOI. One significant challenge was connecting multifunctional team systems in an outside continental United States (OCONUS) environment. Other issues included operating on different frequency bands with no means to replicate at home station, problems with connections specific to OCONUS and INDOPACOM operations, and difficulties with maintaining equipment configurations specific to the area while having equipment available for deployments on order. Resolving these issues involved Soldiers in theater and home station, as well as civilians and contractors from multiple venues around the globe. While the E–MIB is working to identify solutions that are more expedient to positively impact time and resource management, currently it requires an unacceptable amount of time to obtain resolution.

Changing the Certification Environment

To mitigate these issues, the E–MIB changed the way it trains for combat. It executes two brigade-sized certification exercises a year, focusing on Tier 4 and Tier 3 echelons (which encompass individual and team level). Over the past 2 years, the brigade evolved the certification environment from counterinsurgency, to decisive action training environment, and now large-scale combat operations, increasing complexity at each exercise. These exercises certify multifunctional teams, human intelligence Soldiers, and processing, exploitation, and dissemination/tactical ground station platoons in accordance with their mission essential tasks, and are graded with training and evaluation outline reports. Each iteration brought new training opportunities, to include—

- Partnering with local units such as our Reserve Force E–MIB partnered unit and the brigade combat teams.
- Training with the military police.
- Integrating detention facility operations.
- Incorporating ever-more realistic training scenarios.

Meanwhile, the brigade and battalion headquarters are able to increase training complexity and relevancy at each major command post exercise with corps and division units. In this manner, the E–MIB and its subordinate units execute up to five external training iterations per fiscal year.

While the brigade overhauled its training efforts, it took the time to revamp its deployment readiness program too. Over the past 2 years, the E–MIB built a robust deployment readiness program that increased complexity for unit deployment readiness exercises. Because the E–MIB lacks organic transportation specialists and equipment, and must rely on corps echelons to deploy, each battalion trained and certified internal mobility teams to enhance deployment readiness across the force. The platoons, companies, and battalions ensured each level included redundancy in movement officers, air planners, and air/rail/sea teams, to support equipment preparation at various nodes. Conducting no-notice alerts became the norm, and units improved with each iteration. The units executed multiple increasingly complex multimodal deployment operations, becoming experts at their N-Hour deployment sequence checklists. They also executed rail, air, land, and sea deployment operations, honing their standard operating procedures with each iteration. These readiness exercises and practices ensure the E–MIB, as a whole, is ready to deploy to an austere theater at a moment's notice.

Conclusion

With the Army's redirection back to the Pacific and large-scale combat operations, the E–MIB evolved how it connects, collects, and trains to fight and win wars in support of maneuver commanders. The E–MIB grew as it revised internal doctrines to address identified issues and shortfalls, increase intelligence capabilities for the corps and divisions, and improve intelligence sharing across multiple networks, all in support of the corps' current guidance for shaping operations. Soldier and team feedback was vital to understanding variations in each operational environment. Often this feedback directly influenced new ways to equip, test, validate, train, and employ intelligence systems, Soldiers, and teams. It meant—

- Relooking past doctrine.
- Incorporating the latest doctrine.
- Understanding the new environment.
- Seeking answers to unforeseen connectivity issues.
- Increasing face-to-face operations using liaison officers.
- Increasing live environment training events across all disciplines.

This became the forcing function for the E–MIB's successful transition from counterinsurgency to large-scale combat operations.

COL Todd A. Berry is the 201st Expeditionary-Military Intelligence Brigade Commander at Joint Base Lewis-McChord, WA. He previously served as battalion commander of the 303rd Military Intelligence Battalion, 504th Battlefield Surveillance Brigade, at Fort Hood, TX. He is a graduate of the Command and General Staff College and the Army War College and holds a bachelor of arts degree in psychology, a master of science degree in administration (leadership), and a master of science degree in strategic studies. He deployed to Afghanistan as a brigade combat team S-2 and battalion commander.

MAJ Lance C. Turner is the operations officer of the 201st Expeditionary-Military Intelligence Brigade at Joint Base Lewis-McChord, WA. He previously served as the operations officer for the 502nd Expeditionary-Military Intelligence Battalion, 201st Expeditionary-Military Intelligence Brigade, from 2017 to 2018. He holds a bachelor's degree in psychology and is a graduate of the Command and General Staff College. He has deployed to Iraq and Afghanistan and was assigned to Korea for 12 months.

Fort Huachuca Museum
Check out the Fort Huachuca Museum website at:
https://www.ikn.army.mil
Click on the Fort Huachuca Museums link

State of the Intelligence Warfighting Function: Reflections from a Division G-2's Perspective

by Lieutenant Colonel Samuel P. Smith, Jr.

The intelligence warfighting function has gotten so complex and so technical that sometimes you all seem like monks to us—the only people that understand the chanting of monks are other monks. Show us how it works, how it fits. Relate it in terms we understand. You are our experts, and we'll look to you.

—MG Tony Cucolo, Former 3rd Infantry Division Commander

Wars are won by the courage of our soldiers, the quality of our leaders, and the excellence of our training.

—GEN Donn Starry, Former Commandant of the Armor Corps, Commanding General of V Corps, and TRADOC Commander

Introduction

The intelligence warfighting function is complicated—especially the science of our equipment, structure, processes, and authorities. It comprises a diverse set of people and capabilities. For it to be effective, we need a strong foundation of leadership, structure, and equipment to enable our commanders to make timely decisions. Success within the intelligence warfighting function is more an art than a science and requires intelligence officers to have presence, personality, passion, care, and competence to lead our warfighting function.

The intelligence warfighting function is a multi-domain warfighting function. Leaders have stated, from their valid points of view, that the current structure, authorities, manning, training, sustainment, and equipping of intelligence elements at the division and below levels are not fully adequate to provide detailed information in support of commander's decision making.

The 7th Infantry Division is responsible for the training, readiness, and validation of five to seven brigade combat teams (BCTs)/brigades. This article provides my insights as a former 7th Infantry Division G-2 and now the senior intelligence observer-coach-trainer at the Joint Readiness Training Center. Specifically, the article describes my experiences with some issues and challenges the division's intelligence warfighting function faced. It presents techniques and lessons learned to familiarize future BCT and division senior intelligence officers with these problems that might otherwise become evident only after trial and error. It also outlines the challenges and offers solutions.

Task Force Bayonet

The 7th Infantry Division and the intelligence warfighting function executed the commander's readiness guidance through a readiness framework consisting of five complementary lines of effort—man, equip, train, lead, and spirit of the bayonet.

The experience highlighted the following key insights, shown in priority order:

- ✦ A BCT collection management deficiency exists.
- ✦ Readiness guidance for the intelligence warfighting function is a necessity.
- ✦ We need to invest in the talent management process.
- ✦ The Military Intelligence Training Strategy (MITS) framework can be leveraged to develop a system that tracks the maintenance, manning, and team certification status of each intelligence capability.

The Root Cause of the Problem

In his 2017 *The Tactical Leader* article, CPT Brad Wellsandt provided his perspective and analysis of the intelligence warfighting function, stating that the root cause of the intelligence warfighting function's ineffectiveness and marginalization is the friction that exists between the maneuver and intelligence warfighting functions. He further expressed that there is "a definitive lack of understanding and clarity on the roles of key personnel impacting the intelligence fight."[1]

I would contend that progress is being made between the maneuver and intelligence warfighting functions to address the friction and problems CPT Wellsandt identified, though some friction remains among warfighting functions over structure, training, and culture. Several of the challenges persist; however, the state of the intelligence warfighting function has advanced, and it will continue to do so.

Brigade Combat Team Collection Management Deficiency

Formalizing BCT intelligence collection management is required to capitalize on the BCT's lethality. The division

G-2 and BCT S-2 do not have what they need, and the intelligence warfighting function is not properly manned. Synchronized collection at the BCT is challenged by the absence of a trained collection management section and a permanently assigned and trained collection manager. This gap affects BCTs across our Army and has persisted for several years. A challenge most of us confront in the intelligence warfighting function is the art and science of how to find the enemy first through the development of target acquisitions, and then how to synchronize the ability to fix the threat with lethal and nonlethal means to destroy (finish) the enemy. Predictive analysis is critical to enhance the lethality of our commander's capabilities, and lethality is maximized through analysis, planning, targeting, and intelligence operations.

The intelligence staff owes the commander an understanding of the enemy and the environment. We achieve this understanding through the synchronization of information collection and execution of intelligence operations, specifically our support to targeting.

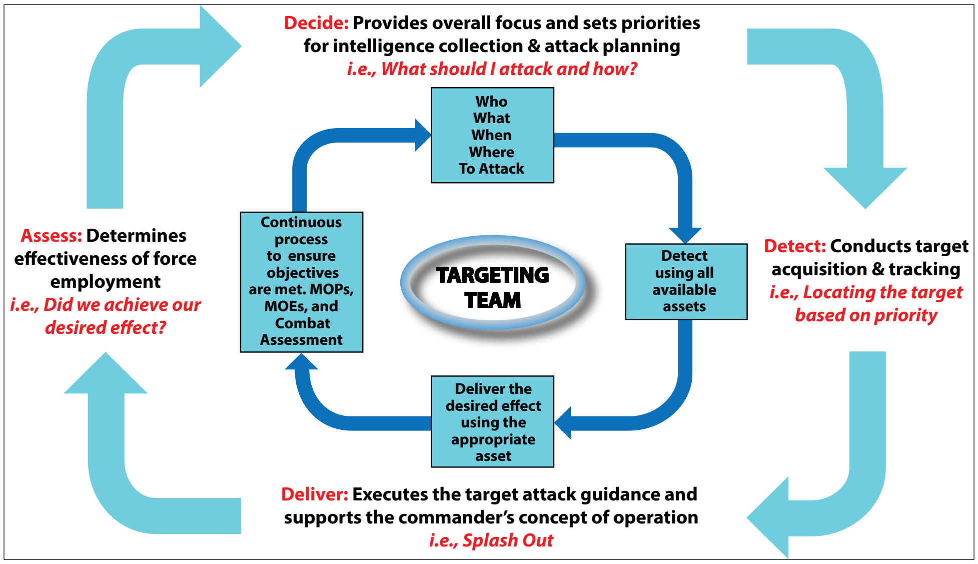

Decide: Provides overall focus and sets priorities for intelligence collection & attack planning
i.e., What should I attack and how?
Who
What
When
Where
To Attack
Detect using all available assets
Detect: Conducts target acquisition & tracking
i.e., Locating the target based on priority
Deliver the desired effect using the appropriate asset
Deliver: Executes the target attack guidance and supports the commander's concept of operation
i.e., Splash Out
Continuous process to ensure objectives are met. MOPs, MOEs, and Combat Assessment
Assess: Determines effectiveness of force employment
i.e., Did we achieve our desired effect?
TARGETING TEAM

Figure 1. Decide, Detect, Deliver, Assess

The collection, processing, and dissemination of intelligence are some of the most critical tasks at the division and BCT. Recent experiences at combat training centers (CTCs) indicate the BCT S-2 section is neither manned nor equipped to process and disseminate intelligence from echelons above brigade or their own organic sensors. The BCT's targeting cycle and process require a fully authorized, manned, trained, and equipped collection management cell. In an antiaccess and area denial environment with a peer adversary, BCT effects and fires rely on echelons above brigade sensors to shape the deep fight (beyond the fire support coordination line). Our warfighting function has demonstrated proficiency in the Decide portion of the Army's primary targeting methodology; however, it lacks the training and experience to fully perform the Detect and Assess portions. This gets at the role of the cavalry squadron and the squadron S-2's ability to influence the commander's decision making (squadron and BCT commanders). The BCT S-2 and squadron S-2 need to help define for the squadron commander the effects he/she wants the squadron to have, which is just as important as where to look.

To achieve success during home-station training certification exercises and CTC rotations, the BCT must develop and disseminate the intelligence running estimate and collection synchronization matrix. The BCT must also perform regular intelligence synchronization engagements.

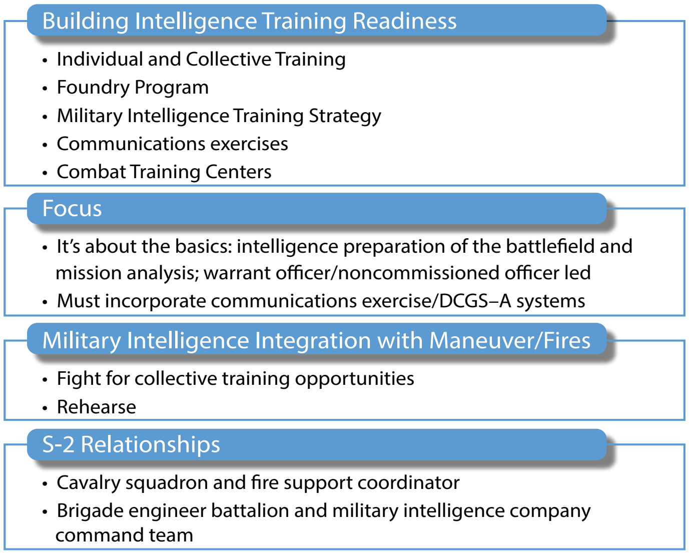
Executing the BCT fight through the teaming of intelligence collection and fires requires leveraging the targeting process to align sensors (organic and echelon above brigade) with joint fires platforms to detect, locate, and engage each BCT high-payoff target. The trends and observations, coupled with the evolution of multi-domain operations, have reinforced the need for the BCT S-2 to have a resourced and trained collection manager and a collection management cell that includes a field artillery targeting warrant officer (military occupational specialty 131A) to facilitate targeting within the brigade intelligence support element. Concepts drive change, and we should operationalize the BCT S-2 with a collection management cell. If there is no growth, one immediate solution in achieving this milestone is repurposing an O-3/captain billet currently on the table of organization and equipment in the BCT S-2 to create a BCT collection manager that is a key developmental position.

Intelligence Warfighting Function Readiness Guidance is a Necessity

The senior intelligence officer's main role is the resourcing and coordination of the manning, equipping, training, and leading lines of effort for subordinate brigades.[2] The intelligence warfighting function is an element of combat power, and we recognize that the integration of the intelligence warfighting function with other warfighting functions results in effective commander decision making. However, if the senior intelligence officer is not directly involved in the decisions being made, there is no way to ensure this integration happens; being invited, included, and having a seat at the table is crucial. In terms of force structure and capabilities, the key challenge is training oversight. The 7th Infantry Division conducted an initial readiness assessment of the intelligence warfighting function in October 2016. The assessment covered significant aspects of manning, equipping, and training for the subordinate brigades. The assessment allowed us to identify areas of strength and areas of weakness. We briefed the assessment to the G-3, chief of staff, and division commander as we started to develop tracking systems and processes for our intelligence readiness, obtaining the buy-in and support from division leadership to concentrate division resources to improve.

We cannot simultaneously focus on all the manning, training, equipping, certification, and intelligence requirements.[3] How do we prioritize and get our commanders to approve where we are assuming risk? Manning, training, and leading are three core principles that require continued emphasis and investment. At a minimum, we must advocate for our senior leaders to approve, publish, and support readiness guidance for the division, BCT, and military intelligence (MI) company's intelligence missions. To be effective, the readiness assessment for the BCT's intelligence functions and tasks must be briefed at quarterly training readiness briefs to the division commander using the MITS framework. The support and emphasis from the commanding general and chain of command on integrating intelligence, fires, and maneuver warfighting functions during the planning and execution of exercises and operations are critical in enhancing the readiness of the intelligence warfighting function teams and platforms.

Given the current alignment of the MI company, brigade engineer battalion commanders are in the position to provide this assessment; however, the level of knowledge required to create the necessary intelligence training and certification resides at the G-2/S-2.



Building Intelligence Training Readiness

- Individual and Collective Training
- Foundry Program
- Military Intelligence Training Strategy
- Communications exercises
- Combat Training Centers

Focus

- It's about the basics: intelligence preparation of the battlefield and mission analysis; warrant officer/noncommissioned officer led
- Must incorporate communications exercise/DCGS–A systems

Military Intelligence Integration with Maneuver/Fires

- Fight for collective training opportunities
- Rehearse

S-2 Relationships

- Cavalry squadron and fire support coordinator
- Brigade engineer battalion and military intelligence company command team

Figure 2. Path to Intel Readiness

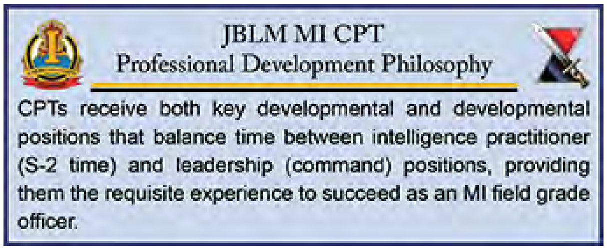
Several programs assisted commanders and G-2s/S-2s in building their intelligence readiness. We established key programs and processes to improve the readiness of the intelligence warfighting function. These included—

- ✦ Conducting consistent G-2/S-2 readiness synchronization meetings.
- ✦ Integrating readiness assessment briefs of the intelligence warfighting function into BCT semiannual training briefs.
- ✦ Directing completion of the BCT S-2 course at home station.
- ✦ Requiring BCTs and battalions to obtain a certain number of Digital Intelligence System Master Gunner, Journeyman, and Leader course graduates.
- ✦ Conducting MITS team certification.
- ✦ Developing organizational inspection program checklists for intelligence warfighting function training and intelligence and electronic warfare maintenance.
- ✦ Leveraging Foundry Program resources to enrich intelligence training.
- ✦ Integrating BCT/MI company intelligence teams in expeditionary-MI brigade table VI exercises.
- ✦ Establishing predeployment intelligence and electronic warfare maintenance services.

These programs supported echelons below division in maintaining equipment authorized by tables of organization and equipment, establishing an intelligence architecture, and communicating the complex threat environment. Additionally, the Foundry platform provided expert support for intelligence discipline training and helped units conduct collective training in intelligence tasks. Finally, the installation's Language and Culture Center prepared units with language training for Army linguists and mission-specific culture, regional, expertise, and language training.

Talent Management

At the core of our profession is the quality of our people and our leadership. The Army requires both specialists and generalists, and it is imperative that we match individuals' skills, competencies, and timelines to achieve the necessary development and growth in our intelligence corps. Given the current alignment and structure, optimizing our capabilities to provide the commander assessments from a range of sources is an art we are required to navigate and master. Results matter, but demonstrating the leadership to trust, collaborate, and take risks through team building and empowering subordinates to improvise, leverage, and adapt strengthens the intelligence warfighting function. This requires G-2s/S-2s to use their presence, personality, passion, care, and competence to address the readiness and core competency challenges.

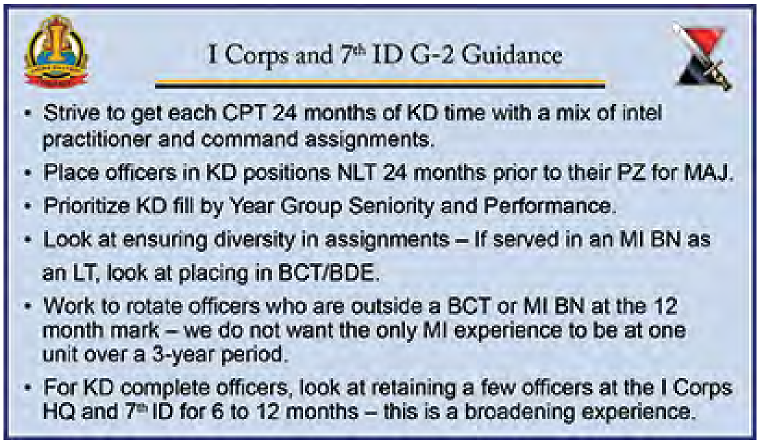


JBLM MI CPT
Professional Development Philosophy

CPTs receive both key developmental and developmental positions that balance time between intelligence practitioner (S-2 time) and leadership (command) positions, providing them the requisite experience to succeed as an MI field grade officer.

Talent management is the mechanism and process that G-2s/S-2s develop on behalf of their commanders, ensuring S-2s and MI company commanders have the right skills, experience, and personality to connect with their commanders. Approximately 30 percent of my time as a division G-2 was dedicated to the talent management process because the chief of staff and division commander delegated the responsibility to lead and manage on their behalf.

Formal talent management engagements were conducted with BCT/brigade S-2s at least every other month for warrant officers, lieutenants, and captains. At least quarterly, talent management boards were conducted for chief warrant officer 3s and majors. This required creating opportunities and engagements with intelligence professionals in the division by hosting professional development seminars; conducting one-on-one office calls with individuals to discuss goals and assess performance; and attending BCT, brigade, battalion, and company training events to meet Soldiers throughout the intelligence staffs. Additionally, monthly conference calls with Human Resource Command assignment officers were conducted to balance each individual's strengths, goals, and career with Army requirements. We discovered that intelligence officers and noncommissioned officers should establish relationships with their brigade S-2, brigade S-2 noncommissioned officer in charge, division G-2, and division sergeant major so that they can discuss career and family goals. We know that Officer and Enlisted Record Briefs are considered a military resume and find that stakeholders review them more than most intelligence professionals realize; therefore, updating these records is important. Developing, identifying, evaluating, and retaining the right talent based on an individual's performance and potential was demanding, challenging, and rewarding, but it needs to be done to best place the intelligence professional for both the individual and the organization. During meetings and discussions with BCT/brigade and battalion commanders, we confirmed that we were aligning the right officer with the right commander, which allowed the S-2 at echelon the best opportunity and potential to succeed. The division G-2 sergeant major conducted a similar talent management process for enlisted intelligence Soldiers.



I Corps and 7th ID G-2 Guidance

- Strive to get each CPT 24 months of KD time with a mix of intel practitioner and command assignments.
- Place officers in KD positions NLT 24 months prior to their PZ for MAJ.
- Prioritize KD fill by Year Group Seniority and Performance.
- Look at ensuring diversity in assignments – If served in an MI BN as an LT, look at placing in BCT/BDE.
- Work to rotate officers who are outside a BCT or MI BN at the 12 month mark – we do not want the only MI experience to be at one unit over a 3-year period.
- For KD complete officers, look at retaining a few officers at the I Corps HQ and 7th ID for 6 to 12 months – this is a broadening experience.

To succeed, you do not need to be the smartest person in the room; however, you must build a team that complements your weaknesses and maximizes your strengths. This is about buy-in from stakeholders inside and, more importantly, outside the intelligence warfighting function.

Knowing Intelligence Capability Readiness

It cannot collect if it doesn't work. Developing a system at echelon that tracks, at a minimum, the maintenance, manning, and team certification status of each intelligence capability is a must. The G-2 owns the maintenance, training, and sustainment oversight of the unit intelligence warfighting function. A unit cannot effectively train without the right people and leaders who are correctly task-organized and resourced with working equipment.

The U.S. Army Intelligence Center of Excellence Lessons Learned team enabled the I Corps G-2 and 7th Infantry Division G-2 teams to observe BCTs from home-station training exercises through CTC rotations. They provided data and information to the senior intelligence officers, which identified progress and priority areas to integrate into future home-station training exercises. This capability was vital in helping the senior intelligence officers to see their training and maintenance program from an outside perspective and greatly enriched the BCT's intelligence training program.

The senior intelligence officer structure and process within the division and BCT are intricate—the chain of command and force structure often complicate the role and responsibility of the senior intelligence officer. A great senior intelligence officer can certainly overcome this, but not every senior intelligence officer is the best communicator and relationship builder.

MITS provides a solid foundation from which to train the BCT intelligence functions and tasks. This requires the S-2 to insert themselves into the information and reporting chain of the MI company commander and brigade engineer battalion commander/executive officer.

In 2006, as part of the Armywide reorganization of combat forces to the modular structure, direct support MI battalions at the division level were separated, and most of their personnel and equipment were reassigned to the brigade support battalions and brigade special troop battalions. The intelligence capability and structure further transitioned in 2013 with the brigade organization initiative. It triggered the reflagging of brigade special troop battalions to the brigade engineer battalions, where the MI company is currently aligned.[4]

Since the 2006 reorganization, the G-2 and BCT S-2 assumed most of the responsibility and oversight for developing and implementing the unit's intelligence warfighting function training strategy and certification requirements. At each echelon, from MI company to Corps, the intelligence warfighting function will certainly not be manned and equipped to train and operate alone. To enhance intelligence readiness, integration of the expeditionary-MI brigade battalion's downward reinforcing mission is a capability that senior intelligence officers need to maximize, in concert with support from the G-6s/S-6s, military intelligence systems maintainers/integrators, and field support representatives, and by conducting maintenance rodeos.

Each echelon needs to rely upon the higher, lower, and adjacent expertise and talents. Working together, we create the synergy needed to provide commander's timely and relevant intelligence. Training and readiness of the intelligence warfighting function are critical to building overall unit readiness and sustaining operational capability.

Looking Forward

MITS and Foundry 3.0 provide a greater focus to increase the proficiency at the team and platform level. Given the Army's modernization strategy, which is designed to ensure Soldiers and units are prepared to confront peer threats, as intelligence professionals we should ask some critical questions going forward:

- ✦ How is the intelligence warfighting function increasing lethality for our commanders?
- ✦ In terms of force structure and capabilities, is the intelligence warfighting function aligned properly to confront tomorrow's threat, while addressing the readiness challenges we face?
- ✦ Has the Army assumed risk in intelligence capability, training, equipment, and manning at the division and below?
- ✦ How are the Army and intelligence warfighting function investing in the BCT collection manager?
- ✦ How can the senior intelligence officer and commander leverage the capabilities of electronic warfare, signals intelligence, and cyberspace, given the current training, structure, and authority challenges?

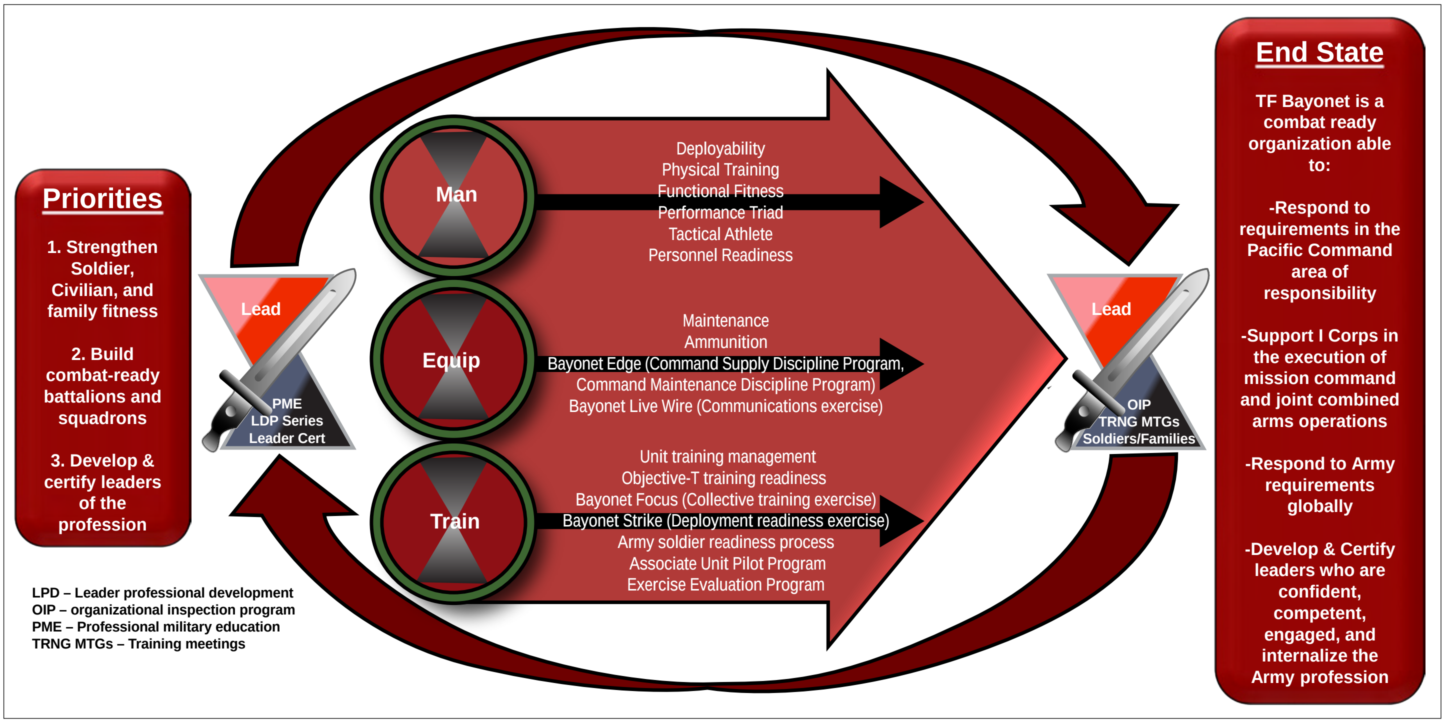

Priorities
1. Strengthen Soldier, Civilian, and family fitness
2. Build combat-ready battalions and squadrons
3. Develop & certify leaders of the profession
Lead
PME
LDP Series
Leader Cert
Man
Deployability
Physical Training
Functional Fitness
Performance Triad
Tactical Athlete
Personnel Readiness
Equip
Maintenance
Ammunition
Bayonet Edge (Command Supply Discipline Program,
Command Maintenance Discipline Program)
Bayonet Live Wire (Communications exercise)
Train
Unit training management
Objective-T training readiness
Bayonet Focus (Collective training exercise)
Bayonet Strike (Deployment readiness exercise)
Army soldier readiness process
Associate Unit Pilot Program
Exercise Evaluation Program
Lead
OIP
TRNG MTGs
Soldiers/Families
End State
TF Bayonet is a combat ready organization able to:
-Respond to requirements in the Pacific Command area of responsibility
-Support I Corps in the execution of mission command and joint combined arms operations
-Respond to Army requirements globally
-Develop & Certify leaders who are confident, competent, engaged, and internalize the Army profession
LPD – Leader professional development
OIP – organizational inspection program
PME – Professional military education
TRNG MTGs – Training meetings

Figure 3. Task Force Bayonet Man, Equip, Train, and Lead

- Have we marginalized tactical signals intelligence with the advancement and placement of electronic warfare capabilities and authorities?
- What are we learning from the 75th Ranger Regiment and U.S. Army Special Operations Command with the investment and activation of their MI battalion?

Conclusion

Communicating our intelligence warfighting function capabilities and readiness to our commanders, so that they can conceptualize and determine how best to leverage our capabilities in terms of combat power, reduces uncertainty for our decision makers.[5] Enhancing the division's and BCT's intelligence capabilities and table of organization and equipment is required, as well as acknowledging force structure constraints, limitations, and the weary debate for MI growth. Leveraging and investing in the national to tactical intelligence effort are paramount to creating training opportunities for achieving readiness and certification.

Significant consideration persists regarding the necessity for an intelligence unit that provides all-source analysis, geospatial intelligence, human intelligence, electronic warfare, signals intelligence, and unmanned aircraft system functions, along with cyberspace support at the division level and below. Currently, the BCT MI company appears to be the investment endeavor that addresses this debate.

Perhaps by having outlined the importance of—

- improving the BCT collection management challenge,
- creating readiness guidance for the intelligence warfighting function,
- investing in the talent management process, and
- developing a system to track manning, equipping, maintenance, and training certification requirements;

we will broaden others' perspective and promote discussion to enhance our intelligence warfighting function.

Epigraphs

Christopher Fincham, "3rd Infantry Commander recalls important intelligence role," *U.S. Army Worldwide News*, February 12, 2009, https://www.army.mil/article/16852/3rd_infantry_commander_recalls_important_intelligence_role.

Lewis Sorley, *Selected Works of General Donn A Starry Volume II* (Fort Leavenworth, KS: Combat Studies Institute Press, U.S. Army Combined Arms Center, September 2009), 717.

Endnotes

1. Brad Wellsandt, "The State of the Intelligence Warfighting Function in the US Army Brigade Combat Team," *The Tactical Leader*, 6 June 2017, https://www.thetacticalleader.com/blog/the-state-of-the-intelligence-warfighting-function-in-the-us-army-bct.

2. Department of the Army, Army Regulation 10-87, *Army Commands, Army Service Component Commands, and Direct Reporting Units* (Washington, DC: U.S. Government Publishing Office, December 2017).

3. Richard D. Conkle, *Creating Situational Understanding at Echelon Corps and Below* (Carlisle, PA: U.S. Army War College, January 2017).

4. GEN Ray Odierno, "CSA Press Conference on Army Force Structure Reductions (As Prepared)," *U.S. Army Worldwide News*, 25 June 2013, https://www.army.mil/article/106355/june_25_2013_csa_press_conference_on_army_force_structure_reductions_as_prepared.

5. Fincham, "3rd Infantry Commander."

The author has observed several brigade combat team, battalion, and brigade S-2s on training exercises, combat training center rotations, and operational deployments. He is indebted to the 7th Infantry Division G-2 team, chain of command, numerous Soldiers, noncommissioned officers, officers, and Civilians of the Joint Base Lewis-McChord intelligence community and several reviewers for their valuable comments and suggestions on earlier drafts of this article. These include COL Timothy Parker, LTC (R) Brian Scott, MAJ Jacob Hina, MAJ Matthew Sheftic, MAJ Ian Fleischmann, former brigade combat team S-2s, CPT Warren Henderson, Mr. Brian Bassett, Mr. Thomas Meaney, and Mr. Terence Sadler.

LTC Samuel P. Smith, Jr., is a former division G-2 and current senior intelligence observer-coach-trainer at the Joint Readiness Training Center. He has served as an Analysis and Control Element Chief, Deputy G-2, battalion executive officer, and battalion S-3 in U.S. Army Forces Command, U.S. Army Intelligence and Security Command, and Joint Special Operations Command units throughout his career, with multiple deployments to Afghanistan, Iraq, and Bosnia. A former intern at the Office of the Secretary of Defense, Joint Chiefs of Staff, and Army Staff, he has an associate's degree from Kemper Military Junior College, a bachelor of arts degree from the University of Maryland, and a master's degree from Georgetown University.

82nd Airborne Division
Military Intelligence Training Strategy Lessons Learned

by Lieutenant Colonel Michael Adamski and Major William Denn

***Editor's Note:** The Center for Army Lessons Learned website published a previous version of this article in May 2018, https://call2.army.mil/ (common access card login required). It has been updated based on the latest iterations of the 82nd Airborne Division's Military Intelligence Training Strategy training and edited for public release.*

Introduction

Previously referred to as Military Intelligence (MI) Gunnery, MI training within U.S. Army Forces Command (FORSCOM) units is now known as the Military Intelligence Training Strategy (MITS). MITS is a tiered training approach at multiple echelons to build MI forces ready to operate on the battlefield. MITS formalizes individual, team, and collective training events for brigade combat teams (BCTs) to ready their intelligence warfighting function for a decisive action environment. Since early 2018, three BCTs from the 82nd Airborne Division volunteered to validate the program of instruction and provide feedback to the U.S. Army Intelligence Center of Excellence (USAICoE) to improve the program before its FORSCOM implementation.

This article describes the planning, preparation, execution, and revision of the MITS training platform from the perspective of the 82nd Airborne Division G-2, which oversaw the execution of the pilot program at Fort Bragg, North Carolina. The 82nd Airborne Division G-2 acknowledges that Fort Bragg's conditions for intelligence training are ideal and that many formations do not have the same access to resources that Fort Bragg offers. These fundamental best practices are provided below, irrespective of access to resources, to improve intelligence training across the force.

In the first quarter of 2018, the 82nd Airborne Division's 2nd and 3rd BCTs (2/82 BCT and 3/82 BCT) partnered with FORSCOM and USAICoE to conduct pilot exercises to validate new standards and methodologies to train and evaluate U.S. MI Soldiers. These pilots were the result of more than a year of planning to build a team of intelligence experts from Fort Bragg and Fort Huachuca, Arizona, in order to leverage their knowledge and expertise. Although the 82nd Airborne Division played only a small part in developing and testing MITS, this article describes our lessons learned from the pilot program, along with recommendations for future evolutions of this training construct.

The key lessons learned from the pilot program and subsequent training are—

- The MITS framework provides a solid foundation from which to train a BCT intelligence warfighting function.
- While MITS focuses primarily on training the MI company, BCT S-2s must be involved in the planning and execution.
- An intelligence systems communications exercise is critical to the success of the MITS exercise.
- Command involvement at the BCT level is necessary for the support and execution of MITS in the context of a BCT's training strategy.

A Need for New Training Methods for Military Intelligence

Over the past 17 years, the U.S. Army fought in operational environments dominated by insurgency and counterterrorism threats in Iraq and Afghanistan, and intelligence training adapted appropriately. The result of this adaptation was a depleted ability to collect and assess in a large-scale conventional military conflict.

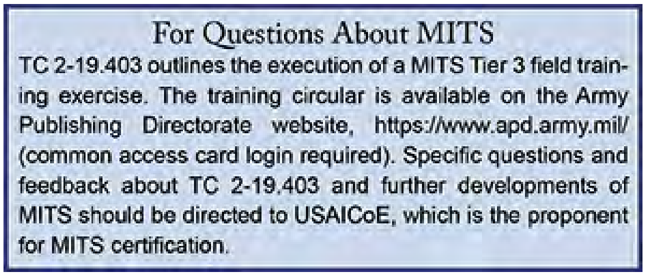
Today the U.S. Army's anticipated threat environment continues to evolve by focusing on a more challenging decisive action training environment that combines both asymmetric and peer conventional force threats. The current hostile and revanchist policies of Russia, China, and North Korea only further necessitate the need for improved training to prepare for confrontation against peer adversaries.

A potential future conflict against North Korea, Russia, or China will be characterized by a need for the U.S. Army to process and analyze intelligence faster than it did for counterinsurgency operations. Intelligence on these types of battlefields must be analyzed and disseminated at the lowest possible level despite degraded communications, and must be conveyed in a manner that allows commanders to make rapid decisions and appreciate risk.

Tomorrow's operational environment requires MI leaders to rethink and relearn how to conduct home-station training. A particular challenge for intelligence Soldiers at the tactical level is that time to train is a precious commodity. Commanders often balance competing demands for their intelligence analysts, such as—

- The need to gain and sharpen technical skills in their area of expertise.
- The need to participate in and support collective training with their maneuver units.
- The need to continue intelligence support to exercises and real-world intelligence analysis even while in garrison.

Adding to these challenges was the complexity of subordinate brigades on different training and deployment timelines, often preparing for varied threat environments.



For Questions About MITS

TC 2-19.403 outlines the execution of a MITS Tier 3 field training exercise. The training circular is available on the Army Publishing Directorate website, https://www.apd.army.mil/ (common access card login required). Specific questions and feedback about TC 2-19.403 and further developments of MITS should be directed to USAICoE, which is the proponent for MITS certification.

The result of these challenges led to an atmosphere in which subordinate brigade intelligence officers, "S-2s," often trained their intelligence formations and MI companies independent of the division headquarters. Brigades focused on deployments while the division focused primarily on their division headquarters mission requirements. This focus created an environment in which the division G-2 section inadequately managed intelligence training.

Cognizant of these demands, challenges, and changes to the scenarios used at the Nation's combat training centers (now referred to as decisive action training environment 3.0), the 82nd Airborne Division G-2 section began efforts in the summer of 2017 to formalize the role of the division G-2 as a facilitator—not a dictator—of appropriate training environments for all brigades within the division.

A Comprehensive Military Intelligence Readiness Strategy

The 82nd Airborne Division G-2 plans team led the development of a comprehensive MI readiness strategy, which served as a guiding document to clarify and operationalize emerging MITS requirements from USAICoE. This guidance was especially important to assist subordinate brigade S-2s in developing their teams and their MI company's training plans. More importantly, the MI readiness strategy helped to clarify the interface points between the division G-2 and the subordinate brigade S-2s, namely the division's role in resourcing and coordinating the *Manning, Equipping,* and *Training* United States Code Title 10 authorities for the subordinate brigades.

A comprehensive approach is essential because all aspects of manning, equipping, and training directly affect MI readiness. A unit cannot have effective training without the right people and leaders who are correctly task-organized and resourced with equipment that works.

Planning the Military Intelligence Training Strategy Pilot

Planning began in the fall of 2017 with the 82nd G-2 plans team integrating into weekly in-progress review and working groups with USAICoE and FORSCOM to design the MITS pilot program. The scope of the pilot focused on designing a training event for MITS Tier 3 (Crew) evaluation. The initial key planning constraints were—

- An MI company would conduct individual Soldier training and an individual certification before a Tier 3 certification, in accordance with TC 2-19.404, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 4*.
- As much as possible, an MI company commander should plan, resource, and execute a MITS Tier 3 event in accordance with TC 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3*.
- An MI company commander would use their installation's mission training complex and Foundry teams to provide the Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) scenario simulation to drive training across MI systems.
- USAICoE would coordinate with the U.S. Army Training and Doctrine Command G-27 in order to develop several standardized scenarios tailored for the combat training center rotations, as well as familiarization specific to the geographic combatant command area of responsibility.
- The division G-2 would provide training oversight of the MITS event.
- The division G-2 would resource/task external evaluators for the MI company to provide objective evaluation and feedback (this was necessary because the BCT S-2 section is not manned appropriately to provide outside evaluation for each intelligence crew in the MI company).

Additionally, the 82nd G-2 team sought partnership with other Fort Bragg intelligence units such as XVIII Airborne Corps, 525th MI Brigade, U.S. Army Special Operations

Command, and other XVIII Airborne Corps separate brigades to integrate their own intelligence crews (especially all-source and signals intelligence) into the MI company Tier 3 field training exercise.

For 2/82 BCT's Tier 3 MI company field training exercise, this planning process lasted approximately 5 months. The majority of this time focused on designing the initial scenario for the Joint Readiness Training Center and building into IEWTPT. For 3/82 BCT's later Tier 3 MI company field training exercise, this planning timeline was shortened to 3 months because much of the work for the scenario was already complete.

Executing the Military Intelligence Training Strategy Tier 3 Field Training Exercise

The following is a summary of our lessons from executing a MITS Tier 3 field training exercise. According to TC 2-19.403, a Tier 3 field training exercise evaluates nine separate crews within the MI company:[1]

- All-Source: Fusion Crew.
- All-Source: Collection Management Crew.
- All-Source: Targeting Crew.
- Geospatial Intelligence Crew.
- Signals Intelligence: Prophet Crew.
- Signals Intelligence: Cryptological Support Team Crew.
- Human Intelligence: Human Intelligence Collection Team Crew.
- Human Intelligence: Operational Management Team Crew.
- Intelligence and Electronic Warfare Maintainer Crew.

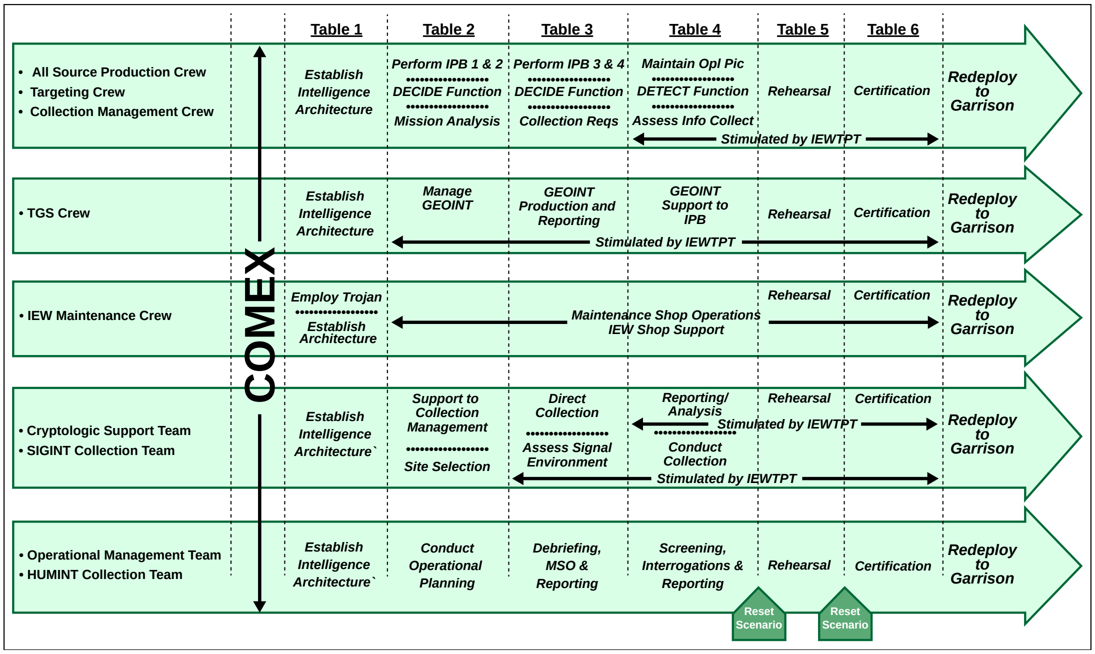


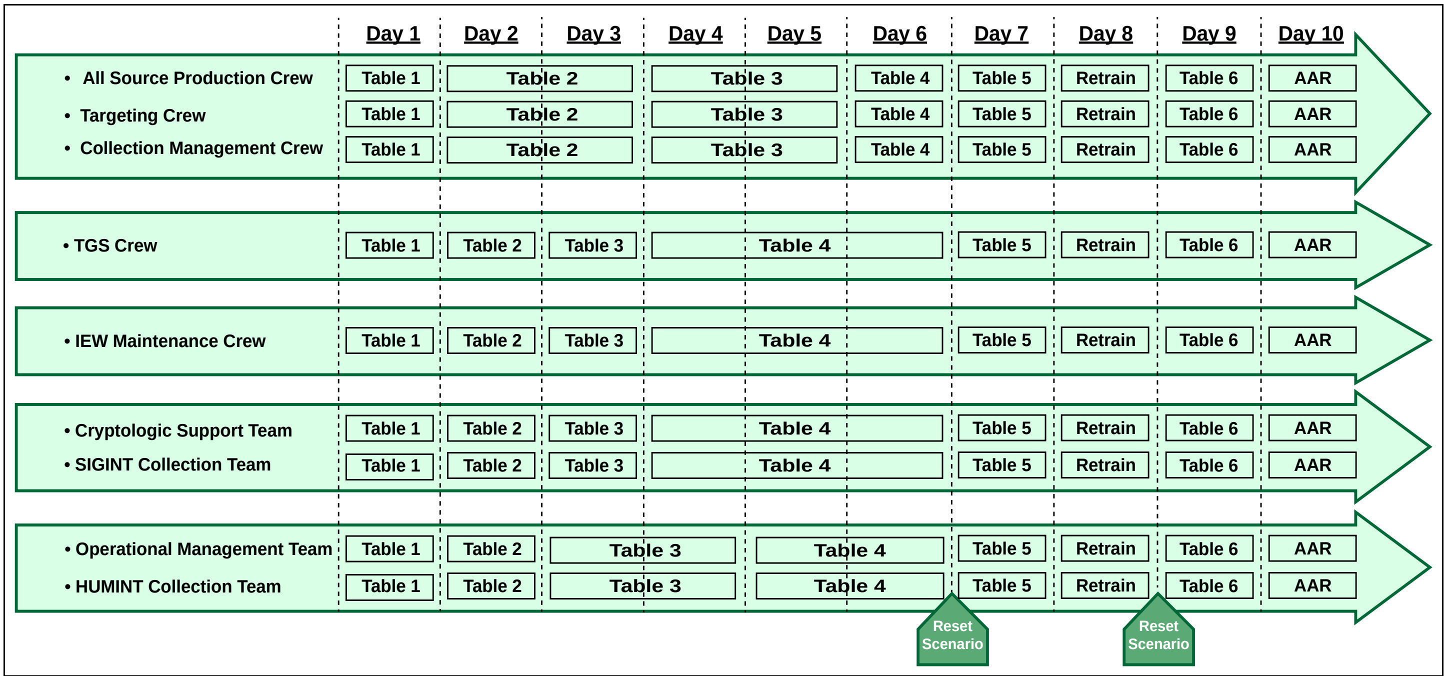
Figure 1. Sequence of Certification Events[2]

These crews conduct their evaluation across six tables specified by TC 2-19.403 over 10 days within a discipline-specific scenario for each crew (see Figure 1 below and Figure 2 on the next page). The evaluation has each crew as being discipline-specific (i.e., no collaboration) to allow the MI company commander and BCT S-2 to separately evaluate the performance of each crew. For example, if a geospatial intelligence crew fails to properly conduct terrain analysis through a modified combined obstacle overlay, then it will not affect the performance of the all-source fusion crew training on intelligence preparation of the battlefield analysis during their own evaluation tables. Similarly, if the collection management crew inadequately designs an information collection plan, it will not negatively affect the performance of the signals intelligence or human intelligence collection crews in the scenario.

While the discipline-specific nature of the Tier 3 field training exercise was one of the most debated issues in the pilot working groups, USAICoE determined that in order to support FORSCOM's Objective-T readiness metrics, a Tier 3 event would move forward in this manner and subsequent Tier 2 and Tier 1 training would allow collaboration among the intelligence crews.

Due to training schedule constraints, 2/82 BCT's February 2018 event could only accommodate a 1-week communications exercise and a 5-day training exercise. Similarly, 3/82 BCT's training schedule had the same constraints; therefore, the 10-day model was adapted to conduct the six tables within 5 days.

For the training location, 2/82 BCT's field training exercise was meant to replicate an MI company that did not have access to field training areas or S-4/S-6 support from the parent battalion. As such, the majority of the exercise took place at the Fort Bragg mission training complex and Foundry sites. Separate classrooms were established for each crew with their own Intelligence Fusion Server stack fed by the IEWTPT scenario. Prophet training occurred in a live environment on Fort Bragg training areas, and the human intelligence



	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7	Day 8	Day 9	Day 10
• All Source Production Crew	Table 1	Table 2		Table 3		Table 4	Table 5	Retrain	Table 6	AAR
• Targeting Crew	Table 1	Table 2		Table 3		Table 4	Table 5	Retrain	Table 6	AAR
• Collection Management Crew	Table 1	Table 2		Table 3		Table 4	Table 5	Retrain	Table 6	AAR
• TGS Crew	Table 1	Table 2	Table 3	Table 4			Table 5	Retrain	Table 6	AAR
• IEW Maintenance Crew	Table 1	Table 2	Table 3	Table 4			Table 5	Retrain	Table 6	AAR
• Cryptologic Support Team	Table 1	Table 2	Table 3	Table 4			Table 5	Retrain	Table 6	AAR
• SIGINT Collection Team	Table 1	Table 2	Table 3	Table 4			Table 5	Retrain	Table 6	AAR
• Operational Management Team	Table 1	Table 2	Table 3		Table 4		Table 5	Retrain	Table 6	AAR
• HUMINT Collection Team	Table 1	Table 2	Table 3		Table 4		Table 5	Retrain	Table 6	AAR

Figure 2. MITS Tables by Certification Day[3]

teams used training interrogation booths at Fort Bragg's Foundry site.

For 3/82 BCT's field training exercise, the MI company sought to test whether the field training exercise event could be executed completely within a field environment. The concept of operations also called for a 5-day exercise (not including a communications exercise) rather than the 10-day model (see Figure 3 on the next page). In this case, the MI company established its brigade intelligence support element tent in a training area and pushed the IEWTPT scenario from the mission training complex to the MI company's TROJAN system. Unfortunately, because of architecture configuration issues, the analysts did not receive much of the IEWTPT scenario for several days while the 35T intelligence and electronic warfare paratroopers reconfigured their systems. These problems further highlighted the importance of a communications exercise, preferably one in the field where the training will occur.

In both cases, the 82nd G-2 provided or coordinated for external evaluators, based on the requirements outlined in TC 2-19.403, from each brigade (resourced from sister brigades, Corps G-2, 525th MI Brigade, and the division G-2 section) to provide objective feedback. The 82nd G-2 also hosted a 2-day evaluator academy to certify all the evaluators to the evaluation standards in accordance with TC 2-19.403, as well as familiarization with the scenario.

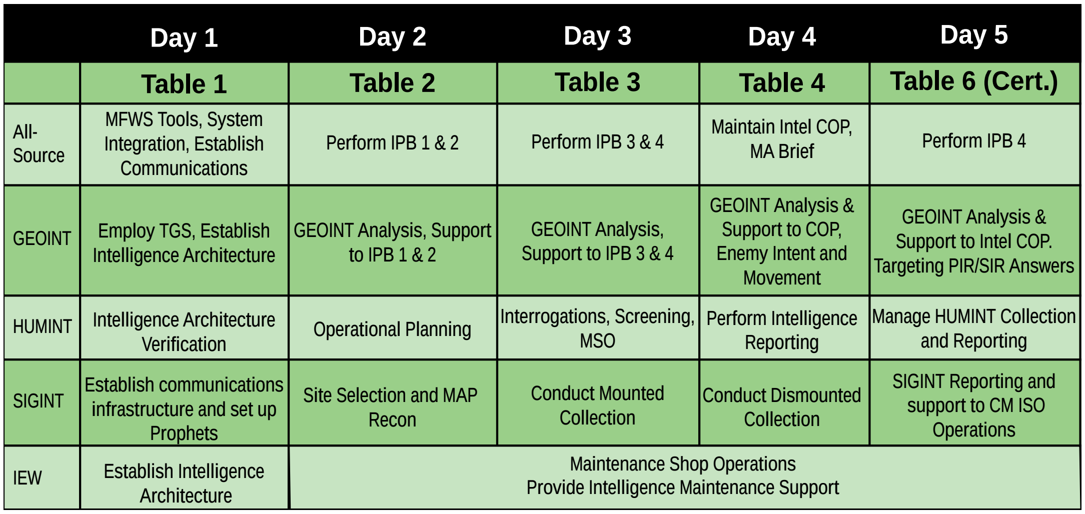
Key Pilot Lessons Learned

Six lessons learned from the pilot exercise are described below.

1. TC 2-19.403 provides an excellent framework to standardize the evaluation of intelligence crews. Overall, we assess that TC 2-19.403 provides the needed standardized and objective framework to assess MI crew readiness across all the intelligence crews within an MI company. While exercise design should continue to be shaped to include the BCT S-2 and consider allowing crew interaction, overall the tables provided within TC 2-19.403 adequately capture the skills necessary for follow-on collective training events.

While both 2/82 and 3/82 BCTs faced several friction points in the execution of the evaluation tables, this was mostly attributed to gaps in the scenario simulation, base order, or architecture configuration problems that were unresolved during the communications exercise conducted the week before the field training exercise. After action report feedback from the field training exercise sent to USAICoE and the U.S. Army Training and Doctrine Command G-27 is adapted to improve and refine any scenario simulation gaps and issues with base order products.

2. Despite a MITS Tier 3 field training exercise being an MI company-led and resourced event, the BCT S-2 should be involved from planning through execution. A MITS Tier 3 field training exercise is a ready-made opportunity for a BCT S-2 to conceptualize training in context of the BCT commander's vision and intent for the intelligence warfighting function within specific mission requirements. It provides the BCT S-2 a platform to task-organize the shop and MI company appropriately. To conduct training of an MI company on its own is a missed opportunity to further the brigade S-2's collective training



	Day 1	Day 2	Day 3	Day 4	Day 5
	Table 1	Table 2	Table 3	Table 4	Table 6 (Cert.)
All-Source	MFWS Tools, System Integration, Establish Communications	Perform IPB 1 & 2	Perform IPB 3 & 4	Maintain Intel COP, MA Brief	Perform IPB 4
GEOINT	Employ TGS, Establish Intelligence Architecture	GEOINT Analysis, Support to IPB 1 & 2	GEOINT Analysis, Support to IPB 3 & 4	GEOINT Analysis & Support to COP, Enemy Intent and Movement	GEOINT Analysis & Support to Intel COP. Targeting PIR/SIR Answers
HUMINT	Intelligence Architecture Verification	Operational Planning	Interrogations, Screening, MSO	Perform Intelligence Reporting	Manage HUMINT Collection and Reporting
SIGINT	Establish communications infrastructure and set up Prophets	Site Selection and MAP Recon	Conduct Mounted Collection	Conduct Dismounted Collection	SIGINT Reporting and support to CM ISO Operations
IEW	Establish Intelligence Architecture	Maintenance Shop Operations Provide Intelligence Maintenance Support			

Figure 3. 3/82 BCT MITS Schedule

objectives. These objectives can be achieved still within the evaluation framework of TC 2-19.403.

3. A successful communications exercise is essential for mission success in the field training exercise. The IEWTPT simulation and scenario helps drive training during the field training exercise. Receiving the scenario and data—whether over the MI company's TROJAN system, or the S-6's tactical communications node backbone, or fiber at a mission training complex—can make or break the training event. The MI company's 353T needs to clearly map out the intelligence architecture plan, nested with how the BCT S-2 will fight, and ensure all parties understand how data is flowing. Reimaging workstations and Intelligence Fusion Servers can often take weeks of preparation even before a communications exercise.

In the future, intelligence data transport will only occur over the S-6's tactical communications node backbone using the modular communications node–advanced enclave TROJAN replacement. When this occurs, it will be especially important for the BCT S-2 to help facilitate the coordination and tasking of the BCT's signal company to participate in future MI company MITS field training exercises.

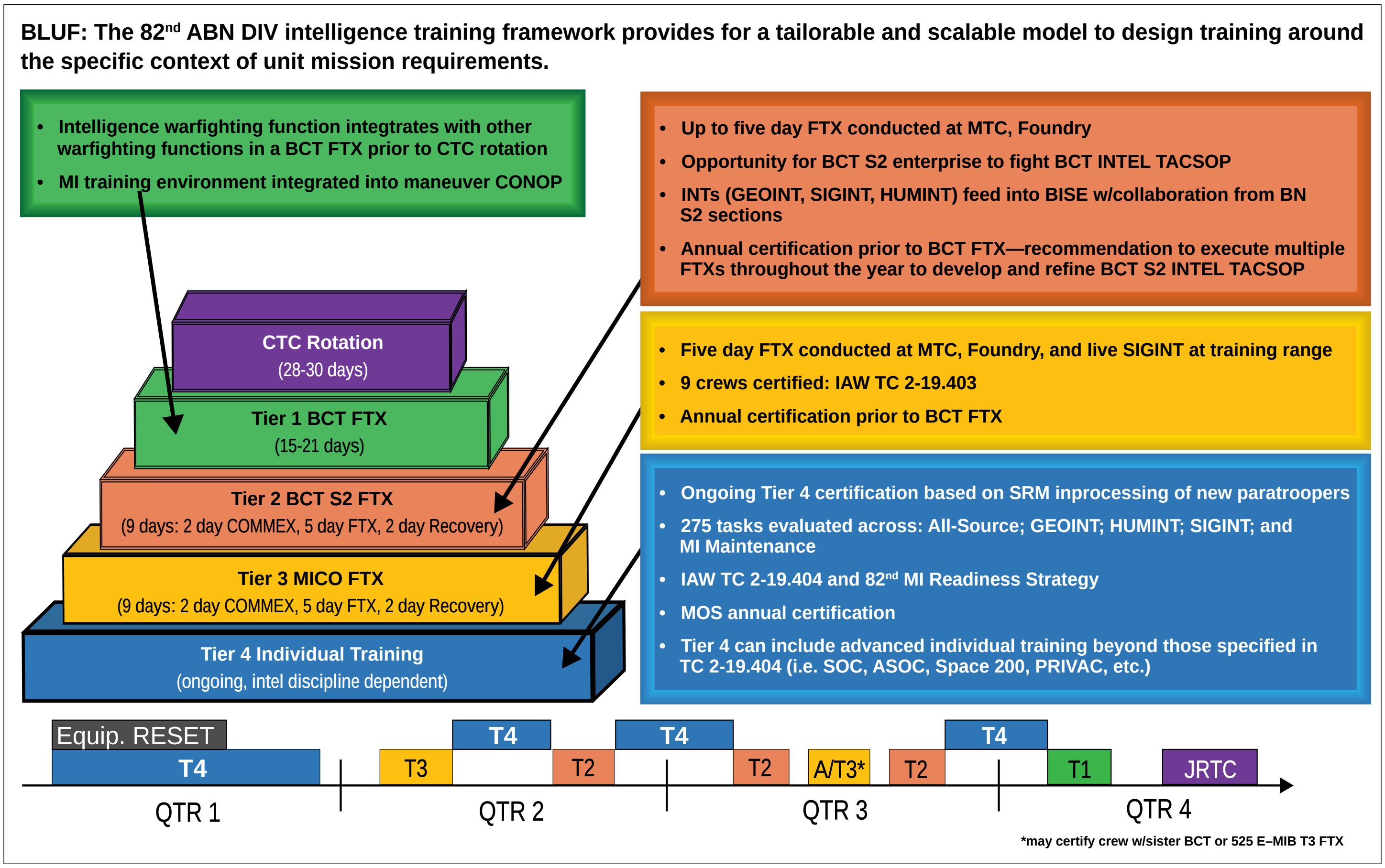
4. Balance the demand for cross-discipline interface with prescribed military occupational specialty-specific training in Tier 3 events. During Tier 3 training events, BCT and MI company leadership will encounter a bottom-up demand for cross-discipline interface. This positive tendency serves to highlight the critical necessity for collaboration during intelligence planning and operations. However, it remains imperative that leaders seek to balance this demand with the prescribed military occupational specialty-specific training that is a critical building block in Tier 3. The more leaders are directly involved, the more they will be able to leverage this positive dynamic to enhance training.

5. Brigade training calendars do not have enough white space for separate Tier 3 and Tier 2 events before a BCT field training exercise prior to a combat training center rotation. All three of the 82nd Airborne's infantry brigades had to be ready for a Joint Readiness Training Center rotation within 6 months of redeployment. Between individual training, collective events like battalion and brigade command post exercises, situational training exercise lanes, and other normal duties, activities, and taskers a brigade encounters, it is difficult to justify separate, independent Tier 3 and Tier 2 events for the intelligence warfighting function before a BCT field training exercise and combat training center rotation.

USAICoE is still developing the concept for what a Tier 2 event encompasses within TC 2-19.402. In our opinion, it should look like an event in which the BCT S-2 can fight and refine the BCT intelligence tactical standing operating procedure. This recommendation is in contrast with the current model of a "platform" training event (i.e., signals intelligence—a combination of a cryptological support team and a Prophet team).

We also recommend that the MI company field training exercise be an opportunity in which a Tier 2 concept of fighting the brigade intelligence support element and BCT S-2 tactical standing operating procedure can be added to the end of the event with little overhead costs. If the MI company is already formed as a brigade intelligence support element in the field, then a scenario can continue for several more days with the BCT S-2 leading the remainder of the field training exercise. This would reduce the amount of time required to redeploy the MI company into the field for a separate training event and would serve as a great preparation for the intelligence warfighting function before a BCT field training exercise. Figure 4 (on the next page) depicts a sample brigade training strategy under the 82nd Airborne's MI training doctrinal template.

6. Sanction MITS as reportable via brigade engineer battalion/BCT in the unit status reporting. Currently, no mechanism exists to measure readiness for a BCT intelligence warfighting function or division G-2 staff. Two key thoughts are worth considering to rectify this gap. First, the capstone



BLUF: The 82nd ABN DIV intelligence training framework provides for a tailorable and scalable model to design training around the specific context of unit mission requirements.

- **Intelligence warfighting function integtrates with other warfighting functions in a BCT FTX prior to CTC rotation**
- **MI training environment integrated into maneuver CONOP**

- **Up to five day FTX conducted at MTC, Foundry**
- **Opportunity for BCT S2 enterprise to fight BCT INTEL TACSOP**
- **INTs (GEOINT, SIGINT, HUMINT) feed into BISE w/collaboration from BN S2 sections**
- **Annual certification prior to BCT FTX—recommendation to execute multiple FTXs throughout the year to develop and refine BCT S2 INTEL TACSOP**

- **Five day FTX conducted at MTC, Foundry, and live SIGINT at training range**
- **9 crews certified: IAW TC 2-19.403**
- **Annual certification prior to BCT FTX**

- **Ongoing Tier 4 certification based on SRM inprocessing of new paratroopers**
- **275 tasks evaluated across: All-Source; GEOINT; HUMINT; SIGINT; and MI Maintenance**
- **IAW TC 2-19.404 and 82nd MI Readiness Strategy**
- **MOS annual certification**
- **Tier 4 can include advanced individual training beyond those specified in TC 2-19.404 (i.e. SOC, ASOC, Space 200, PRIVAC, etc.)**

CTC Rotation
(28-30 days)
Tier 1 BCT FTX
(15-21 days)
Tier 2 BCT S2 FTX
(9 days: 2 day COMMEX, 5 day FTX, 2 day Recovery)
Tier 3 MICO FTX
(9 days: 2 day COMMEX, 5 day FTX, 2 day Recovery)
Tier 4 Individual Training
(ongoing, intel discipline dependent)
Equip. RESET
T4
T3
T4
T2
T4
T2
A/T3*
T2
T4
T1
JRTC
QTR 1
QTR 2
QTR 3
QTR 4

*may certify crew w/sister BCT or 525 E–MIB T3 FTX

Figure 4. 82nd Sample MI Training Strategy

event (Tier 1 MITS training event) must validate training by contributing to a larger combined arms exercise. This will demonstrate to maneuver commanders how individual through collective progression supports the specific mission for which a particular BCT is training. Second, MITS certifications must be rolled up as part of a "T" rating of the brigade engineer battalion/BCT. This is most easily captured via the metrics gathered in MITS Tiers 1 through 3.

82nd Airborne Division MITS Exercises Since the March 2018 Pilot Exercise

In June 2018, 1st BCT, 82nd Airborne (1/82 BCT), conducted a MITS Tier 3 field training exercise. In this iteration, 1/82 BCT applied lessons from previous Tier 3 events and adopted a variation of the 3/82 BCT model. Key takeaways are as follows:

- ✦ The BCT S-2 was involved from planning to execution to ensure the MI company's Tier 3 field training exercise's training objectives were synchronized with the BCT S-2's intelligence vision.
- ✦ The MI company deployed analysts and intelligence platforms to the field in order to form the brigade intelligence support element and simultaneously practice field craft in an austere environment.
- ✦ The brigade intelligence support element used the S-6's tactical communications node backbone to provide data transport as they would in a deployed scenario attached to a brigade tactical operations center.
- ✦ Crews certified independently shared a common IEWTPT scenario fed by the Fort Bragg mission training complex and Foundry teams (Joint Readiness Training Center's decisive action training environment 3.0).
- ✦ The 82nd Airborne Division G-2 provided evaluators resourced from sister brigades and XVIII Airborne Corps to provide an external look into the performance of the brigade's intelligence crews.

Building on lessons from previous iterations, 1/82 BCT applied two new concepts to the Tier 3 event. First, 1/82 BCT synchronized its MITS Tier 3 field training exercise with a brigade staff command post exercise. The benefit of this action was that the S-2 section and MI company commander successfully conducted a communications exercise and had sufficient troubleshooting time on the backbone of a functioning brigade tactical operations center network. Whereas the pilot field training exercises had scenario and networking problems during their table evaluations, 1/82 BCT was able to start its evaluation on time with a functioning scenario to drive the field training exercise. This observation further emphasizes the importance of a well-resourced communications exercise using the actual architecture network of the field training exercise.

Second, the 1/82 BCT S-2 planned to conduct a "Tier 2 concept" MITS field training exercise immediately after the completion of the Tier 3 field training exercise. Upon completion of the Tier 3 Table VI certification, the brigade intelligence support element planned to conduct a series of distributed intelligence reachback operations from multiple nodes in order to simulate how the BCT S-2 would phase in the brigade intelligence support element during an airborne operation. The "Tier 2" field training exercise would require the brigade intelligence support element to coordinate from several nodes and for the crews to cooperate under the umbrella of one overarching IEWTPT. In essence, this event sought to validate the BCT's intelligence tactical standing operating procedure battle rhythm, architecture, and reporting plans.

Unfortunately, because of training calendar conflicts, the planned Tier 2 MITS event was cut short and not revisited until the BCT's culminating field training exercise in July 2018. In concept, however, this "Tier 2" exercise could have easily been incorporated as an addition to the MITS Tier 3 event, given enough space on the unit's training calendar.

Concluding Thoughts

The sample MITS construct and six lessons articulated above can serve as a road map toward planning and executing effective intelligence training. However, it is critical to reiterate that training is commanders' business, and the impact of a MITS-related tiered progression is enhanced when there is direct commander involvement. To attain this, a division G-2 must effectively communicate their role as a training facilitator to commanders at all echelons, and a BCT S-2 must be intimately involved in planning and executing their MITS training to ensure it is within the context of the commander's intent and the mission at hand.

Endnotes

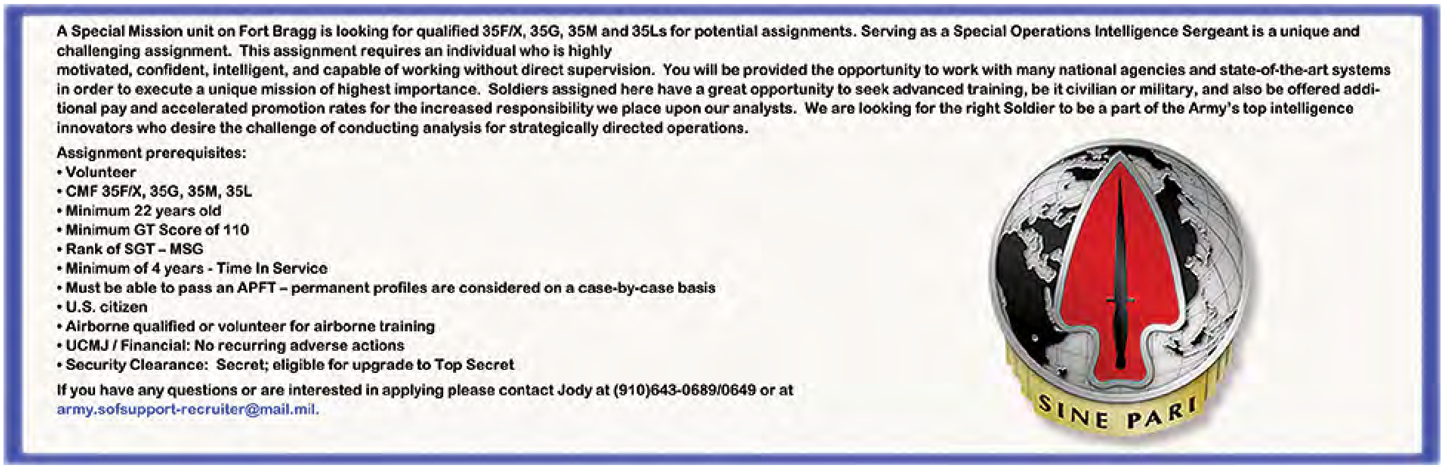
1. Department of the Army, Training Circular 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3* (Washington, DC: U.S. Government Publishing Office, 30 May 2018), 1-3.

2. Ibid.

3. Ibid.

LTC (P) Mike Adamski is a National Security Fellow at the John F. Kennedy School of Government at Harvard University. Previous assignments include G-2, 82nd Airborne Division, and S-2, 173rd Airborne Brigade, and he led the Counterterrorism/Special Operations Branch within the Joint Staff J-2. A graduate of Norwich University, he holds a master of arts degree from Georgetown University and a master of science degree from National Intelligence University.

MAJ William Denn is currently the Brigade Combat Team S-2 for the 1st Brigade Combat Team, 82nd Airborne Division. Previously he was the division G-2 planner for the 82nd Airborne Division where he designed the division's Military Intelligence Training Strategy and Military Intelligence Readiness Strategy. MAJ Denn is a 2006 graduate of the U.S. Military Academy at West Point and holds master's degrees from the John F. Kennedy School of Government at Harvard University, the U.S. Army Command and General Staff College, and the U.S. Army School of Advanced Military Studies. He is a recipient of the General Douglas MacArthur Leadership Award and the Command and General Staff College General George C. Marshall Award.



Training to Win: 4th Infantry Division Experience with Warfighter Exercise 18-04

by Lieutenant Colonel Thomas W. Spahr and
Chief Warrant Officer 3 Angelina Oliva

Introduction

For a division or corps to achieve maximum success against the agile and lethal Mission Command Training Program (MCTP) opposing force (OPFOR), it must start with an effective intelligence team. The 4th Infantry Division (4th ID) G-2 had a significant impact on the division's success during Warfighter Exercise (WFX) 18-04 in April 2018 in large part because it had an effective intelligence training plan. The team built a sound and redundant intelligence architecture, conducted multiple repetitions on our warfighting tasks, and successfully reached across the U.S. Army's intelligence community to leverage the necessary support. This article describes how the 4th ID G-2 section trained for WFX 18-04 so that Army leaders, especially other G-2s and S-2s, can build upon this success and learn from the challenges. The WFXs can be incredibly effective and rewarding events; and if the division G-2 arrives prepared, the positive effects multiply exponentially.

Creating a Climate to Excel

WFX 18-04 was a multinational corps- and division-focused exercise based on Korean terrain; the exercise incorporated a blend of Korean threat equipment augmented by near-peer capabilities. The live training audiences included the 18th Airborne Corps, the 3d (United Kingdom) Division, and the 4th ID. Within the 4th ID, the division artillery and 4th Combat Aviation Brigade were also live training audiences. WFX 18-04 was the first WFX that incorporated an international training audience and a mission-partnered environment network, which presented additional challenges for the communications architecture and intelligence sharing.

The 4th ID commander created a climate that enabled the intelligence team to excel. He approached this exercise with the mantra of "winning matters" and afforded the staff the time, focus, and resources to learn what it would take to win. The G-2 team was able to study the enemy and MCTP operational environment, and share with the division staff what they learned in leadership professional development (LPD) sessions. The division leadership created a simplified battle rhythm and minimized production requirements to allow time to think and collaborate. The division staff determined early on in its study of the problem that targeting was key to success, and thus the G-2 focused on the targeting process. The result was that the division succeeded in eliminating a large number of enemy forces and seizing its operational objectives.

4th Infantry Division Intelligence Training Glide Path

Key to the G-2's success was the development of clear training guidance early on that emphasized intelligence preparation of the battlefield (IPB), the targeting process, and building proficiency through repetition. The IPB included a detailed study of the terrain, threat, and understanding the MCTP operational environment—and then sharing that knowledge across the division staff. About 10 months out from WFX 18-04, the G-2 team conducted the first of several video teleconferences with the G-2 from another division that had just completed a WFX. In all, the team gathered lessons from five different divisions through video teleconferences, teleconferences, and visits.

Next, the intelligence team took full advantage of the MCTP OPFOR ride-along, sending eight personnel spread over the four rotations before WFX 18-04. The OPFOR ride-along is a program during which MCTP allows personnel preparing for a WFX to visit and see how the OPFOR is organized and operates during another unit's WFX. This event offers the opportunity to truly understand how the OPFOR fights and the limitations of the simulation. We applaud the MCTP team for accepting our leaders and their openness during these visits. The OPFOR ride-along helped the 4th ID to understand the operational environment.[1]

The 4th ID chain of command supported the G-2 massing personnel on the MCTP academics event. By taking seven G-2 leaders to this conference, the intelligence team gained an expanded understanding of the exercise, conducted important repetition on the military decision-making process, and had a good team-builder with the division staff, including a new division commander. Having the leaders of the different intelligence functions present to hear the new commander's guidance was important to practicing disciplined initiative throughout the WFX.

Next, the intelligence team worked closely with the Fort Carson, Colorado, Foundry Platform and mission training complex to design training. In the months before the intensive WFX train-up, the staff conducted multiple division-led brigade field training exercises. During these events, the G-2 forged a strong relationship with the Foundry and mission training complex leaders and gained an expanded understanding of how simulations work.

Intelligence architecture was a priority, especially with the addition of the mission-partnered environment network. Early in the training progression, the G-2 set a goal of having five Digital Intelligence Systems Master Gunner (DISMG) graduates in the division headquarters. While the G-2 team only achieved four DISMGs, these leaders, representing different intelligence disciplines, proved important to achieving success with our digital systems. While DISMGs alone could not maintain the complex intelligence architecture that was required for WFX 18-04, they proved critical in establishing roles and responsibilities for architecture design within the G-2, and they established an architecture glide path with adequate touchpoints to ensure the 4th ID G-2 was ready for the WFX. In addition, the 4th ID G-2 DISMGs developed a network of personnel throughout the Army intelligence community that they regularly contacted for support.

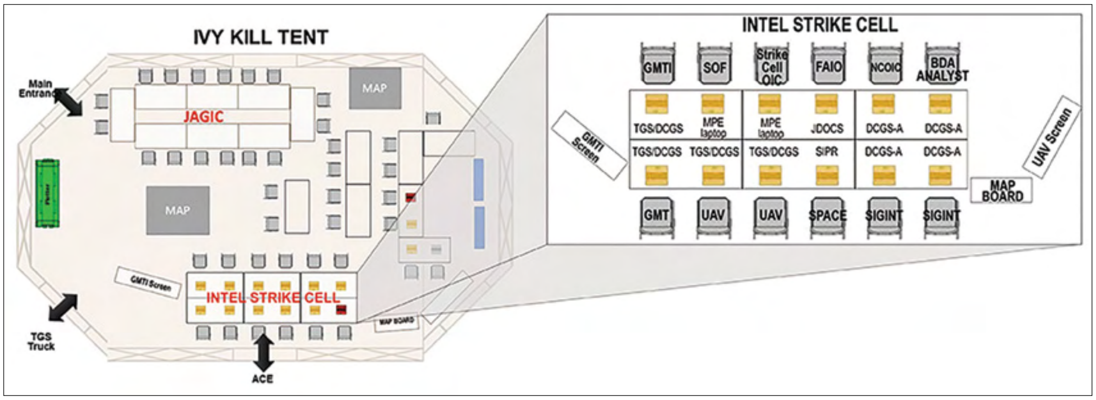


Figure 1. Kill Tent and Strike Cell

Finally, the division embedded several analysts into other divisions during WFX 18-03, conducted in February 2018, to learn through experience. Specifically, the G-2 embedded two ground moving target indicator (GMTI) operators, one signals intelligence (SIGINT) analyst, and the division intelligence targeting officer (a military intelligence captain) into the 101st Airborne Division and 1st Infantry Division during WFX 18-03.

During these visits and exercises, the 4th ID learned several key lessons that shaped future preparation. The division artillery commander and the division G-2 established early on that efficiency in the targeting process—linking the sensor to shooter—would be essential to achieving success. The team lived with the ideal that every analyst supported the targeting planners and focused energy on building an efficient processing, exploitation, and dissemination cell (that we referred to as the strike cell), locating it next to the Joint Air Ground Integration Center (JAGIC). Proximity led to cooperation, and the strike cell and JAGIC rapidly developed targets and tracked battle damage assessments together. The team learned that manned-unmanned teaming was extremely effective in the simulation, which influenced the decision to allocate two of four Gray Eagles to manned-unmanned teaming, working directly for the combat aviation brigade for a large portion of the fight. Having a combat aviation brigade that was a live training audience also made manned-unmanned teaming significantly more lethal. Other divisions shared that the GMTI was very effective in the simulation, and with practice, an analyst could detect clear patterns and indicators.

The 4th ID team also observed that other divisions were struggling with their intelligence architecture, specifically when using their Distributed Common Ground System-Army (DCGS–A) Analysis and Control Element (ACE) Block II for data correlation to manage large volumes of message traffic. The division SIGINT teams in particular struggled to make sense of the thousands of SIGINT tactical reports that were important to both targeting and predictive analysis. These correlation challenges contributed to the G-2's decision to push for an early fielding of DCGS–A Version 3.2.5 Service Pack 1 instead of receiving Version 3.2.4. Version 3.2.5 came with a Fusion Exploitation Framework correlation system that replaced the ACE Block II, and Generic Area Limitation Environment (GALE) software that facilitated SIGINT targeting based on the geospatial location of reports. Service Pack 1 also provided additional geospatial intelligence (GEOINT) tools that proved important during IPB steps 1 and 2 (terrain-focused). This was a calculated risk because the 4th ID was due to upgrade in December, just 5 months before WFX 18-04. With significant assistance from Project Manager DCGS–A, and tremendous help from the 4th ID DCGS–A field software engineer, the team successfully completed the upgrade. Fort Carson was fortunate to have resident a DCGS–A field software engineer who was an expert on Version 3.2.5 Service Pack 1, and requested and received support during WFX 18-04 from field software engineers stationed at other posts who shared this expertise.

Experience Matters

By day 6 of WFX 18-04, the 3rd Armored Brigade Combat Team, 4th ID, had penetrated the enemy flank and was about to launch an attack in the OPFOR rear area. The OPFOR still maintained in reserve a battalion (-) of M1985 240mm rocket launchers that were concealed in an underground facility. The G-2 team's IPB and study of historic GMTIs identified several likely locations of the M1985 battalion and helped focus our deep named areas of interest for our GMTI processing, exploitation, and dissemination team. At 0330, the OPFOR rocket battalion emerged and moved into position to fire on the 3rd Armored Brigade Combat Team. The private first class who had been embedded with the 1st Infantry Division during WFX 18-03, and was the subject matter expert on GMTI, identified the M1985 battalion immediately by its signature as it moved into firing position. He alerted the intelligence strike cell chief and the JAGIC chief who immediately vectored close air support on the location and destroyed the entire battalion of M1985s before they could fire.

To disseminate the growing knowledge of the threat throughout the G-2 and the rest of the staff, the intelligence team published multiple iterations of a smart book and conducted LPD sessions. The most valuable portions of the smart book included charts with the key weapons systems and their ranges and vulnerabilities. The division commander led the staff LPD program and placed a heavy emphasis on intelligence. These training sessions included a lessons learned presentation that the G-2 led based on visits to other divisions and OPFOR ride-alongs, and a terrain-specific LPD session featuring fly-throughs of the key locations. The division's fire support coordination cell and the division engineer also led LPD sessions on enemy fires and engineer capabilities. The G-2's internal LPD program focused on the intelligence architecture and lessons from other divisions' rotations—whenever members of the G-2 visited another division or conducted an OPFOR ride-along, they were required to lead a working lunch discussion to disseminate what they had learned. Finally, as the team expanded its knowledge of the environment, it became necessary to review the intelligence architecture during the weekly G-2 training meeting to identify friction points and ensure shared understanding.

The G-2 and G-3 teams also invested early in understanding the terrain and experimenting with how best to visualize the battlefield. The 4th ID GEOINT team led one of the first division LPD sessions, which focused on the Korean topography. The GEOINT Soldiers leveraged the new tools that came with their upgraded DCGS–A to display fly-through perspectives of the main routes and key terrain in the scenario. This LPD session served as a forcing function for the GEOINT analysts to become proficient with new capabilities that came with DCGS–A Service Pack 1 and helped the staff realize the terrain challenges present in this scenario. This LPD session enabled the division leadership to weigh in on how they liked to visualize the terrain and ultimately influenced many of the division commander's decisions throughout WFX 18-04.

Five months before the exercise, the G-2 and G-3 established what the standard division map would look like and built a map that made the dominant land features easy to see. Utilizing the Situational Awareness Geospatially Enabled tool on our DCGS–A GEOINT workstation, the 4th ID GEOINT analysts leveraged hill shade and a color-tinted shaded relief layer to make the higher elevations stand out. The analysts used a transparent yellow (restricted) and red (severely restricted) cross hash to annotate restricted terrain. Next, the GEOINT team ensured the standard map was displayed in analog throughout the tactical operations center and in all of our mission command systems. They worked with the division G-6 and the field support representatives for the major systems—notably Command Post of the Future—and learned how to push the digital map from the GEOINT server to each staff member's computer. The efforts of the GEOINT analysts made the terrain easy to visualize; and by using the same map in both our analog and digital systems through the final field training exercise, military decision-making process, and WFX, the staff became very confident with their knowledge of and could easily visualize the battlefield.

Building Muscle Memory through Repetition

In addition to emphasizing IPB and the intelligence architecture, the 4th ID G-2 programmed repetition on the intelligence systems into the training schedule. The intelligence architecture was complicated by the incorporation of the mission-partnered environment network and the new DCGS–A Version 3.2.5 Service Pack 1. It was evident that the team needed a few practice runs. The 4th ID was able to conduct only two command post exercises in preparation for WFX 18-04, but the division took full advantage of two brigade field training exercises by standing up the division main operations center in a field environment and training on targeting and battle tracking. The 4th ID also benefitted from other divisions' training events.

In early January 2018, the G-2 section conducted an intelligence communications exercise using data from the 1st Infantry Division's command post exercise-3 to practice with the newly issued DCGS–A Service Pack 1. The Global Simulation Center, which supports division command post exercises with simulation data from its location on Fort Leavenworth, Kansas, enabled the 4th ID to receive the

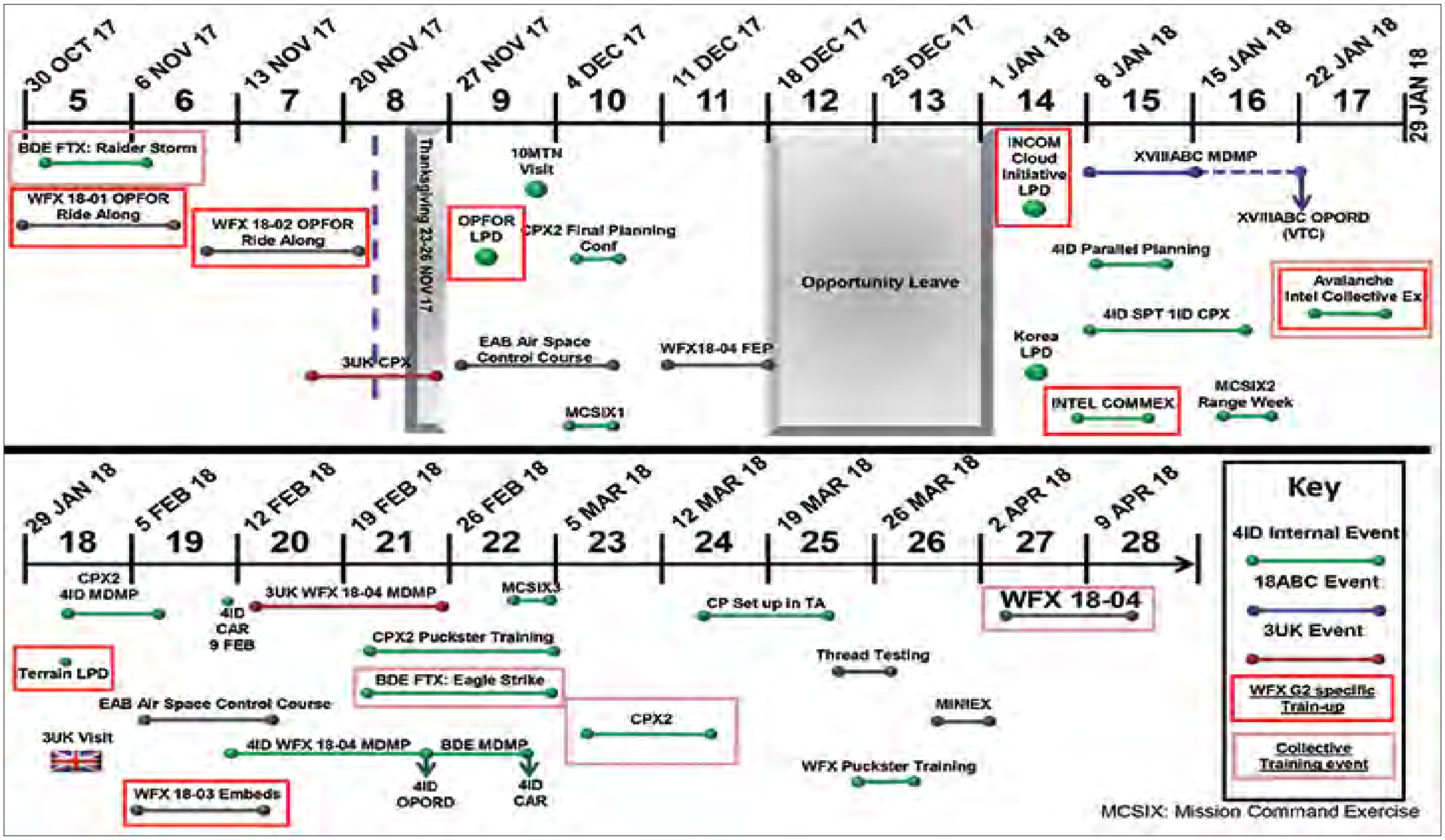


Figure 2. Road to WFX 18-04

same data feed as the 1st Infantry Division so that the analysts could practice manipulating messages with their new systems. Project Manager DCGS–A sent an intelligence process and analysis team to Fort Carson to help train during this communications exercise. The intelligence communications exercise filled critical gaps in training for data correlation and database management using the Fusion Exploitation Framework. The ACE was also able to establish the intelligence architecture to pass data between the Joint Worldwide Intelligence Communications System and SECRET Internet Protocol Router Network (SIPRNET), and between SIPRNET and the mission-partnered environment using the Cross Domain Solution Suite Tactical Communications Support Processor Version 9.1. Finally, the SIGINT team practiced processing tactical reports using the DCGS–A Enabled Single Source Version 6.6 and GALE on SIPRNET. The communications exercise set the team up for success as it began division collective training.

The division G-2 section gained another valuable repetition during the intelligence collective exercise, Avalanche ’18, conducted in late January. Avalanche ’18 was an exercise supported by the Foundry Intelligence Training program, Intelligence and Electronic Warfare Tactical Proficiency Trainer, and U.S. Army Training and Doctrine Command (TRADOC) G-27. The exercise served as the Tier 2 testing for the division’s Military Intelligence Training Strategy and gave the intelligence team time to work on its systems, at its own pace, in isolation from the division staff. The exercise incorporated the division G-2 section and portions of the 4th ID division artillery S-2, 4th Combat Aviation Brigade S-2, and the division’s fire support coordination cell. Project Manager DCGS–A again sent mentors to work closely with the analysts on DCGS–A Version 3.2.5 Service Pack 1. The TRADOC G-27 built the scenario based upon guidance from the G-2 and the Foundry program director, as well as conversations with TRADOC counterparts at MCTP. The goal was to mirror what the 4th ID would experience during WFX 18-04. The Intelligence and Electronic Warfare Tactical Proficiency Trainer constructed the simulated message traffic based on the scenario the TRADOC G-27 designed. Finally, Foundry instructors and other units located on Fort Carson and in Colorado Springs (10th Special Forces Group and U.S. Northern Command) acted as observer controllers.

During Avalanche ’18, the G-2 section focused heavily on mastering and presenting the IPB and on conducting the intelligence portion of the daily targeting brief. The exercise began with the G-2 section deploying its portion of the division main command post to the back pad at the Fort Carson mission training complex, which worked well because it forced the team to operate in tents and use power generators as they would during WFX 18-04. At the same time, the G-2 leadership simplified the communications architecture by plugging into the mission training complex's hard-wire SIPRNET to avoid delays sometimes caused by the division's tactical communications systems, thus allowing the intelligence analysts to focus on mastering their tools on DCGS–A. Perhaps the most beneficial part of this exercise was isolating the G-2 team from daily garrison activities so that they could practice on their systems.

When the time arrived for the division's second and final command post exercises in March, the G-2 team had already conducted multiple repetitions, which enabled them to move beyond the science of the WFX and into the art necessary to win. During the first few days of this exercise, the G-2 and JAGIC leaders regularly walked into the mission training complex and talked in person with the subordinate support cells, the pucksters (a.k.a. virtual soldiers), and the unmanned aircraft system pilots. By witnessing firsthand how manned-unmanned teaming works versus flying unmanned aerial vehicles on Multiple Unified Simulation Environment boxes, the collection management team was able to make better decisions on how to allocate the division's Gray Eagles for different missions. Command post exercise-2 was a slightly longer exercise (8 days) than a typical command post exercise, which provided an effective repetition for the strike cell and JAGIC to continue to build the synergy between these two elements that proved so important for dynamic targeting during WFX 18-04.

Throughout each of these exercises, the G-2 team worked hard to build redundancy into the network. The division invested heavily in building a support area command post that had all the functions of the division main command post plus a more robust SIGINT and human intelligence element. The G-2 ensured that both Trojan SPIRITs and Cross Domain Solution Suites were fully functional and running at the division main and support area command posts, which provided reliable top secret communications and a backup to the G-6 SIPRNET connection.

The intelligence team also invested early in learning to access and manipulate the U.S. Army Intelligence and Security Command Cloud Initiative (ICI) as a backup to the Fusion Exploitation Framework for data correlation. The ICI team on Fort Bragg, North Carolina, participated in the intelligence communications exercise, Avalanche '18, and during both division command post exercises. Approximately 4 months before WFX 18-04, the ICI lead visited Fort Carson and conducted an LPD session for all the intelligence leaders on post. ICI served as the redundant method to correlate the massive volume of U.S. message text formatted message traffic and the primary method during division main command post jump operations. The ICI functioned independently from the 4th ID architecture, and all the correlation happened at the ICI location on Fort Bragg. The 4th ID received the correlated data with a lag time of under 1 second via the ICI portal on SIPRNET. Since our division tactical command post was intended to be light, mobile, and only a temporary command and control node while the division main command post jumped, the G-2 relied exclusively on the ICI at that location.

Conclusion

WFX 18-04 was a challenging yet rewarding exercise for the 4th ID team, and we are grateful to all the intelligence professionals across the Army who supported this event. The division G-2 was able to adequately inform the division commander's decision cycle by defining the problem early on, implementing redundant solutions, and then practicing our trade in multiple collective exercises. By providing accurate and timely intelligence, the 4th ID intelligence team was a significant contributor to the division's success.

Endnote

1. For a more detailed description of the opposing force (OPFOR) ride-along, see Jennifer Chapman and Patrick Madden, "A Division G-2's Impressions During an OPFOR Ride Along," *Red Diamond Threats Newsletter* 8, no. 4 (April 2017): 17-22, https://community.apan.org/wg/tradoc-g2/ace-threats-integration/m/documents/210969/.

Reference

4th Infantry Division G-2 memorandum to Program Management Distributed Common Ground System-Army and U.S. Army Training and Doctrine Command Capabilities Manager. "4th Infantry Division's Integration of DCGS–A SP1 for Warfighter 18-04." 6 June 2018.

LTC Thomas W. Spahr served as the division G-2 for the 4th Infantry Division (4th ID) from June 2016 to June 2018. His prior assignments include speechwriter for the Vice Chief of Staff of the Army; brigade combat team S-2, 4th Brigade Combat Team, 82nd Airborne Division; and S-3 of the Army Geospatial Intelligence Battalion. He has a Ph.D. in history from Ohio State University and taught history at West Point and the U.S. Air Force Academy. LTC Spahr is currently a student at the Army War College.

CW3 Angelina Oliva served as the deputy collection manager and senior Digital Intelligence Systems Master Gunner for the 4th ID G-2 from July 2017 to July 2018. She served within the 4th ID as the targeting technician and senior all source intelligence technician from August 2015 to June 2017. Her prior assignments include deputy branch chief, Counterterrorism Branch–Southeast Asia Division, Joint Intelligence and Operations Center, U.S. Indo-Pacific Command; and senior all source intelligence technician G-2 Analysis and Control Element, III Corps. CW3 Oliva is currently a degree completion program student at the University of Colorado.

Soviet Shapers of the Russian Approach to Large-Scale Combat Operations

by Lester W. Grau, Ph.D.

The author assumes responsibility for the veracity, accuracy, and source documentation material, including no use of classified material and conformity to copyright and usage permission. The views expressed in this article are those of the author and do not necessarily represent the official policy or position of the Foreign Military Studies Office, Department of the Army, Department of Defense, or U.S. Government.

Editor's Note: Dr. Grau wrote this article in tandem with the article that follows by MAJ Charles Bartles, titled "Russian Force Structure for the Conduct of Large-Scale Combat Operations."

Our class enemies are empiricists, i.e., they move from case to case, directed not by an analysis of historical development, but by practical experience, routine, quick assessment and scent.
— Leon Trotsky

What's past is prologue.
—William Shakespeare, The Tempest

Introduction

The new Russia has emerged as a Eurasian power, determined to regain its status and defend its borders. Although a lot has changed in the past 27 years, much of current Russian military thought still uses the Soviet concepts of strategy, operational art, and tactics. Artillery also remains a major component of large-scale combat operations, as well as the use of a mathematical model known as the correlation of forces and means (COFM). The Soviets/Russians have used the COFM model to identify the right amount of combat power needed, allowing flexibility in operational planning. An upgraded COFM model, operational art, fires, and maneuver will continue to influence Russian operational planning, as will the memory of Soviet experiences in World War II and the nuclear standoff of the Cold War. Russia is again determining how best to conduct conventional maneuver operational war under nuclear-threatened conditions, should this become necessary.

The "Revolution in Military Affairs"

In many respects, the U.S. Army has a tactical focus. The Russian Army has an operational focus. This difference is due to differences in geography, history, culture, military thought, and use of mathematical determinism. The Russian Empire, Soviet Empire, and modern Russia had/have the world's longest borders and a large landmass to defend. Throughout its history, all of its neighbors have invaded Russia—even non-bordering countries have gone well out of their way to invade them. Extending from this, today's Russia feels threatened, particularly by the North Atlantic Treaty Organization (NATO) expansion, color revolutions,[1] the U.S. abrogation of the Anti-Ballistic Missile

Treaty, and the U.S. Prompt Global Strike Command. In this context, Russians ask, how do we best defend the motherland?

During World War II, equally sized American and Soviet tactical units were not usually a match for equally sized units of their German enemy. The German Army was tactically proficient, regionally based, and better trained. The Soviet Union, which bore the brunt of the fight against Germany, won the war, not on the tactical level, but on the operational level. After the defensive operations of Kursk and Stalingrad, the Red Army began a series of offensive operations (by armies and fronts—a *front* is roughly an army group of three to five armies) against the Germans. Thirty-one Soviet fronts were constituted during the war. The General Staff designed these offensive operations not to culminate before launching another operation in a different sector. This constantly wrong-footed the Germans, who continually moved their operational and strategic reserves to the wrong area while the Red Army triumphantly advanced in another. During the Great Patriotic War (the Soviet war with Germany), the Soviets conducted more than 100 multi-front operations and more than 1,000 frontal operations. The Soviets won their war against Germany and their short war against the Japanese Kwantung Army on the operational level. Soviet military and civilian dead exceeded 20 million. More than 8 million of these were military from the 30 million raised for the war. From this horrendous experience, the Soviet Government decided that never again would it accept such losses.

The Soviet acquisition of atomic weapons in 1948 provided the possibility that the Soviets could use these weapons to avoid such future losses. However, Stalin envisioned future war only as a conventional war similar to that which the USSR had just conducted. Atomic weapons were merely more powerful artillery. However, with the death of Stalin in 1953, the "Revolution in Military Affairs" (the marriage of the atomic weapon with cybernetics and a long-range delivery system) began. The Soviet military began dual tracking for both conventional and nuclear war. Ground forces were cut from four to two million to provide funding for the development and fielding of the Strategic Rocket Forces. The assumption was that future war would become nuclear at a certain stage. This changed in 1968. The assumption had been that nuclear war would be short and violent and that the tempo of combat would greatly increase. However, the Voroshilov Academy of the General Staff conducted a study to determine whether nuclear weapons would really increase tempo. The findings were that tempo would be practically identical in both nuclear and conventional warfare in Europe. Irradiated zones, flooding, forest fires, destroyed cities, destroyed infrastructure, disease, and pestilence would severely retard the tempo of an advance in a nuclear conflict. And the prevailing winds in Europe blow to the east—carrying radioactive contamination with them.

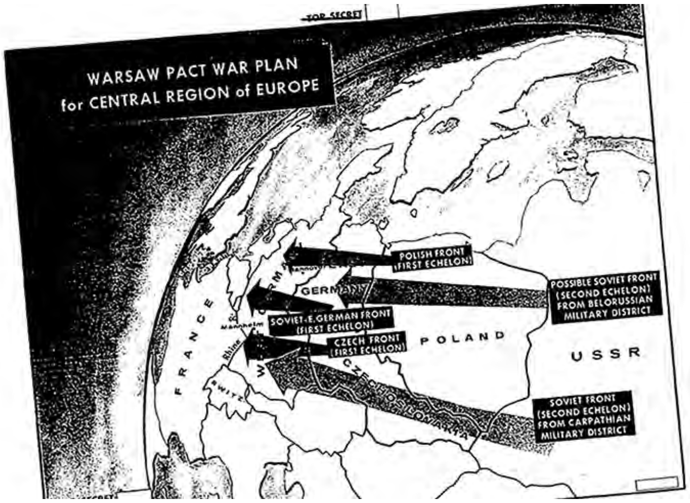

TOP SECRET
WARSAW PACT WAR PLAN for CENTRAL REGION of EUROPE
POLISH FRONT (FIRST ECHELON)
POSSIBLE SOVIET FRONT (SECOND ECHELON) FROM BELORUSSIAN MILITARY DISTRICT
GERMANY
SOVIET-E.GERMAN FRONT (FIRST ECHELON)
Mannheim
CZECH FRONT (FIRST ECHELON)
POLAND
USSR
Rhine
FRANCE
SWITZ
CZECHOSLOVAKIA
SOVIET FRONT (SECOND ECHELON) FROM CARPATHIAN MILITARY DISTRICT

Photo courtesy of the CIA's Historical Collections

June 1968. This map from the booklet "CIA Analysis of the Warsaw Pact Forces: The Importance of Clandestine Reporting" was developed by the CIA to show the Warsaw Pact war plan for the central region of Europe.

Soviet planning returned to a balanced capability and a doctrine for fighting both nuclear and conventional war. New weapons and technology, such as micro-circuitry, directed energy, and genetic engineering blurred the distinction between nuclear and conventional war. As the Soviet Union and NATO faced off during the Cold War from 1968 to the collapse of the Soviet Union, both sides assumed that a future war in Europe would involve large maneuver forces from NATO and the Warsaw Pact fighting under nuclear-threatened conditions on the European plains. The NATO plan was primarily a large-scale defense to weaken and delay the Soviet offensive. There was a tacit understanding that at some point the confrontation could move into operational and, possibly, strategic nuclear exchange. All Soviet Cold War plans supposedly had a nuclear annex. In order to conduct a war against NATO or China, the Soviet Union reportedly had 210 to 211 motorized rifle and tank divisions, 17 artillery divisions, 8 airborne divisions, 5 antiaircraft and missile air defense divisions, and 11 rear-area divisions, plus specialized divisions such as coastal defense and machine gun-artillery border defense divisions. Not all of these divisions were full-up, ready divisions. The ready divisions were facing China and NATO. Many of the other divisions were mobilization divisions with sufficient combat equipment, but only partial manning by cadre staffs and an understrength regiment or two. During general mobilization, reservists were to fully man these divisions. In a nation where all able-bodied males were conscripted for 2 or

3 years of military service, there were plenty of reservists with specific mobilization assignments.

The Great Debate

Current Russian military thought is grounded in the Tukhachevsky-Svechin debates of the 1930s [described below], the Soviet operational experiences of World War II, and the lessons of the Cold War nuclear standoff. The destruction school, headed by Marshal Mikhail Tukhachevsky (and including such luminaries as Mikhail Frunze, Vladimir Triandafilov, and Nikolai Varfolomeev) argued that future war was about mobility and firepower. To those Russian military minds, defense is useless because a country cannot defend against such weaponry. The enemy should not be allowed to visit destruction on the Soviet Union. Rather, when the enemy attacks, the proper response is to mount a series of immediate overwhelming counterstrikes against the enemy's territory. The proletariat of the enemy nation would rise and greet the Soviets as liberators. The attrition school, headed by General Aleksandr Svechin, argued that, in a world war, attrition is sensible and economic and the only way to achieve victory. A resolute attack consumes incalculable resources and, as a rule, is not justified by operational gains. Attacking forces run the risk of interdiction of lines of communication and flank attacks. The Soviet Union is vast, and the Soviet territory most likely to be involved in an enemy attack is rolling plains, vast rivers, large swamps, forests, and limited roads (which are impassable during the spring thaw and the wet autumn partial freezes). The best way to defend the Soviet Union is to draw the enemy into the depths of the country where the enemy's combat power and logistics would be stretched to the breaking point. Only after the enemy had reached its culmination point, should the Soviets conduct a massive counterstrike to destroy the enemy within the depths of the Soviet Union. This debate continued over a decade, but Svechin ultimately lost. When Germany attacked the Soviet Union in June 1941, the Soviets first mounted uncoordinated counterstrikes and then piled up defensive forces far forward—these blunders almost cost the Soviet Union the war. The popular theorist of today's Russian military is Svechin.[2]

Soviet/Russian Military Art is Divided into Strategy, Operational Art, and Tactics

Current Russian military thought still uses the terms and concepts from the Soviet period: strategy, operational art, and tactics.

Strategy investigates the nature and laws of armed conflict. It is derived from military doctrine, military experience, and an analysis of contemporary political, economic, and military conditions. It includes the preparation and conduct of strategic operations, the conditions and character of future war, methods for preparing for and conducting war, types and use of armed forces, and strategic support of operations and leadership.[3]

Soviet/Russian Military Art

Strategy: investigates the nature and laws of armed conflict.

Operational Art: encompasses the theory and practice of preparing and conducting operations by large units.

Tactics: deals with the preparation and conduct of combat by division and below.

Operational art encompasses the theory and practice of preparing and conducting combined and independent operations by large units (fronts and armies). It holds the intermediate position between strategy and tactics. Stemming from strategic requirements, operational art determines the methods of preparing for and conducting operations to achieve strategic goals while determining the task and direction for the development of tactics.[4]

Tactics deals with the preparation and conduct of combat by division, regiment, battalion, and below.[5] Consequently, large-scale military combat is still classified within the Russian operational art and deals with the management of armies and fronts.[6] During World War I, there was not a climactic final battle that decided the conflict. The best that the contending forces could achieve was tactical or temporal success. From this observation at the time, Soviet military theorists studied the changing nature of war and determined that there was an operational realm. Their main theorists discussed and debated this concept, including most of the participants in the Tukhachevsky-Svechin debates of the 1930s. All agreed on the importance of conducting successive operations.[7] This was a pivotal time for the development of Soviet military thought and led to the Soviet victories in World War II. Unfortunately, none of this distinguished group of military theorists survived to view their success. They all were victims of Stalin's purges (1937 to 1938) preceding the German invasion. The terrain, weather, and incredible sacrifices of the Soviet peoples slowed the German advance while the Red Army rebuilt itself and learned to fight on the operational plane.

Key to the operational art that developed during World War II was deception planning. The Soviets did not conceal their intention to attack as much as the scale, scope, and location of the attack. The Soviets proved they could conceal what they wished to conceal and put an extensive effort into it.

Timing was also a key factor of the developing operational art. There was never a simultaneous Soviet attack along the entire front. Artillery fires should be sufficient and massed, and so one attack would be launched and then the artillery divisions would be shifted to support the next attack. The Soviets noted that the Germans would always move their reserve to deal with the initial attack, and if they launched enough attacks, the operational reserve would never get committed. The first place that the Soviets would attack would usually end up as the main effort, but often the Soviets had more than one effort. The Germans became proficient in using Soviet artillery patterns and reconnaissance efforts as indicators of attack. The Soviets discovered this and began duplicating these patterns as part of their deception efforts.

Operational encirclements were a key element of the developing operational art and grew out of the works of Tukhachevsky. More than 200 Axis division-sized units were surrounded and destroyed during 12 major Soviet encirclements.[8] Toward the end of the Cold War, the functional tasks of the Soviet operational planners were to—

- "Investigate the rules, nature, and character of contemporary operations (combat action).
- Work out the means for preparing and conducting combat operations.
- Determine the function of large units (fronts, armies) and formations (divisions) of the Armed Forces.
- Establish means and methods for organizing and supporting continuous cooperation, security, and command and control of forces in combat.
- Delineate the organizational and equipment requirements of large units of the Armed Forces.
- Work out the nature and methods of operational training for officers, and command and control organs.
- Develop recommendations for the operational preparation of a theater of military operations (TVD).
- Investigate enemy views on the conduct of operational combat."[9]

These functional tasks could almost be the table of contents of current Russian professional military education journals.

Fire Enables Maneuver and is a Form of Maneuver

Artillery has always held pride-of-place in the Soviet/Russian military. Direct fire artillery and/or mortars were an integral part of Soviet infantry battalions, and it was normal practice for an artillery battalion (sometimes two) to be in direct support of an infantry (motorized rifle) or tank battalion. The Soviet Army was an artillery army with a lot of tanks. Massed artillery could blast gaps through stubborn defenses, defeat counterattacks, deny critical terrain to an enemy, gain ground, and create induced psychological paralysis and terror in enemy forces. Massed artillery was tighter and more effective within a 10-kilometer range, so Soviet artillery was always much further forward than that of NATO forces. Much of this artillery was positioned in direct lay for "fire over open sights." Direct fire artillery is more responsive, more accurate, and more destructive. Further, direct fire or minimum elevation artillery firing allows friendly aviation to overfly friendly territory without closing down artillery support.

Precision-fire artillery and the development of a quick detect-destroy cycle had long been a goal of Soviet artillery. Remarkable headway was made in this direction (and has been achieved today), but the need, efficacy, and wide range of applications of massed fire artillery remain.

Like all competent gunners, the Soviets prefer to move their artillery after a fire mission to avoid enemy counterbattery fire. However, the Soviets also developed the concept of "maneuver by fire" [манёвр огнём]. Maneuver by fire shifts massed artillery fires within range onto a single key target to destroy it rapidly. The gunners accept risk by continuing firing, without shifting firing positions, until they destroy their target. The fire planning can be for a single concentrated mission or several, and the mission may be against several targets or shifted from one heading to another. Maneuver by fire is intended to accept risk in order to gain fire superiority over the enemy. Maneuver by fire can defeat counterattacks, deny critical terrain to an enemy, gain ground, or perform other maneuver force missions.[10]

Artillery has always been a major component of Soviet/Russian large-scale combat operations. Artillery was well integrated within the Soviet maneuver units, but there was also a significant artillery reserve held at army, front, and the supreme command (Stavka) during World War II. This artillery was used to weight the offensive or defensive in key sectors. Larger special-purpose artillery (siege guns and mortars, railroad guns, and, later, nuclear-capable guns) were normally retained in artillery reserves.[11]

There was not a democratic distribution of assets, personnel, and supplies during World War II. Units that were making the main attack got what they needed. Units in a supporting or reserve role got less or got by with what they had. Artillery, as a major component of combat power, went to where it was needed to accomplish the mission. Calls for fire were treated similarly. This philosophy carried into the

By Пользователь/Creative Commons[12]

The 9K22 "Tunguska-M" Gun/Missile Air Defense System (NATO reporting name: SA-19 "Grison") photographed during the 2008 Moscow Victory Day Parade, May 9, 2008.

Cold War, and it is still one of the most visible aspects in present-day Russian training exercises and even actions in Ukraine.

Tactical Predictability Enables Operational Flexibility

Since its inception, the Soviet Army relied on scientific and mathematical approaches to problem-solving and operational planning. Marxism-Leninism was presented as a "scientific" approach to organizing society, and centralized planning was applied to society as a whole—creating upheaval, famine, economic disaster, and eventually a public compliance.

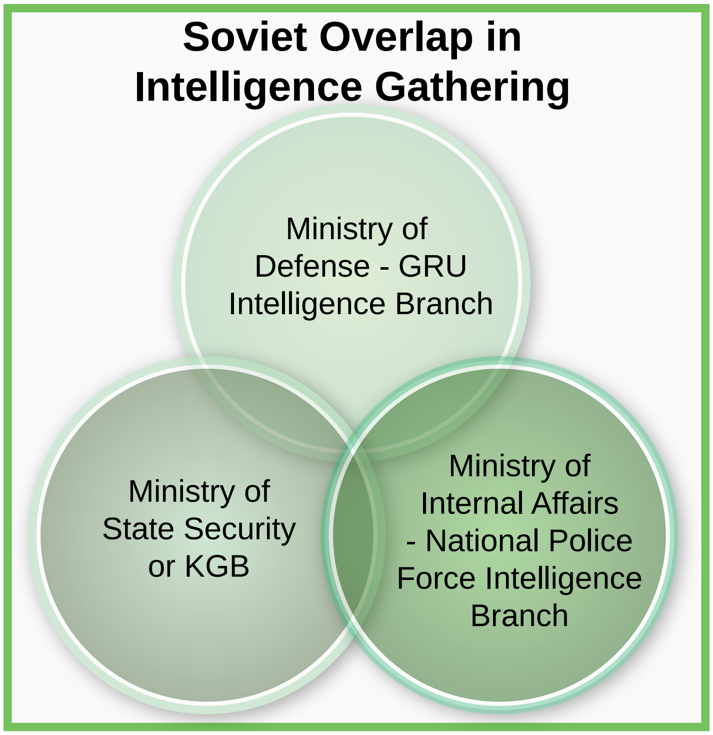
Fortunately, mathematics has a more reliable and more direct applicability to military affairs, and there was little math anxiety in the Soviet officer corps. Mathematics, in fact, is still emphasized throughout civilian and military education, and many articles in professional military journals are collections of formulae and a discussion of their applications. Recurring military activities such as movement rates, fuel consumption, distribution of rounds in an impact area, emplacement times, smoke dispersal, and the like, can be mathematically determined—and readily adjusted for variations in terrain, weather, and altitude. Many of these activities were encompassed by applicable formulae and nomograms[13] to allow quick and accurate solutions.

The Soviets further applied a scientific approach to operational planning with significant success. The Soviets studied military history as operations research and began to model combat based on detailed combat histories. One of the first problems was how to quantify military combat power. All tanks are not the same, nor are aggregates of like tanks comparable to aggregates of different tanks. A Soviet motorized rifle platoon may differ from a Belgian mechanized infantry platoon in size, vehicles, communications, armament, training, combat experience, morale, and motivation. Terrain, artillery support, and mission will further complicate any comparison.

The Soviets began by using their T-54 medium tank as base 1. All other tanks were compared to the T-54 using criteria such as armor, armaments, rate of fire, radius of action, chemical, biological, and radiological survivability, height, weight, fordability, communications, accuracy, cross-country mobility, rounds on board, and the like. All tanks were assigned a value relative to the T-54. Personnel carriers and other ground equipment were also rated against the T-54 and assigned a relative value. When the appropriate equipment was aggregated into respective tables of organization and equipment, it was possible to determine a mathematical value for the combat power of one unit and to compare it to another unit. However, this was not enough to determine if an attacker had a 3:1 advantage over a defender.

Combat is not fought on a pool table or chessboard. Mission (attacking, defending, retreating), terrain, training, time in combat, morale, readiness status, logistics support, regular soldiers versus reservists, and other factors all impact the mathematical value of the combat power of the unit. The Soviets determined mathematical "K" factors to apply to varying conditions to arrive at the realistic mathematical combat power for this unit.

The Soviets were interested in modeling tactical predictability where the outcome of a planned combat could be mathematically determined so that adequate combat power could be applied, while not committing too much power where it was not needed. This mathematical predictability of tactical combat allowed a great deal of flexibility in operational planning—where the Soviets had won their wars with Germany and Japan. This modeling is called the correlation of forces and means, or COFM. The Soviets produced corollary COFMs for artillery combat, air defense combat, air combat, and, reportedly, nuclear exchange. The Russian military inherited these models and the military scientists who devised and maintained them. This type of modeling is readily programmable in modern computer technology as are tactical formulae and nomograms.



Soviet Overlap in Intelligence Gathering

Ministry of Defense - GRU Intelligence Branch
Ministry of State Security or KGB
Ministry of Internal Affairs - National Police Force Intelligence Branch

Intelligence Drives the COFM Model

To the Soviet military mind, the best intelligence came from a scout, commander, attaché, agent, spy, or mole who had been on the ground and made an informed determination. Electronic sensors, trackers, transmissions, and devices can be duped or reprogrammed. The Soviets invested heavily in all types of electronic reconnaissance but preferred reports from the man or woman on the ground.

The Soviets had three uniformed armed forces under three different ministries. The most apparent was the Army, Navy, Air Force, Airborne Forces, and Strategic Rocket Forces of the Ministry of Defense. Its intelligence branch, the GRU [*Главное Разведывателное Управление*], was responsible for collecting military and technical intelligence on external threats and allies. The Ministry of Internal Affairs was responsible for internal security and constituted a national police force that kept public order, suppressed and investigated crime, incarcerated felons and ran prisons, fought fires, managed the nationwide internal passport and registration system, suppressed gangs and riots, and managed traffic. It was more than normal police forces and highway patrols since it had divisions of uniformed soldiers for internal control. Its police intelligence branch watched the citizenry and suppressed crime (except for political crimes). The Ministry of State Security or KGB [*Комитет Государственной Безопастности*] was a major intelligence and security organization responsible for foreign intelligence, counterintelligence, security investigations, border guards, guarding of communist party and Soviet Government leadership, and organization and safeguarding of government communications, as well as combating nationalism, dissent, anti-Soviet activities, and other political crimes. In addition to the border guards, it had divisions of uniformed soldiers to protect the Soviet Government. The Soviet Government further maintained these three powerful, uniformed armed forces as a protection against a coup de main by one of these ministries. Naturally, there was a lot of overlap in intelligence gathering, as the missions overlapped. Despite the division of labor, all three agencies could be working the same target.

Deconflicting intelligence reports from different agencies can be difficult. One of the advantages of the COFM model was its mathematical neutrality. The model presented a predictable outcome, but the model could be tweaked to safe-side an operational plan if the intelligence reports so indicated. Still, the COFM model required substantial input and regular updating to maintain its effectiveness. At the time, this could best be handled by intelligence operations focusing at the strategic and operational level. Today, it is harder to discern, but the idea of feeding the various mathematical models with data is voluminously evident in their unclassified military writings (discussions).[14]

Dealing with the New/Old Russia

The new Russia that emerged from the chaos following the dissolution of the Soviet Union is different from its communist past, but its history, culture, language, values, and worldview remain intact. Over the past decades, Russia has examined the Western world, adopting much of its technology but little else. It has reemerged as a Eurasian power with an increasing capacity to reach outside its traditional space. Russia challenges the world to regain its status and leadership and defend its borders. Small-scale difficulties such as Georgia, Crimea, the Donbas, and Syria can be handled with small forces. But this and future Russian leadership faces conditions that the Soviet leadership did not, such as a smaller population to guard a huge border, a more open media that forces the leadership to be more sensitive to casualties, and the loss of the western and southern buffer zones. New Russian military thinking must reflect these conditions as well. Russia is again determining how best to conduct conventional maneuver operational war under nuclear-threatened conditions, should this become necessary. Russia has made significant changes in how it will do so, but much remains the same. The key role of the operational art, fires, and maneuver, coupled with an upgraded, computerized COFM model, and other improved mathematical tools should be expected to continue to shape Russian operational planning. Current indicators are that they do.

T-72B3M main battle tanks at the Zapad 2017 exercise, September 14, 2017.

Photo courtesy of Ministry of Defense of the Russian Federation/Creative Commons[15]

Epigraphs

Leon Trotsky, "Military Doctrine or Pseudo-Military Doctrinairism," 1921, as translated by Dr. Grau from a 1988 source. A similar translation is available on the marxists.org website where David Walters has transcribed "Questions of Military Theory, Military Doctrine or Pseudo-Military Doctrinairism," in *The Military Writings of Leon Trotsky*, *Volume 5: 1921-1923*, https://www.marxists.org/archive/trotsky/1922/military/ch37.htm.

William Shakespeare, *The Tempest*, act 2, sc. 1.

Endnotes

1. The term *color revolution* describes "various related movements that developed in several countries of the former Soviet Union and the Balkans during the early 2000s. The term has also been applied to a number of revolutions elsewhere...These movements generally adopted a specific colour or flower as their symbol." Wikipedia, s.v. "Color revolution," last modified 11 September 2018, 11:47, https://en.wikipedia.org/wiki/Colour_revolution.

2. For an excellent English-language edition, see Aleksandr A. Svechin, *Strategy* (Minneapolis: East View Information Services, 1992) with introductory essays by Andrei A. Kokoshin, Valentin V. Larionov, Vladmir N. Lobov, and Jacob W. Kipp.

3. N. V. Ogarkov, "Стратегия Военная" [Military Strategy], *Советская Военная Энциклопедия* [Soviet Military Encyclopedia], vol. 7 (Moscow: Voyenizdat, 1979), 555-565. Note that the Soviets/Russians define doctrine as the nation's officially accepted system of scientifically founded views on the nature of wars and the use of armed forces in them.

4. V. G. Kulakov, "Оператйвное Искусство" [Operational Art], *Советская Военная Энциклопедия* [Soviet Military Encyclopedia], vol. 6 (Moscow: Voyenizdat, 1978), 53-57.

5. I. G. Pavlovskiy, "Тактика" [Tactics], *Советская Военная Энциклопедия* [Soviet Military Encyclopedia], vol. 7 (Moscow: Voyenizdat, 1979), 628-631. Today, the brigade would also be considered a tactical unit; however, depending on the theater, a division or brigade could have an operational impact. Military districts and the supreme command are strategic entities that support operations.

6. Fronts are a wartime formation. Army groups are a peacetime designation for the same concept.

7. David M. Glantz, "The Nature of Soviet Operational Art," *Parameters* 15, no. 1 (Spring 1985), 2-12, https://ssi.armywarcollege.edu/pubs/Parameters/articles/1985/1985%20glantz.pdf.

8. I. D. Veprev and V. A. Smirnov, "Окружение" [Encirclement], *Советская Военная Энциклопедия* [Soviet Military Encyclopedia], vol. 6 (Moscow: Voyenizdat, 1978), 37-38.

9. Glantz, "The Nature of Soviet," 11.

10. Ministry of Defense of the Russian Federation, "манёвр огнём," *Воелнный Энциклопедический Словарь* [Military encyclopedic dictionary], vol. 2 (Moscow: Ripol Klassic, 2001), 27.

11. This changed when the Soviets developed an effective 152mm tactical nuclear round and most 152mm howitzers could then be used in this role.

12. Photo by Пользователь - 9 мая 2008, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=10907606.

13. A nomogram (also called a nomograph) alignment chart is a "graphical calculating device, a two-dimensional diagram designed to allow the approximate graphical computation of a mathematical function." Wikipedia, s.v. "Nomogram," last modified 13 July 2018, at 19:47, https://en.wikipedia.org/wiki/Nomogram.

14. As an example of a COFM approach, see "A Russian Approach to Interagency Cooperation," *OE Watch* 8, no. 4 (April 2018): 60, https://community.apan.org/wg/tradoc-g2/fmso/p/oe-watch-issues. The original article is Е.Г.Анисимов, В.Г. Анисимов, и И.В.Солохов, Проблемы Научно-методическово обеспечния межведомственного информацонного взаимодействия, Военная Мыцл, Но.12, Декабр 2017, 45-51. (Y.G. Anisimov, V.G. Anisimov, and E.V. Solohov, "The Issue of Providing for Scientific Methodological Interagency Information Cooperation," *Military Thought*, no.12 [December 2017], 45-51.)

15. Photo by Mil.ru, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=62469060.

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

Russian Force Structure for the Conduct of Large-Scale Combat Operations

by Major Charles K. Bartles

Introduction

The current discussion of Russian military activities is oriented either on strategic-level matters, such as nuclear weapons, information operations, and cyberspace warfare, or on tactical-level matters, such as battalion tactical groups, brigades, and divisions. What is rarely discussed is how Russia bridges strategy to tactics, which happens at the operational level of war.[1] Russia has a long history of studying operational art and with many great theorists. There are numerous studies of Russian operational art during World War II and the Cold War, but relatively little has been written on the topic since the collapse of the Soviet Union.

The mass warfare involving multiple echeloned armies and fronts that the Soviets anticipated during the Cold War will probably never occur. But this does not mean it is no longer necessary to study Russian operational art. It is unlikely that Russia intends to occupy any North Atlantic Treaty Organization (NATO) nation or desires a military confrontation with the United States or NATO; but the author believes there are plenty of opportunities for an unintended armed conflict that could escalate to the level of large-scale combat operations. The Russian Federation is not the Soviet Union, and it has a substantially smaller military than the Soviets. The army and front-level formations that Soviet operational planners war-gamed no longer exist, so understanding Russia's current force structure for the conduct of large-scale combat operations involves a discussion of its army groups, Joint Strategic Commands, the Russian General Staff, and other related topics.

Joint Strategic Commands

The Soviet system had 16 military districts, and each military district commander was responsible for garrisoning, training, rear-area logistical support, protection of strategically vital areas, and coordination of civil defense. These missions were the commander's primary concern and fulfilling them involved overseeing pre-conscription training, conducting the fall and spring conscription campaigns, operating military state farms, doling out pensions, etc. In wartime, the military district was responsible for conducting mass mobilization, including the preparation of units for combat, transportation of units to the front, logistical support, and replenishment. The military district commander was not responsible for the operational control of most units in his territory. In peacetime, this responsibility generally lay within the Branches of Arms (Ground Forces, Air Force, Navy, etc.). In 2010, Russia reformed its military district system. It did this by giving the military district commanders operational control of most military and Ministry of Defense (MoD) forces in their respective regions, with the exception of all nuclear and certain strategic assets, such as the Strategic Rocket Forces, Airborne Forces, and the Main Intelligence Directorate (i.e., *Главное Разведывателное Управление*, commonly known as GRU) Spetsnaz units. At this time, the Russians renamed the military districts "Joint Strategic Commands" (*Объединённое стратегическое командование* [OSK]), although they still use the term "military district" when referring to the organization if it is involved with more mundane rear-services activities, such as conscription.[2]

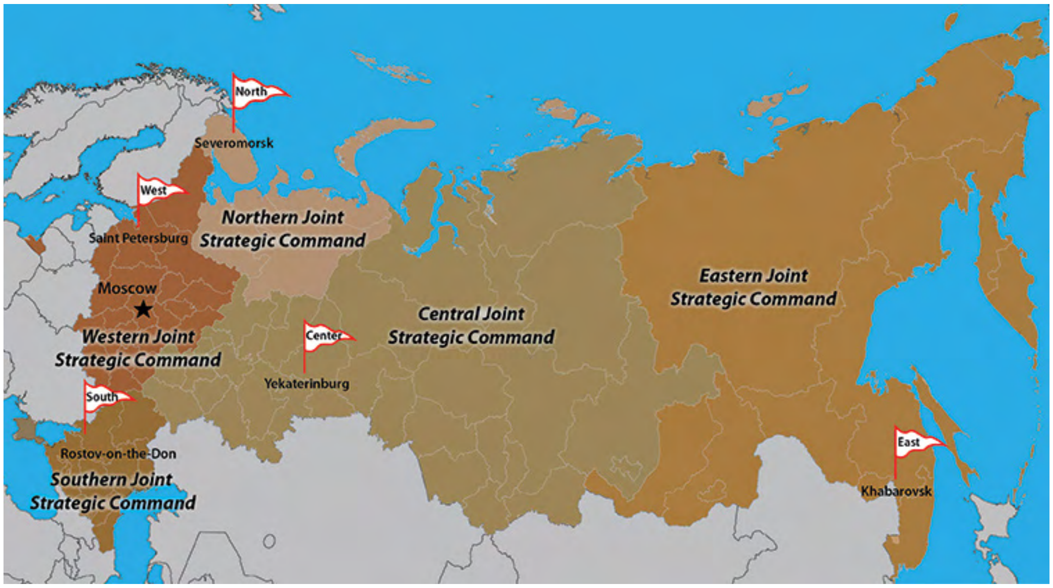

North
Severomorsk
West
Saint Petersburg
Northern Joint Strategic Command
Moscow
Western Joint Strategic Command
Center
Central Joint Strategic Command
Yekaterinburg
Eastern Joint Strategic Command
South
Rostov-on-the-Don
Southern Joint Strategic Command
East
Khabarovsk

Figure 1. Russian Joint Strategic Commands

The OSK is an operational-strategic level of command that bridges national-level strategy to the operational-level commands (army groups). A three-star general typically commands the OSK. The OSK commanders also control the naval fleets that are in their respective territories. This fact illustrates an interesting difference between the United States and Russia in terms of command and control. The naval fleet commander, a three-star admiral, reports to the OSK commander, a three-star general. A flag grade officer reporting to an officer of the same grade is relatively rare in the United States but not so in Russia. The Russian military is much less rank-conscious than the United States military; in the Russian system, positional authority, not rank, is paramount. This situation is important for two reasons. The first is that it reduces the need for high-ranking officers. Considering that the Russian military has no senior civilian leaders, and it has no four-star flag officers in the Navy, Aerospace Forces, Airborne Forces, or Strategic Rocket Forces, Russia's senior leadership is remarkably "lean" in comparison to its United States counterparts. In practice, this means there are numerous examples of one- and two-star Russian flag officers carrying out duties that United States three- and four-star flag officers typically perform. In terms of the Ground Forces, one-star generals command divisions, while two-star generals command army groups. The second important reason relates to the impact on joint and interministerial operations. Russians have no difficulty with attachment issues due to the ranks of different commanders. Occasionally, senior officers have even been subordinated to junior officers if deemed expedient or in the best interests of the State. Perhaps the most important takeaway in terms of planning is understanding that the Russian correlation of forces and means do not take into account the rank of a commander, only the capabilities at his command. U.S. planners should be careful not to assume a deterrence value simply because of a U.S. commander's rank or title.

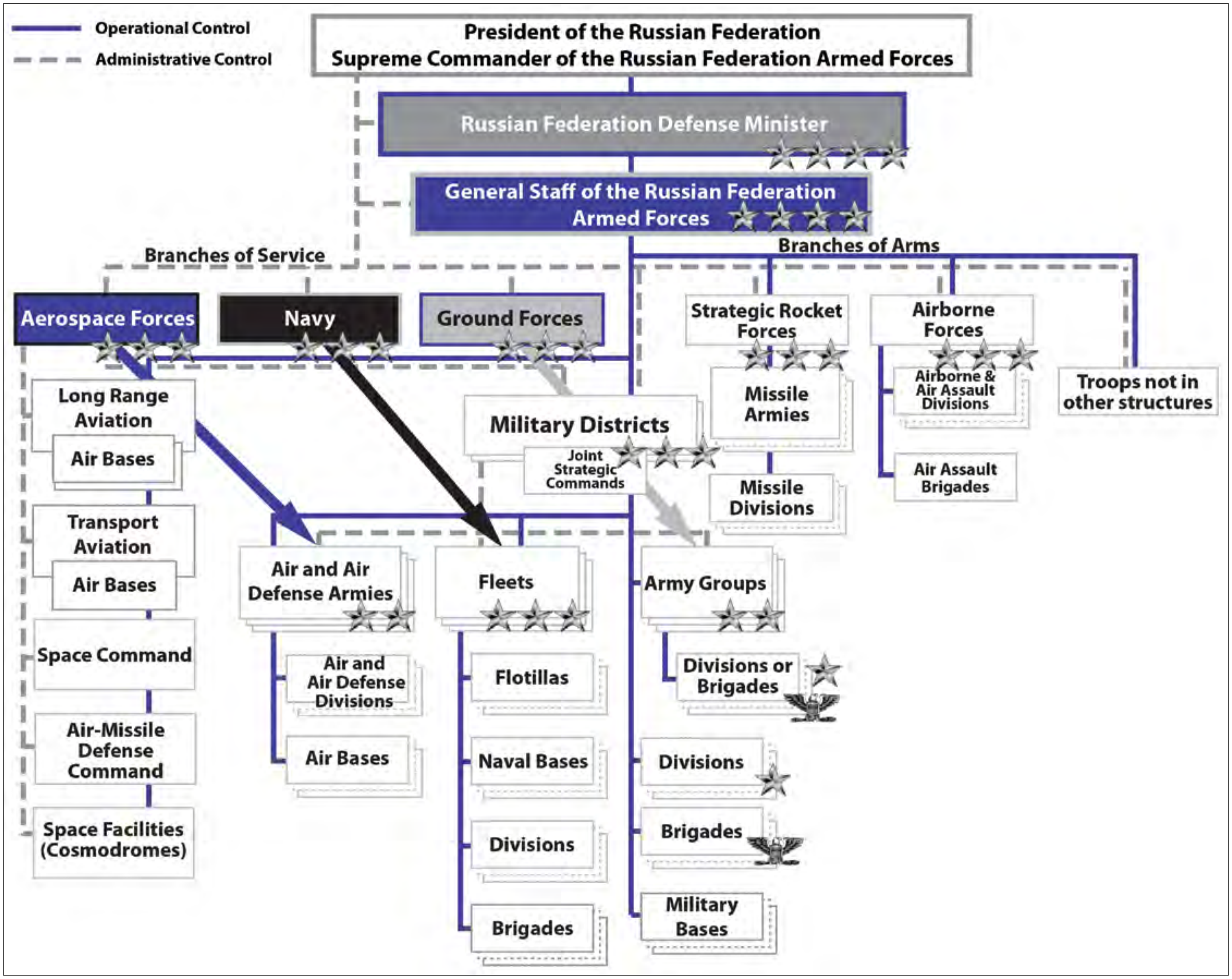


Figure 2. Relationship Between OSKs and Service Branches

The OSKs resemble the U.S. regional geographic combatant commands because they both provide a system for the command and control of joint forces. Similarities certainly exist, but so do some important differences. Perhaps the most obvious difference is the scope of operations. Russia's five OSKs do not encompass the globe as the United States system does because the scope of operations is much more limited, focusing solely on the Russian landmass, with a few exceptions regarding Russian assets abroad. Since OSKs are not externally oriented, they have no security cooperation mission or associated staff. Administratively, regular and General Staff officers man the OSKs, which have permanently embedded interagency liaisons. OSK Headquarters are significantly smaller than geographic combatant commands and are collocated with the OSK's Air and Air Defense Army. The Air and Air Defense Army controls most of the Aerospace Forces' aircraft and strategic air defense assets (e.g., S-300s, S-400s, and S-500s) in the OSK.

In terms of the command and control of forces, an important difference exists in maintaining operational control of forces. In a situation where the United States would form a single (large) joint task force to provide command and control of an operation in a given theater, Russia instead uses multiple, smaller army groups as needed. An additional difference is that an OSK has many tactical units that directly report to it and that it operationally controls (unlike geographic combatant commands). These units may be attached as a whole, or in part, to subordinate commanders where needed. Typical direct reporting units include logistic bases and units, Railroad Troop corps, electronic warfare brigades, pontoon-bridge brigades, heavy artillery brigades, multiple launch rocket system brigades, and theater-level command and control (signal) brigades.

These different command and control relationships that have resulted from Russia's restructuring of its military district system mean that the OSK commander is much more closely involved with the "fight" than his geographic combatant command counterpart. This situation is not surprising because it better situates the Armed Forces to deal with threats stemming from Russian perceptions on the nature of current and future war. Russians believe large-scale war will not just occur at certain flash points between two large opposing conventional armies; they believe it will occur throughout the tactical, operational, and strategic depths, possibly with special operations forces, cyberspace attacks, social media instigation, etc.

Army Group (Combined Arms Army or Tank Army)

The intermediate echelon of command between the OSKs and maneuver units (divisions and brigades) is the army group (a combined arms army or tank army).[3] In Russian parlance, the army group is generally considered an operational-level formation, which a two-star general usually commands.[4] Unlike Russian brigades and divisions, these army groups do not currently possess a uniform set of capabilities or assets. This area is undergoing change, with an effort toward developing a standard set of capabilities for each army group. In the future, it is likely each army group will have at least—

- ✦ Several motorized rifle and tank divisions and brigades.
- ✦ Headquarters, artillery, air defense, reconnaissance, missiles, and material technical support/logistics brigades.
- ✦ Engineer and nuclear, biological, and chemical regiments.

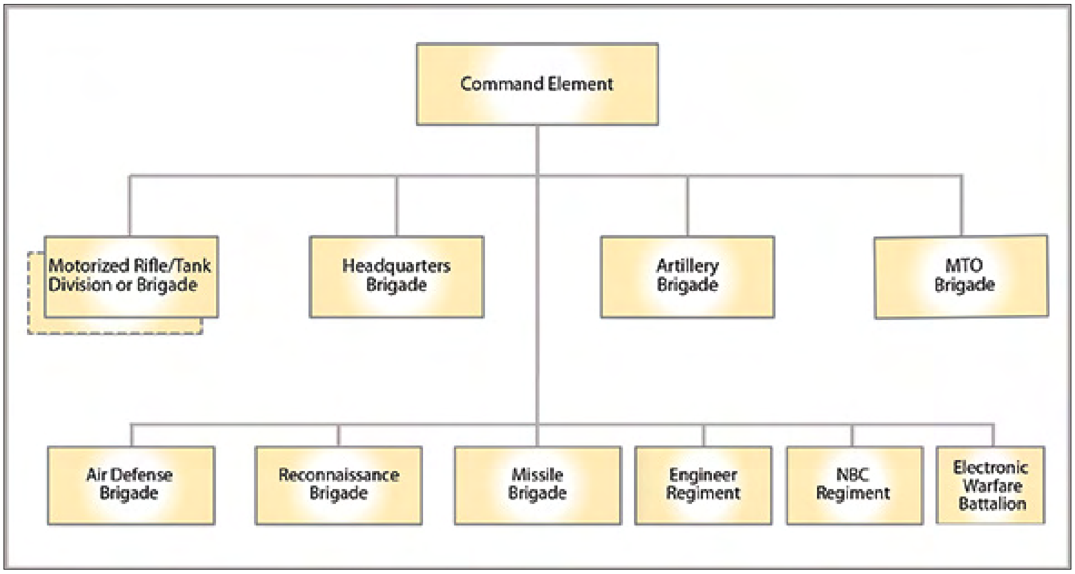


Figure 3. Proposed Army Group Structure

During operations, the army group detaches needed assets to support the various maneuver units. Perhaps the most important assets that the army group provides in this endeavor are the material technical support brigades, which feed, fuel, supply, and maintain the maneuver unit(s), and the artillery brigades, which regularly detach assets to support the formation of subordinate units' artillery groups, which will be further discussed.[5]

Typical Subordinate Units of an Army Group. The following are typical subordinate units, with notes about their equipment/role:

- **Motorized rifle/tank division or brigade (one or more):** Brigades do not report to divisions.
- **Headquarters brigade:** Signal (satellite, tropospheric/high frequency, and fiber-optic) and automated command and control systems.
- **Artillery brigade:** 2S4 Tyulpan 240mm self-propelled mortar, 2S7M Malka 203mm self-propelled howitzer, standard multiple launch rocket systems, howitzer, and antitank units.
- **Material technical support (logistics) brigade:** Motor transport, maintenance, pipeline, route security, bath and laundry, supply, fuel units.
- **Air defense brigade:** Buk-M2/Buk-M3 (SA-17 Grizzly) units.
- **Reconnaissance brigade:** Reconnaissance battalion(s), ground surveillance radar, acoustic, and signals intelligence units.
- **Missile brigade:** Iskander short-range ballistic missile/ground-launched cruise missile (SS-26 Stone/SSC-7).
- **Engineer regiment:** Standard horizontal engineering and possibly cover and concealment (maskirovka) units.
- **Nuclear, biological, and chemical regiment:** Nuclear, biological, and chemical reconnaissance and decontamination units, and thermobaric weapon (RPO Shmel/TOS-1A Solntsepyok) units.

Army groups are the next echelon above divisions and brigades and have a significant number of enablers; they are like a "corps" in terms of capabilities but have much less combat power than a U.S. Army corps. Administratively, army groups were gutted during the "new look" reforms that began in 2008 because the emphasis shifted to fielding permanently ready brigades. But recent Russian activities in Ukraine and Syria brought to light some command and control difficulties resulting from this policy, and army groups are now being more fully manned. Although the army group has logistic enablers, in high-intensity conflict situations the OSK would likely need to support or augment it.

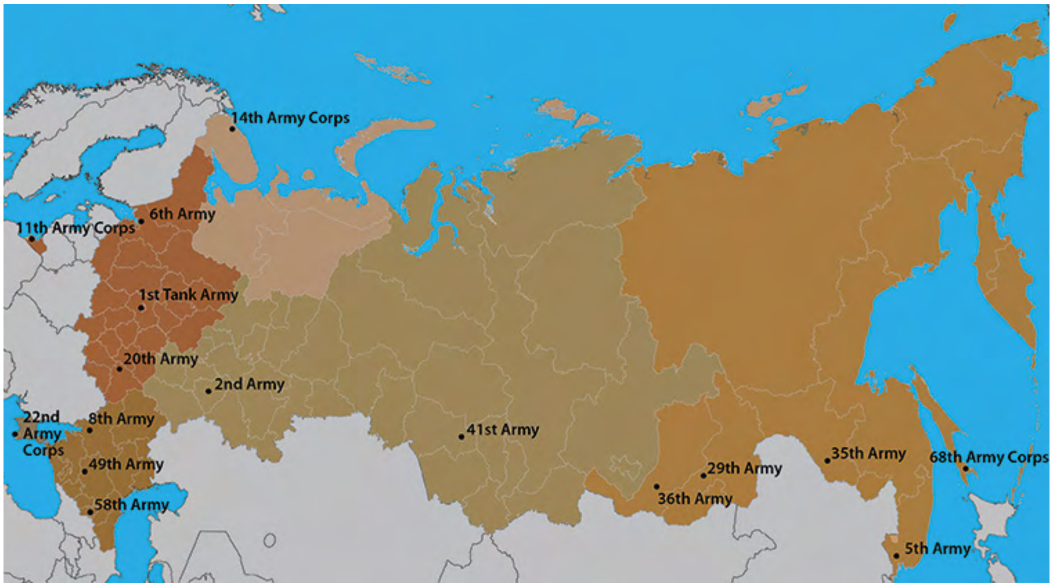


Figure 4. Russian Army Group Dispositions

Aside from providing command and control and "pushing" assets to subordinate units, the army group also functions as the basis of what might be considered a joint task force. Unlike in the United States, each branch of service (Army, Navy, etc.) is not capable of functioning as the basis of a joint task force. In the Russian system, joint capabilities are usually attached to the army groups. To facilitate this command and control, General Staff officers partially man the army group; and during combat operations, the army group usually receives a General Staff augmentation cell to support planning. Although representatives from the regional and local government and other ministries are not assigned to the army group, they likely would be attached if needed. The army group staff primarily concerns itself with conducting and sustaining lethal military action. Higher-level concerns, such as information operations and cyberspace warfare, are likely handled by the General Staff Headquarters or, more likely, at the national level.

Possible Army Group Attachments. The following are possible attachments, with notes about their corresponding equipment/support:

- Naval operational-level fires: Kalibr-NK (SS-N-27 Sizzler/SS-N-30A).
- Ground Forces operational-level fires: SSC-8.
- Coastal Defense Troops: Naval Infantry and Coastal Defense Artillery.
- Aerospace Forces: Army Aviation - helicopters/Su-25 and Frontal Aviation - Mig-29/Su-27, possibly air defense assets.
- Operational Strategic Command assets: multiple launch rocket system; nuclear, biological, and chemical; electronic warfare; and logistics.

- General Staff: GRU Spetsnaz, augmentation cell, and/or augmentees.
- MoD assets: Airborne Forces; assets from other OSKs; and strategic intelligence, surveillance, and reconnaissance.
- National Guard: Ministry of Internal Affairs-Internal Troops, Special Rapid Response Detachment, and Special Purpose Mobile Detachment.
- Federal Security Service: Border Troops.
- Regional/local government and ministry cells.

Army Corps

Russia also has army corps, which serve a similar function as a combined arms army or tank army. All army corps are currently oriented on coastal defense missions, and all except for one are assigned to, and collocated with, a naval fleet headquarters. The 22nd Army Corps (Sevastopol/Black Sea Fleet), the 11th Army Corps (Kaliningrad/Baltic Sea Fleet), and the 14th Army Corps (Severomorsk/Northern Sea Fleet) provide command and control of mostly Coastal Defense Troop units (Naval Infantry and Coastal Defense Artillery), and some motorized rifle and artillery units, which would otherwise be subordinated to the Ground Forces. Only the 68th Army Corps at Yuzhno-Sakhalinsk on Sakhalin Island in the Pacific Ocean is assigned to the Russian Ground Forces. A one-star general typically commands each army corps, and although they are considered a lower-echelon formation than an army group, there is no difference in functional capability between the formations and no appreciable difference in combat power. (Some army corps have more combat power than some combined arms armies.) Just as Russian maneuver brigades are not subordinate to divisions, no army corps is subordinate to a combined arms army or tank army.

How Russia Implements "Joint"

In the Russian system, the General Staff is responsible for operational- and strategic-level planning. Russia has a fairly nuanced view of the differences between the tactical, operational, and strategic levels of military science. The difference between these levels is based upon the mission scope, not simply the size of the unit. For example, a brigade fighting under an army group would be considered a tactical asset, but the same brigade fighting independently in a different situation could be considered a tactical-operational asset. The General Staff's operational planning duties typically involve the operational and operational-strategic level—or, in Russian parlance, "operational art." Proponency for strategic planning resides with the Russian Security Council, which is an interministerial body that is chaired by high-level officials, weighted heavily with the intelligence and security services. Although the Russian Security Council is the chief proponent of Russian strategy, the Chief of the General Staff does sit on the council, bridging operational art to the national security strategy.

Just as important as what the General Staff does is what the General Staff does not do. It does not have operational control of the force. Although there were Goldwater-Nichols–like reforms that removed operational control from the service chiefs (Ground Forces, Air Force, etc.) and placed the operational control of most forces with OSKs, little has changed with the General Staff's role as operational planners since Soviet times. The Chief of the General Staff does have day-to-day control of the GRU, a directorate of the General Staff, which in turn controls the GRU Spetsnaz brigades and several strategic assets. These include the Russian Airborne Forces, which function as a strategic reserve. In combat, however, the appropriate field commander, not the General Staff, would operationally control these warfighting assets.

Photo courtesy of Russia Ministry of Defense/Creative Commons

GRU Headquarters Moscow

The Russian General Staff system is based upon the Prussian-style general staff system and so has retained its personnel system. Unlike the U.S. military, officers do not rotate through "joint" assignments. In the Russian system, General Staff personnel exclusively handle "joint" matters, such as operational- and strategic-level planning and capabilities and doctrine development. Officers who serve in the prestigious General Staff are usually selected at the major or lieutenant colonel level (when they are in their late twenties or early thirties). They permanently replace their branch insignia with general staff insignia and become General

Staff personnel. Since the General Staff decides matters of military doctrine and procurement, it is considered essential that officers break their fixation with their branch of service (Ground Forces, Navy, Air Force, etc.) and branch of arms (infantry, armor, artillery, etc.) to avoid the "trade union mentality" that hinders military doctrine and procurement matters in Western armies.[6] Once selected for the General Staff, a Ground Forces officer will usually spend the remainder of his career doing staff work at the army group, OSK, and General Staff Headquarters in Moscow. (Officers in other branches of service will have slightly different assignments.) These officers are subject matter experts about the branches of service and specialties in which they have previously served and will be closely associated with these specialties, as planners, for the remainder of their careers (i.e., a signal officer in the General Staff will typically always work signal issues). Officers from maneuver (tank, motorized rifle, artillery, and missile) branches exclusively hold high-level positions of leadership within the General Staff (for example, Chief of the Main Operations Directorate), but an officer of the appropriate specialty will lead the specialty directorates, such as topography and electronic warfare.[7]

This system develops a caste of professional planners for handling operational-strategic matters, while freeing the remainder of the Russian Armed Forces officer corps to continue to specialize in their particular branch of service and arms at the tactical level. An obvious implication of this personnel system is that different career paths are available for officer advancement. Although selection for the General Staff is prestigious, it is not the desired path for all officers. Maneuver officers who enjoy command may best serve by not pursuing assignment to the General Staff. On this path, officers have a chance to hone their tactical skills because there is no need for service in joint or out-of-branch assignments. However, educational requirements still exist, such as attendance in a combined arms academy. Promotions typically happen much faster in the Russian military than in the United States military (it is not uncommon to see a 32-year-old battalion commander), and command tours have been known to last up to 6 years. In this system, a brigade commander (on the tactical path) would have more years of command experience than his U.S. counterpart because he has the ability to specialize in tactical leadership.[8]

It is important to understand that General Staff officers do not just work at the General Staff Headquarters in Moscow. These officers rotate between army group, OSK, and General Staff Headquarters assignments. Russia perceives this system to be advantageous because it allows officers to specialize as operational or tactical planners. Unlike Western officers, Russian officers do not need to divide their time between both of these challenging endeavors. (Since there are no out-of-branch assignments, for a Russian officer every assignment is a key developmental position.) Aside from the perceived advantages of different career tracking for operational and tactical planners, different career paths for tactical- and operational-level commanders also provide advantages in regard to tactical bias. In the U.S. Army, high-ranking maneuver commanders have similar career paths, ranging from platoon to corps commander, and most officers will follow the same path regardless of how far they advance up the ranks. This is not the case in the Russian Armed Forces because Russian officers destined for a high rank are selected early in their careers and trained differently. In the Russian view, the "truths" that commanders learn while commanding tactical units (platoons, companies, battalions, regiments, brigades, and divisions) can bias commanders when commanding operational-level units.[9]

Improving Mission Command Through Automated Command and Control

Russia has long been interested in developing an automated command and control system to enhance command and control of its Armed Forces and has already fielded several such systems at the tactical level. Automated command and control is a particularly good option for Russian commanders in tactical situations because of the somewhat "commander-centric" Russian military decision-making process. The decision process functions not by the commander's staff developing courses of action, but by the commander simply choosing a course of action early in the decision-making process and then making adjustments as necessary. Automated command and control systems facilitate this process by reducing the Russian decision-making cycle, so that the Russians' observe, orient, decide, and act loop is faster than that of potential adversaries. According to Russian military expert Viktor Murakhovskiy, a well-implemented automated command and control system can reduce the decision-making cycle by up to 2.5 times. Automated command and control systems are seen as essential elements of reconnaissance-strike loops because they facilitate rapid reconnaissance, planning, and, most importantly, action. Russia has recently begun fielding the Akatsiya-M automated command and control, an operational-level system that will be fielded in Russia's 12 army groups and 4 army corps. The system will not only provide command and control and situational awareness for the operational commander regarding his own directly subordinate units, but it will also allow for liaising with, or the command and control of, attached subordinate units of the Navy, Aerospace Forces, and Airborne Forces.

Reportedly, the Akatsiya-M will also integrate with the Russian National Defense Control Center in Moscow. The fielding of the Akatsiya-M is likely closely tied to a variety of new communications systems (satellite, tropospheric/high frequency, and fiber-optic) that have been or are now being fielded in army groups and army corps, as the Akatsiya-M likely requires a resilient communications backbone to operate.[10]

Organization of Fires and the Artillery Group System

The Russians do not have a concept of warfighting functions and therefore do not have a "fires" warfighting function.[11] In practice, this means there is no grouping of air defense artillery and artillery capabilities on the staff or into any type of "integrated fires command." The Russians would find grouping these capabilities odd because their associated sensors are quite different. Unlike the United States military, the Russians divide air defense duties between Grounds Forces (Army) and Aerospace Forces (Air Force). The Russian Ground Forces possess a robust air defense capability echeloned at the regiment, brigade, division, and army group levels; but in any large-scale combat operation, it can be expected that the Aerospace Forces' strategic air defense assets, such as the S-300, S-400, and S-500, would also be protecting the army group as needed.

Perhaps the most interesting aspect of how the Russians organize fires is how they conduct command and control of their artillery assets. In garrison, artillery assets are assigned to their respective units, as typically depicted in standard line-block charts; but when engaged in combat, Russian units typically form "artillery groups." Artillery groups can form at the army group through the regimental level and consist of the unit's organic artillery, in addition to attachments from higher-echelon units but minus detachments to lower-echelon units. Artillery groups are a doctrinally defended asset and are typically protected by air defense and electronic warfare assets. In terms of command and control, the unit's deputy commander for artillery or the senior artillery unit commander typically commands the artillery group. The OSKs possess tactical artillery assets (heavy multiple launch rocket system) but do not form an artillery group, so they pass assets directly to the army artillery group or to the division artillery group/brigade artillery group if no army artillery group was formed. As a rule, assets are usually only pushed down to the next lower level. Of particular note, the Iskander short-range ballistic

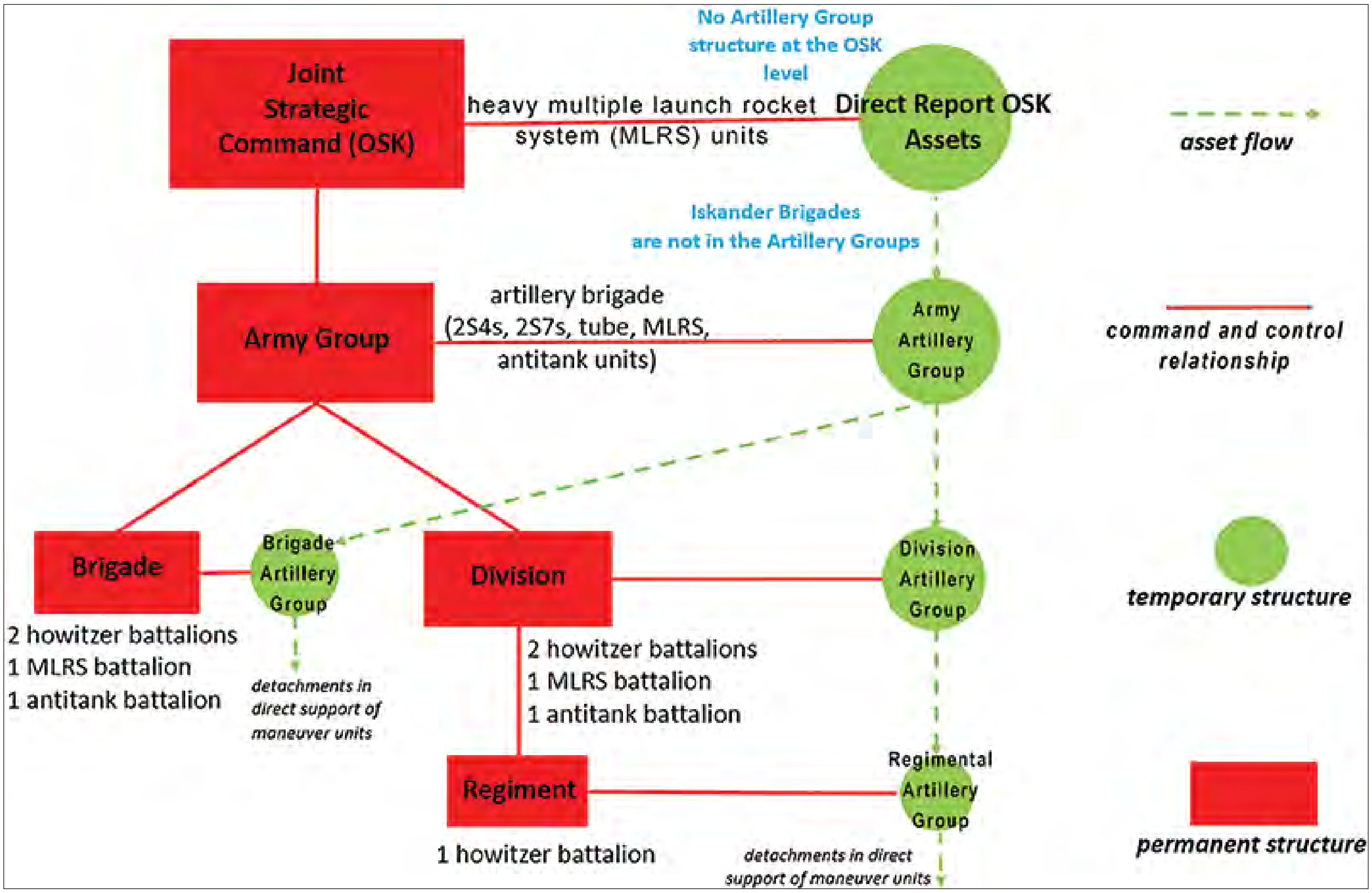

No Artillery Group structure at the OSK level
Joint Strategic Command (OSK)
heavy multiple launch rocket system (MLRS) units
Direct Report OSK Assets
asset flow
Iskander Brigades are not in the Artillery Groups
Army Group
artillery brigade (2S4s, 2S7s, tube, MLRS, antitank units)
Army Artillery Group
command and control relationship
Brigade
Brigade Artillery Group
Division
Division Artillery Group
temporary structure
2 howitzer battalions
1 MLRS battalion
1 antitank battalion
detachments in direct support of maneuver units
2 howitzer battalions
1 MLRS battalion
1 antitank battalion
Regiment
Regimental Artillery Group
permanent structure
1 howitzer battalion
detachments in direct support of maneuver units

Figure 5. The Artillery Group System

missiles/ground-launched cruise missiles (SS-26 Stone/SSC-7) are not part of the artillery groups. These high-value assets are likely considered a special reserve asset for the army group commander and are therefore not put under the command of the artillery group. In addition, the range of the Iskander (500 kilometers) allows it to remain much farther in the rear, so it does not need to be physically located with the other artillery assets, which puts it at less risk of an enemy strike. At the brigade and regimental level, detached assets are under the direct control of motorized rifle and tank battalion commanders in direct support of their missions. The artillery group system is essential for understanding Russian tactical- and operational-level fires because it explains the subordination of these assets.

Cross-Domain Fires

Although cross-domain fires is a new concept in the United States, it has long been the practice in the Russian Armed Forces. The notably land-centric Russian General Staff has much experience furthering efforts for cross-domain fires in terms of air, land, and sea. For example, most new Russian antitank guided missiles (including barrel-launched) have a limited capability to hit low- and slow-flying aircraft; the coastal defense missiles can strike targets on land; the Iskander short-range ballistic missiles/ground-launched cruise missiles have warheads with seekers that can target ships; and the short-range air defense systems (Buk-M3) can hit targets on land. Small automated turrets (Arbalet-DM) are being fielded; they are designed for intelligence, surveillance, and reconnaissance and engaging ground targets but are also able to destroy small unmanned aerial vehicles. Future strategic air defense systems (S-500/A-235 Nudol) can destroy low-earth orbit satellites. The development of secondary (sometimes marginal) capabilities for weapon systems may appear to be inefficient (poor use of resources), but Russia views these limited secondary capabilities as essential for maintaining resiliency.

In terms of command and control, Russia's reconnaissance fire system is implementing cross-domain fires through the Strelets reconnaissance, command and control, and communications system. If the Strelets system proves successful, the Russian Armed Forces will need only one system to task fires rapidly at all levels of battle, from front-line artillery to deep-strike aviation, through rear-area missile strikes. This would include ground-based tube artillery and rocket artillery, ballistic and cruise missile, strike aviation, and ship and coastal naval fires. The end state would result in the fielding of a truly unified reconnaissance fire system that facilitates cross-domain fires at both the tactical and operational depths.[12]

Likely Interministerial Support

Russia's Soviet legacy made stove-piped militarized intelligence and security agencies the norm, as the Soviets were leery of investing all military power in a single organization or ministry because of fears of a coup. Since the Russian civilian leadership now has few concerns about its ability to control these militarized security and intelligence services, the Russian Federation has been trending toward the consolidation of these organizations' powers to reduce bureaucracy and redundancies.[13] In 2016, the Russian Federation established the National Guard of the Russian Federation *(Rosgvardiya).* It is unlike the U.S. National Guard because these well-trained troops are on Active Duty, with an internal security focus, performing such duties as dealing with riots and domestic unrest. Rosgvardiya controls most of Russia's internally oriented militarized intelligence and security services, including the—

- Ministry of Internal Affairs-Internal Troops.
- Special Rapid Response Detachment.
- Special Purpose Mobile Detachment.
- Ministry of Internal Affairs-Prompt Response and Aviation Forces' Special Purpose Center.
- Aviation subunits.

Estimates of the total uniformed personnel controlled vary between 200,000 and 300,000.[14] Russia's militarized intelligence and security services are now mostly consolidated under three main government bodies—the MoD, Federal Security Service, and Rosgvardiya—instead of being spread throughout a myriad of ministries, services, and agencies.

Russia's dispersal of military power is important for two reasons. The first is that Western calculations of Russian military power rarely account for Russia's military forces that are not in the MoD. These forces are often highly trained and equipped with heavy weapons, armored personnel carriers, artillery, and mortars. Although these forces are significantly lighter than their MoD counterparts, they are more than sufficiently equipped to handle light forces such as insurgents, airborne troops, and special operations units. Not only do these forces provide significant numbers of combat-capable personnel, but they also free the heavier MoD forces from the manpower-intensive duties of rear-area security and counterinsurgency operations, duties that Western planners anticipate will be executed by MoD troops. The net effect could cause an underestimation of Russian combat power. In past conflicts, Russia has subordinated its militarized security intelligence and security forces to the MoD in varying degrees. Some of these forces will likely be attached to the OSK and army group during large-scale combat operations, while the remainder will operate under their existing control structures. Although not as well suited for deployment as MoD units, some of these forces may be drawn from other regions to defend a threatened axis. Any assessment of Russian combat power that does not account for other militarized security services is incomplete at best.

Reserve System

Although reservists have been little, if at all, used in Ukraine and Syria, reservists would be an important factor if Russia engaged in large-scale combat operations. The Russian MoD has been tinkering with wide-scale reforms of the military reserve system for several years, with varying degrees of success. The current Reserve system is inherited from the Soviet Union and is designed to support a doctrine that requires maintaining a large Strategic Reserve of troops that can mobilize in the event of large-scale combat operations. It comprises conscripts and officers who completed their mandatory service obligation and received discharge from active service, with rare and infrequent call-ups to test mobilization capabilities. There has been some debate about whether Russia needs to maintain a large Strategic Reserve or should switch to a more Operational Reserve. Opinions vary between two major camps. The reformers say an Operational Reserve would do far more to enhance security because an Operational Reserve would be smaller, better trained, more able to quickly become combat ready in a national emergency, and more likely to be called in an emergency. The older retired senior officers believe Russia should at all costs maintain the capability to mass mobilize. Debate on this issue appears to be somewhat settled, as Russia is increasing both capabilities.

The large Strategic Reserve will be developed by maintaining the universal conscription system and increasing the size and scope of the Volunteer Society for Cooperation with the Army, Aviation, and Navy programs that provide military training and militarily useful skills to Russian youth. In conjunction, the Russian Armed Forces are attempting to develop an Operational Reserve along two different models. The first model is reminiscent of the U.S. style of an Operational Reserve, with Reserves reporting for duty and serving alongside active service members or serving in Reserve units that support the Active Component. This system consists of an Active Reserve Component conducting annual training requirements, receiving monthly stipends, and being voluntary. The intent is to maintain a cadre of officers and enlisted soldiers who regularly train at a mobilization center or with particular active units; and in the event of mobilization, the reservist would be called to duty to provide support or backfill as needed.[15] The second model involves the use of reservists in stand-alone units called "territorial-defense units." (Russia experimented with these in the Vostok-2014 military exercise.) Territorial defense units have appeared elsewhere in Eastern Europe and usually consist of relatively lightly armed infantry soldiers assigned to secure critical infrastructure in the rear. These forces are not intended to serve in high-intensity combat operations or abroad. The intent of this form of Operational Reserve is to unburden the Active Duty force of mundane rear-area security duties, allowing the Active Duty force greater freedom of movement to conduct combat.[16] Due to the relative sizes and economic differences between Russia and NATO, time required to build up United States combat power on the European landmass, and Russian correlation of forces and means calculations, it is likely that a successful outcome for Russia in any large-scale combat operations against NATO would be measured in days and weeks, instead of months and years. Russia would try to bring about a conclusion of operations, under favorable terms, before the United States/NATO fully brought combat power to the fight. Therefore, Russia's Operational Reserve might mobilize, but the Strategic Reserve would likely not be a factor in most situations. The Reserves' contribution to a large-scale combat operation is difficult to ascertain at best because the institution is still under development.

Conclusion

The U.S. force structure for the conduct of large-scale operations is much the same as it was during the Cold War. The United States still uses theater armies and field armies, albeit with ongoing modifications to their structures, but this is not so for the Russians. The Russians have chosen to abandon their fronts and armies and to adopt different structures that they believe will be more capable of facing current and future threats in the operational environment. In order to understand how Russia will conduct large-scale combat operations, one must now understand army groups, OSKs, and the Russian General Staff. Much as the laws of physics appear to change at the macro and micro levels, the "truths" of mission command may differ from the tactical to operational level. For example, the

Wehrmacht of Nazi Germany generally had far better tactics than Soviet forces (especially at the beginning of the war), but the Soviets did not defeat Nazi Germany because of better tactics. The Soviets defeated the Nazis because of better operational art. Rough comparisons can be made between Nazi Germany and the Soviet Union, and the United States/NATO and Russian Federation if engaged in conflict today. The United States military prides itself on tactical proficiency, but success against the Russian military during large-scale combat operations will require not only an understanding of Russian tactics but also a knowledge of Russian operational art. This is because a successful Russian outcome against the United States/NATO in armed conflict will likely be due to the acumen of Russian operational planners as much as the tactical proficiency and tenacity of Russian commanders in the field.

Endnotes

1. An "operation" is the highest form of the application of the Ground Forces' combat power in local wars and armed conflicts. The operation is a combination of coordinated and interrelated missions to fulfill a particular objective in furtherance of strategic, operational, or operational-tactical tasks in a certain area within a specified period. Sergey Batyushkin, *Preparation and Conduct of Military Actions in Local Wars and Armed Conflicts* (Moscow: KnoRus, 2017), 17.

2. Christopher Donnelly, *Red Banner: The Soviet Military System in Peace and War* (Coulsdon, Surrey, UK: Jane's Information Group, 1988), 149-151.

3. The author has been unable to find much recent information about the term "army group" and its exact relation to combined arms armies, tank armies, and army corps. Older definitions make it clear that this was an ad hoc formation, but more recent use of the term implies it is equivocal to the before-mentioned ground-based operational-level commands. For the purposes of this article and clarity, the term "army group" is defined as a ground-based operational-level command (combined arms army, tank army, or army corps) that functions as an intermediate command between a Joint Strategic Command (OSK) or naval fleet, and tactical divisions and brigades.

4. Aleksey Nikolskiy, "Moscow Moves Staffers Up to the Front Line," *Vedomosti* Online, 12 May 2016, http://www.vedomosti.ru/politics/articles/2016/05/12/640715-shtabistov-peredovuyu. The Soviets developed the army group system during World War II, when the echelons of corps and armies were merged.

5. "Every Combined Arms Army Will Receive an Engineering Assault Brigade by 2020," *TASS* Online, 2 December 2015, http://tass.ru/armiya-i-opk/2492454.

6. Although this system does alleviate many resource allocation problems within the Ministry of Defense (MoD), significant battles for economic resources still exist with which the MoD must contend. Because of its Soviet heritage, Russia has powerful militarized intelligence and security services (National Guard, Federal Security Service, Border Troops, etc.) that directly compete with the MoD for resources. This resource competition is especially acute now because Russia no longer believes that the primary threat to its sovereignty stems from overt military invasion, but instead from social movements in the flavor of the "color revolutions," the Arab Spring, and the Maidan movement. This perception of threat could increasingly divert certain funds away from the MoD to militarized security forces with more of a dedicated internal security mission.

7. Donnelly, *Red Banner*, 139-145.

8. The preceding four paragraphs are from Lester Grau and Charles K. Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), 10-12.

9. Georgii Samoilovich Isserson, *The Evolution of Operational Art*, trans. Bruce W. Menning (Fort Leavenworth, KS: Combat Studies Institute Press, U.S. Army Combined Arms Center, 2013), x-xii.

10. Aleksey Ramm and Aleksandr Kruglov, "The Defense Ministry Will Deploy Akatsiya for 21 Billion: Combined-Arms Armies Will Transfer to Automated Command and Control in Real Time," *Izvestiya* Online, 5 July 2018, https://iz.ru/761052/aleksei-ramm-aleksandr-kruglov/minoborony-razvernet-akatciiu-za-21-mlrd.

11. Charles K. Bartles, "Recommendations for Intelligence Staffs Concerning Russian New Generation Warfare," *Military Intelligence Professional Bulletin* 43, no. 4 (October-December 2017): 10-17.

12. Lester W. Grau and Charles K. Bartles, *The Russian Reconnaissance Fire Complex Comes of Age* (Oxford, UK: Changing Character of War Centre, Pembroke College, University of Oxford, May 2018), http://www.ccw.ox.ac.uk/s/The-Russian-Reconnaissance-Fire-Complex-Comes-of-Age-lz7p.pdf.

13. Charles K. Bartles, "Getting Gerasimov Right," *Military Review* 96, no. 1 (January-February 2016): 30-38.

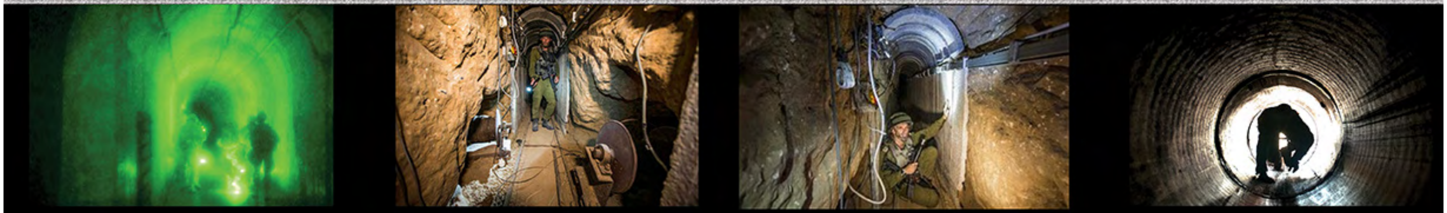
14. Aleksandr Igorev, "A Place in the Formation Has Been Designated for the Russian Guard: The President Has Defined the Missions of the New Service," *Kommersant* Online, 11 April 2016, http://www.kommersant.ru/doc/2961750.

15. Bogdan Stepovoy, Aleksey Ramm, and Yevgeniy Andreyev, "In the Reserve, on Contract," *Izvestiya* Online, 13 February 2018, //iz.ru/706732/bogdan-stepovoi-aleksei-ramm-evgenii-andreev/v-rezerv-po-kontraktu; and Vladimir Pasyakin, "Reservists: on the Line," *Flag Rodiny* Online, 13 September 2016, http://sc.mil.ru/files/morf/military/archive/FR_2016-09-12.pdf.

16. "Four Territorial Defense Subunits Manned by Reservists Taking Part in Kavkaz-2016 in the Southern Military District," *Ministry of Defense of the Russian Federation* Online, 6 September 2016, http://function.mil.ru/news_page/country/more.htm?id=12094815@egNews.

MAJ Chuck Bartles is an imagery officer and space operations officer assigned to the 76th Division (OR) and commands the U.S. Strategic Command Army Reserve Element in Colorado Springs, CO. As a civilian, he works as a Russian analyst at the Foreign Military Studies Office, Fort Leavenworth, KS.

Analyzing an Underground Facility for Large-Scale Combat Operations



by Captain Nicholas G. Pena

Introduction

When learning about underground facilities, the intelligence professional might ask, "How are we supposed to provide a maneuver commander with accurate and timely threat assessments of an underground facility during large-scale combat operations?" Then there is the logical follow-on question: "And how is that intelligence professional expected to provide the same information about any one of an estimated 4,800 underground facilities with little or no intelligence?"

This article shares the lessons learned from my intelligence section during a deployment to the Republic of Korea on a regionally aligned forces mission. While deployed, we conducted intelligence preparation of the battlefield and the military decision-making process for countering weapons of mass destruction during subterranean operations. We had to learn a new set of skills and study a new field of information not presented to us previously. Ultimately, we learned that the subterranean environment is unique and that acquiring a basic understanding of its uniqueness will allow intelligence professionals to add valuable information to the decision-making process and increase the survivability of our Soldiers.

Background

The United Nations predicts that by 2030, urban areas are projected to house 60 per cent of people globally and one in every three people will live in cities with at least half a million inhabitants.[1] This prediction is one of many that have refocused U.S. Army efforts to lay the groundwork for future operations in densely populated urban areas. This multi-domain ground conflict will include surface, vertical urban, and subterranean realms. The subterranean domain will encompass underground facilities, building substructures (basements and parking garages), civil works (subways, transportation tunnels, and sewers), and their supporting infrastructure systems. Like military and government underground facilities, substructures and civil works provide similar challenges to the intelligence professional, but in a larger volume.

A perfect scenario would allow the intelligence team to collect city works blueprints, diagrams, or maps of these subterranean structures to use during the planning phase. More than likely, this information will not be available, and the intelligence team must use any imagery and open-source information it can obtain to answer the intelligence gaps. In the urban environment, the unknown terrain features will always outweigh the known. An example of this is the Iraqi campaign to retake Mosul from the Islamic State of Iraq and Syria (ISIS) fighters in 2017. It became apparent that ISIS was using a network of tunnels to move undetected throughout the city, but it was not until Iraqi forces began clearance operations that they discovered entire city blocks were connected by passages created in the building walls. This discovery enabled the development of tactics, techniques, and procedures that forces used for the remainder of the operation.

When conducting operations inside urban areas and megacities, the team must identify the cultural construction norms to assist in planning. Terrain and cultural practices will drive construction characteristics for housing, subway systems, and underground civil works, and will establish a planning base. The team can then verify the assumptions developed during planning or can discard them as the operation develops. Understanding the terrain inside a megacity is challenging, and the subterranean domain is only a portion of this vast environment.

Understanding an Underground Facility's Purpose

Underground facilities are not a new addition to the modern battlefield. Soldiers and civilians have used tunnels and underground terrain before—in World Wars I and II, the Korean War, the Vietnam War, and the War on Terrorism. Technological advances have expanded the complexities of these underground facilities, thus creating a more challenging environment for friendly operations. To resolve this problem, the intelligence professional cannot always wait for the different intelligence entities to answer information requirements and fill intelligence gaps. The intelligence professional must draw conclusions with limited information and deduce what makes sense in order to assist the unit's operations process. To fulfill the intelligence warfighting requirements for subterranean operations, it is important to understand the purpose of the underground facility, assess the environment that friendly forces will encounter inside the facility, and effectively map the facility for current and follow-on operations. These tools do not only relate to the Korean theater of operations; the underground facility remains a point of contention in Army studies and refinement efforts in identifying the best approach to the multi-domain megacity challenge.

Understanding an underground facility's purpose is the largest piece of the puzzle, and it will provide the most relevant information to the ground force commander. ATP 3-21.51, *Subterranean Operations*, describes this environment and its characteristics. To understand the subterranean world, analysts first need to comprehend the surface terrain features and their significance to the associated underground facility. Dynamic pieces of the puzzle include roadways, areas cleared of vegetation, footpaths, power lines, ventilation shafts, sewer pipes, portal locations, and civilian infrastructure. If roadways are present leading into the underground facility, then the corridors inside will be wider than facilities with a footpath entrance, reducing the risk of overpressure[2] injuries and increasing maneuverability.

Assessing the Underground Facility and Creating the Visual Product

Depicting the known location of portals[3] on a topographic map creates a relative size comparison for the facility, which can assist in determining its maximum occupant capacity and relationship to one another. The locations of these portals also assist in determining if the underground facility is multilevel based on differences in elevation. The facilities' umbilicals[4] will also be identifiable on the surface level. Underground facilities of greater importance will be more sophisticated and will contain internal and external life-support systems. Evaluating these systems will aid in determining the amount of time a facility is able to remain closed off from the outside environment. Selectively removing any of these critical systems provides courses of action to the ground force commander for offensive approaches to deprive the threat and improve the probability for a successful tactical callout.

The type and level of a facility can be determined using these tools and readily available intelligence such as basic imagery. Hardened artillery sites, weapons depots, battle positions, continuity of operations bunkers, and factories are just a few types that are of a different construction, with a variety of defensive measures and barrier levels. Different barrier levels require different breaching assets and time allocations for a successful breach to occur.

After assessing an underground facility's purpose, create a visual product showing the assessed underground facility's layout. This product will become the tool for the ground force commander to plan all aspects of the surface and subterranean operation; therefore, it needs to be comprehensive. The product should depict portal locations and type, internal barrier classification[5] and evaluated breach times, internal wall construction, types of rooms located inside (aid station, command post, munition storage, etc.), defensive measures, and ultimately the threat's composition and disposition. The visual product's level of detail

Photo by SSG Michael Armstrong, 2SBCT, 2ID

Soldiers of 2nd Stryker Brigade Combat Team, 2nd Infantry Division, provide security during an exercise focused on subterranean operations, 17 May 2018.

is time-dependent and can be digital, analog, or a combination of both. The best method to create this product is to begin with a blank piece of acetate laid onto a topographic map encompassing the underground facility's location.

To start, identify and mark the known portal locations to identify the size of the underground facility and its internal network. The ventilation shaft, observation posts, or other umbilicals will aid in the layout because their ties to the underground facility are more than likely associated with underground corridors or rooms. After depicting all the known information, remove the sketch from the map and fill in the remaining information gaps. Accomplish this by deducing what makes sense based on what is known and by using a practical approach to annotate the unknowns. An example is assuming that the command post is closer to the center of the underground facility, not close to the portals where it is more vulnerable. After all of the knowns and unknowns are illustrated, an analyst has a working product to refine and expand on. This is a critical process and is the base for all other warfighting functions and commanders to plan operations.

Photo by SSG Michael Armstrong, 2SBCT, 2ID

Soldiers of 2nd Stryker Brigade Combat Team, 2nd Infantry Division, prepare to clear a corridor during an exercise focused on subterranean operations, 17 May 2018.

A Toxic Environment

The environment inside an underground facility is more lethal to our forces than the threat forces themselves. Add the potential for weapons of mass destruction, and it becomes the deadliest environment a Soldier will encounter. The air, lighting, structural integrity, overpressure risk, sound amplification, and threat forces play a role in this lethal environment and are all equally important to consider. Oxygen levels, explosive gasses from firearms, smoke, carbon monoxide, carbon dioxide, and chemical and biological agents will at a minimum reduce the stamina and effectiveness of our forces and have the potential to be fatal. That is operating on the assumption that a sufficient oxygen ratio is present inside the underground facility to begin with and the use of oxygen tanks is not required. Chemical detectors and air quality sensors are the most effective way to detect these threats once inside, but the intelligence analysts must provide planning assessments prior to entry.

The threat and civilian protective measures displayed on the objective before arrival is a starting point to determine the environment of an underground facility; however, forces should take into account that less-developed countries may have different safety standards and regulations. At a minimum, though, forces that approach an assessed weapons of mass destruction site must wear mission-oriented protective posture (MOPP) level four gear, with the appropriate detectors. When approaching a non-weapons of mass destruction site, forces should apply a deliberate tempo to avoid passing the point of no return before any symptoms take effect. The intelligence section owes the ground force commander an assessment of when to transition friendly forces into MOPP gear when countering weapons of mass destruction operations. Only when the environment demands it should Soldiers wear MOPP gear because it affects Soldiers' combat effectiveness by reducing their stamina and overall situational awareness. The chemical officer's knowledge of the chemical, biological, radiological, and nuclear agents assessed to be on the objective will assist the intelligence section in determining the various MOPP gear transition points and protection level upgrades for friendly forces as they approach the underground facility.

U.S. forces own the night, but not the dark. Night vision devices rely on ambient lighting to enhance images for the operator to see. Inside an underground facility, lighting systems may turn off at a moment's notice; before gaining entrance, operators need to plan how they will produce ambient lighting with infrared lasers, chemical lights, or visible lights, or use thermal imaging devices. A ground force commander may decide to use the lack of lighting as an offensive measure if access to the power supply system is ready and if the team has assessed the threat to lack night vision capability.

Structural Integrity and Overpressure

Finally, it is critical to understand the structural integrity of the underground facility and overpressure potential. The structural integrity of the floors, walls, and ceiling directly corresponds to the level of facility assessment and correlates to the classification level of the portal barriers and overall facility importance. Higher barrier classification levels present at the portals indicate a more important facility, resulting in finished and reinforced walls and ceilings in most instances. The internal construction methods affect overpressure and the efficiency with which it channels through space. The stronger the walls and ceiling within the underground facility, the more damage it can withstand from small arms and explosives, such as grenades, but this will also increase the ricochet effects of rounds and shrapnel, and will channel overpressure more directly.

Photo by SSG Michael Armstrong, 2SBCT, 2ID

Soldiers of 2nd Stryker Brigade Combat Team, 2nd Infantry Division, prepare to clear a corridor during an exercise focused on subterranean operations, 17 May 2018.

Because a shockwave over atmospheric pressure causes overpressure, it can be lethal to humans and can result in severe disorientation similar to the effects of alcohol intoxication. Smaller spaces, larger explosions, and proximity to overpressure-producing sources will increase the effects of overpressure. This requires analysis so that the ground force commander can determine weapon employment and direct fire control measures inside the underground facility.

Mapping the Underground Facility

Multiple levels, corridors, portals, rooms, and dead space result in an interweaving maze that could continue for kilometers with no end in sight. The templated layout derived from the overall purpose of the underground facility and environmental characteristics will only provide a limited understanding and is primarily a planning tool. When the entry and clearance operation begins, it is imperative that a designated element be responsible for mapping the underground facility, and the element must consistently provide updates to the tactical operations center. Human intelligence reports from civilians or enemy prisoners of war near the objective can be helpful to refine the understanding of the facility. If not, refinement will only commence after ground forces or robots gain entrance to the underground facility. Refinement will remain an ongoing process that is critical to the overall success until the operation is complete.

The best approach to mapping the underground facility is to display the templated layout next to a clean piece of acetate or on a whiteboard visible to all personnel inside the operations center. Having both products side by side will provide a visual product to battle track with, create a common operational picture, and refine the underground facility's layout simultaneously. Using one of these methods, begin mapping from the point of entry and continue based on reports from the clearing unit as the operation unfolds. The blank slate approach allows for easy modification of the templated layout. Human intelligence and lead unit reporting can improve the layout, which can also depict significant activities in time and space. If possible, the clearing team should constantly be searching the underground facility for diagrams or writing on walls to assist with the mapping process.

Ultimately, friendly forces will clear the underground facility and subsequently begin exploitation. The exploitation phase is when final mapping refinement is completed. Techniques include using a paceman or measuring wheel for distance and protractors or rudimentary angles for azimuth (because the underground environment may affect compass accuracy). If available, three-dimensional mapping cameras are useful to create a digital rendering of the facility. This is especially helpful for planning purposes if a higher unit's exploitation team is required at the objective, such as the chemical response team or nuclear response team.

Conclusion

The underground facility is the worst imaginable environment in which friendly forces will conduct operations. The unknown facts surrounding underground facilities outweigh the known facts tenfold. Intelligence professionals owe the ground force commander accurate assessments of underground facilities even when intelligence is limited. Using only surface-level information collection products, an analyst is more than capable of assessing an underground facility's purpose. The analyst can provide information about the underground facility's environment and can produce accurate mapping updates of the underground facility throughout the operation and until completion of the exploitation phase. Most importantly, the intelligence analyst must provide recommendations to the ground force commander that allow the commander to identify, assume, and mitigate risks when planning and executing the clearance operation inside the underground facility. As intelligence professionals, we cannot fear assessing the unknown; we must do what we can for friendly forces to conduct successful operations within an underground facility.

Photo by SSG Michael Armstrong, 2SBCT, 2ID

Soldiers of 2nd Stryker Brigade Combat Team, 2nd Infantry Division, provide security during an exercise focused on subterranean operations, 17 May 2018.

The use of subterranean facilities will remain an affordable and effective means to defeat high tech information collection assets in the future. If the intelligence team focuses on each aspect of the subterranean environment, refines assumptions throughout the operation, and studies the cultural construction norms, the team can answer megacity intelligence gaps for the ground force commander.

Endnotes

1. United Nations, Department of Economic and Social Affairs, Population Division, *The World's Cities in 2016* (2016), ii, http://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf.

2. *Overpressure* is the "pressure caused by a shock wave over and above atmospheric pressure." Department of the Army, Army Techniques Publication 3-21.51, *Subterranean Operations* (Washington, DC: U.S. Government Publishing Office, 21 February 2018), 3-30 (common access card login required).

3. A *portal* is the "structure surrounding the immediate entrance to a mine; the mouth of a cave or tunnel." Ibid., 1-15.

4. *Umbilicals* are the "supporting Infrastructure that allows a system to function." Ibid.

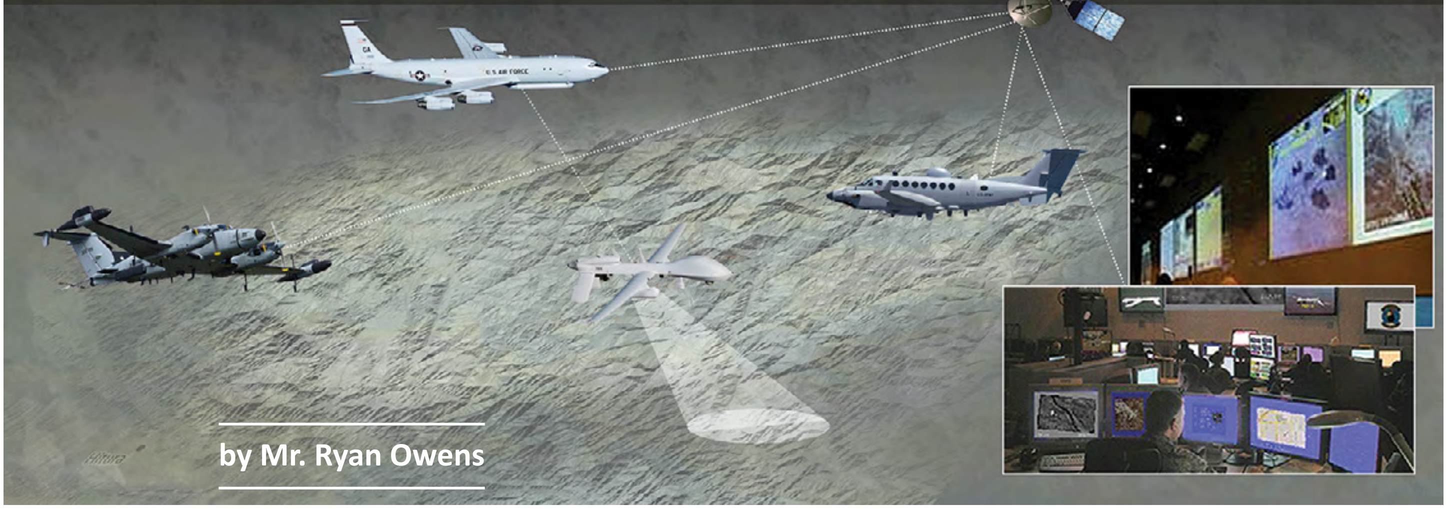
5. There are three barrier classification levels. "The classification of barriers is used to quickly identify and describe the materials used to build portals and entrances to subterranean spaces and structure." Ibid., 1-17.

CPT Nicholas Pena commissioned into the U.S. Army as an infantry officer from the University of Central Florida Reserve Officers Training Corps program in 2012, graduating with a bachelor's degree in business management. He served as an infantry platoon leader and executive officer in the 2nd Battalion, 502nd Infantry Regiment, 2nd Brigade Combat Team, 101st Airborne Division, from 2012 to 2017 and deployed to Afghanistan in support of Operation Enduring Freedom. After attending the Military Intelligence Officer Transition Course and Military Intelligence Captains Career Course at Fort Huachuca, AZ, CPT Pena was assigned to the 2nd Battalion, 7th Infantry Regiment, 1st Armored Brigade Combat Team, 3rd Infantry Division, as a battalion intelligence officer, deploying as part of a regionally aligned force to the Republic of Korea in 2018.

"A STRONG NATION REQUIRES a strong intelligence organization."

—President George Bush, News conference, 8 May 1991

Tactical Information Collection: How Intelligence Sustains the Faster Pace of Large-Scale Combat Operations



by Mr. Ryan Owens

Editor's Note: Mr. Ryan Owens wrote this article with input from members of the Information Collection Planner Course cadre, all of whom are part of the Information Collection Community of Practice.

Introduction

During large-scale combat operations, the intelligence staff must synchronize with the rest of the staff to provide timely and relevant intelligence that supports the commander's decisions. The G-2/S-2 collection manager is the cornerstone for this synchronization. During the counterinsurgency fight, the process for providing intelligence support to the staff and commander was often abbreviated, which is not ideal for large-scale combat operations. Returning to the basics of intelligence production and applying doctrinal collection management tools, techniques, and procedures will help ensure synchronization and success on the battlefield.

Set the Right Foundation for New Challenges

Thorough and in-depth intelligence production is the foundation of any operation. Haphazard, unfocused, and rushed intelligence production is detrimental, especially in large-scale combat operations. Military intelligence Soldiers use intelligence preparation of the battlefield (IPB) to understand the environment and the threat. They support the military decision-making process (MDMP) by leading the IPB effort and providing all-source intelligence products and tools. They also perform relevant and timely collection that provides situational understanding enabling the commander's informed decision making. However, many military leaders say that the focus on counterinsurgency operations has caused a loss in the basic skills of IPB, MDMP, and information collection tasks. Collection managers must now consider the challenges of information collection against a peer threat, across all domains, and become, or remain, proficient at the basics—IPB and MDMP—as well as more advanced skills like developing timely and coherent collection plans that support commanders' priority intelligence requirements (PIRs).

Robust and ongoing IPB is the foundation for an equally robust and timely information collection plan. Although all four steps of IPB are important, defining the operational environment and describing its effects provide an understanding of where the enemy may pose a critical threat. During multi-domain operations, the intelligence staff officer must understand and evaluate each domain to inform commanders of possible vulnerabilities. During shaping and preventing operations, the intelligence staff officer plans the collection of information that leads to an intimate understanding of threats. Understanding threat capabilities and formations allows the intelligence staff officer to speak accurately about the threat's intentions and capabilities. The intelligence Soldier's awareness of potential threats also informs staffs about threat strengths and tactics in all possible situations. When the G-2/S-2 fully and accurately leads IPB considering all domains, the intelligence section can develop and present threat situational templates and event templates that support the MDMP in a way that reduces uncertainty about the enemy. Doing this results in focused collection requirements and avoids overtasking collection with more data and information, which analysts must then exploit. Developing a well-thought-out event template enables building a coherent collection plan, which can provide focused collection, confirming or denying enemy courses of action (COAs).

Doctrine advises the use of operational and mission variables when analyzing the operational environment. This does not change during large-scale combat operations. The Soldiers in the intelligence section must actively engage during each step of MDMP to apply their skillset appropriately. In the counterinsurgency fight, the intelligence community focused heavily on targeting, and intelligence did not always support the entire staff. This often resulted in long collection times over large, unfocused named areas of interest. Collection concentrating on high-value individual targeting while flying collection assets for the maximum flight time will not work during large-scale combat operations. A more focused collection will limit risk and heighten survivability and accessibility of finite collection assets. During MDMP, the G-2/S-2 must create a collection plan that answers all staff elements' needs, not just maneuver and targeting, and refine that plan for each friendly COA.

Role of the G-2/S-2 and Collection Manager

The G-2/S-2 and collection manager are responsible for synchronizing the collection for each friendly COA and do so by building an information collection plan that meets the staff's needs in time and space. The collection manager is enabled to do so effectively when they tie together all the commander's critical information requirements (CCIRs), information requirements, and intelligence requirements. Simply put, during MDMP the commander's intent drives determination of the commander's requirements. The staff then translates the commander's requirements into—

- CCIRs—information requirements identified by the commander as being critical to facilitating timely decision making. They are divided into one of two categories:
  - What information the commander and staff need to understand about friendly forces and their support (friendly forces information requirement).
  - What the commander and staff need to understand about the threat and the operational environment (PIR).

In addition to nominating CCIRs, the staff also identifies and nominates those aspects about the friendly force that must be protected. These are essential elements of friendly information (EEFIs). Approval of EEFIs allows the staff to plan and implement measures to protect friendly force information such as military deception and operations security.

Our job as military intelligence professionals is to thoroughly know the enemy and provide that knowledge to the rest of the staff. However, it is equally important to know the full range of our own asset capabilities and limitations. Unfortunately, there is an overreliance on airborne collection assets. The G-2/S-2 and the collection manager must understand ALL available assets, including the effective use of scouts. The underlying responsibility of the collection manager is to answer the commander's information requirements irrespective of the asset. The intelligence staff must advise the commander, during MDMP, on the best way to leverage ALL assets to meet their needs. Critical to large-scale combat operations, is that information collection must occur early enough to provide reaction time. Sometimes that collection supports indirect fires being used to shape the battlefield, and sometimes that collection supports maneuver by collecting and reporting on enemy formations as they approach engagement areas. Collection must be predictive and advise friendly forces where and when they are going to engage the enemy. Only with thorough planning and wargaming will this be successful.

Photo by U.S. Army National Guard SGT Saul Rosa

Virginia National Guard Soldiers assigned to the Staunton-based 116th Infantry Brigade Combat Team use a magnetic map board to track troop movement during a command post exercise April 14, 2018, at Fort Pickett, VA.

Timely Collection is Key

Doctrine mentions constant collection, but timely collection is more important during large-scale combat operations. Collection assets are vulnerable to enemy actions and defeat. Planning for and employing long collection times will more likely result in the loss of critical, perishable, and finite assets. In the past, the responsibility of a unit's collection was to the maximum range of that unit's weapons systems, such as artillery or aviation. Currently, because of organic asset vulnerabilities against peer threat capabilities, the collection assets of a brigade combat team will rarely ever be able to collect the entire area of its longest ranging weapon systems. The result is the revived and needed use of intelligence handover lines to synchronize information collection with higher echelons. This emphasizes the requirement to produce a focused event template and detailed information collection plan. Without a focused plan, friendly forces will not know which requirements they can answer organically, and thus which requirements they need to send to higher echelons.

Information collection managers must use the strategies of mixing, cueing, and redundancy to reduce vulnerability and increase the survivability of assets in our formations. A collection plan that uses these strategies, and is focused on PIR, will not likely have to re-task assets to cover additional or unexpected named areas of interest. As the staff answers PIRs, they update intelligence products supporting preferred friendly COA. The next PIR(s) lead to the next preferred COA. Like an engineer's flowchart across the operational environment, the collection assists maneuver to achieve success. However, this COA development must be rehearsed and planned during MDMP. When the staff has time to discuss all possible actions, reactions, and counteractions, success on the battlefield is greatly enhanced. Lastly, the information collection plan will also allow assets to report relevant information to those units accurately and rapidly. Collectors who know and understand the collection plan, and its expected results, give staffs the ability to gain and maintain contact with the enemy.

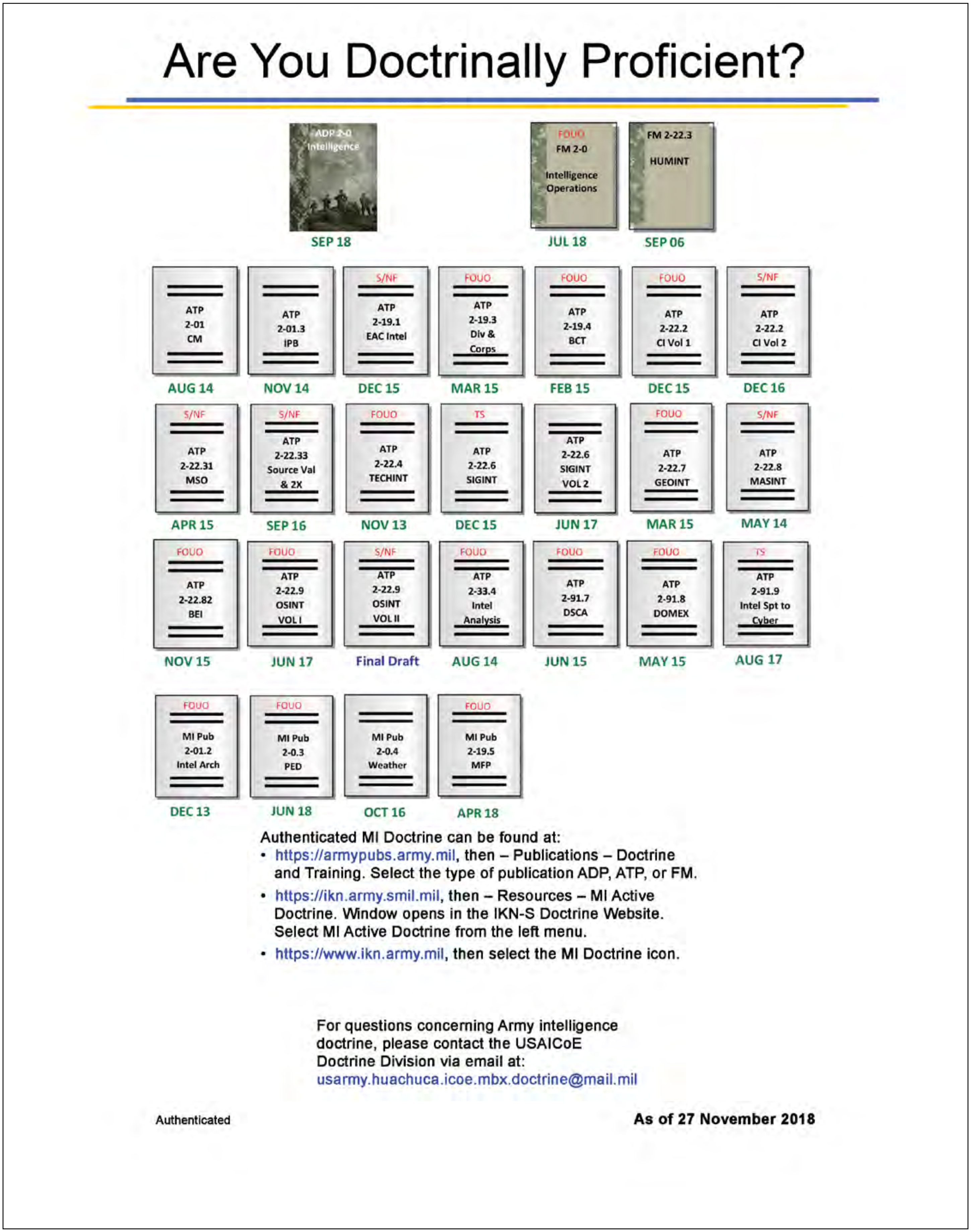
Photo by U.S. Air Force SrA Ricky Best

Army CPT Eugene Hunt and Air Force Capt Charles Carter review an aeronautical chart used by 379th Air Expeditionary Wing (AEW) aircrews. CPT Hunt is a ground liaison officer and Capt Carter is an intelligence weapons officer, both assigned to the 379th AEW.

It's Time to Refocus

Reviewing new and emerging doctrine makes it clear that the role of military intelligence is just as important now as it has ever been, and its effects are as important as the efforts of all other staff sections. To maintain that relevancy and a seat at the table, military intelligence Soldiers must be active and present to meet those responsibilities. During ANY operation, the G-2/S-2 has the responsibility for answering the commander's PIR. Commanders, staff, and intelligence professionals have lost their edge on some collection and intelligence analysis skills after years of the counterinsurgency fight. Now it's time to refocus. During large-scale combat operations, the commander's decision cycle will be tied to the speed of battle. Commanders will have to make decisions and assume risk based on limited collection. When the G-2/S-2 goes back to basics with MDMP and encourages staff participation in answering the PIR, information collection management during large-scale combat operations will not be such a daunting task. Proactive information collection managers, who take the time to plan, stay engaged, and use a "schoolhouse-style" collection plan that is synchronized, thorough, and timely, will support the warfighter in a multi-domain operational environment.

Mr. Ryan Owens was a U.S. Army all-source intelligence technician and currently works as an Information Collection Planner Course contractor instructor at the U.S. Army Intelligence Center of Excellence.



Are You Doctrinally Proficient?

ADP 2-0 Intelligence SEP 18	FOUO FM 2-0 Intelligence Operations JUL 18	FM 2-22.3 HUMINT SEP 06

ATP 2-01 CM AUG 14	ATP 2-01.3 IPB NOV 14	S/NF ATP 2-19.1 EAC Intel DEC 15	FOUO ATP 2-19.3 Div & Corps MAR 15	FOUO ATP 2-19.4 BCT FEB 15	FOUO ATP 2-22.2 CI Vol 1 DEC 15	S/NF ATP 2-22.2 CI Vol 2 DEC 16
S/NF ATP 2-22.31 MSO APR 15	S/NF ATP 2-22.33 Source Val & 2X SEP 16	FOUO ATP 2-22.4 TECHINT NOV 13	TS ATP 2-22.6 SIGINT DEC 15	ATP 2-22.6 SIGINT VOL 2 JUN 17	FOUO ATP 2-22.7 GEOINT MAR 15	S/NF ATP 2-22.8 MASINT MAY 14
FOUO ATP 2-22.82 BEI NOV 15	FOUO ATP 2-22.9 OSINT VOL I JUN 17	S/NF ATP 2-22.9 OSINT VOL II Final Draft	FOUO ATP 2-33.4 Intel Analysis AUG 14	FOUO ATP 2-91.7 DSCA JUN 15	FOUO ATP 2-91.8 DOMEX MAY 15	TS ATP 2-91.9 Intel Spt to Cyber AUG 17
FOUO MI Pub 2-01.2 Intel Arch DEC 13	FOUO MI Pub 2-0.3 PED JUN 18	MI Pub 2-0.4 Weather OCT 16	FOUO MI Pub 2-19.5 MFP APR 18			

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

Authenticated

As of 27 November 2018

Proponent Notes

OCMI US Army Intelligence Center and Fort Huachuca
Office Of The Chief, Military Intelligence

Personnel Structure Changes for Multi-Domain Operations

by Lieutenant Colonel Brian H. Cunningham, Master Sergeant Mary M. Breslin, Sergeant First Class Seth K. Nuckols, and Sergeant First Class Demes S. Kilby

During fiscal year (FY) 2018, Headquarters, Department of the Army (HQDA) Executive Order 048-18 directed personnel authorization mergers to maintain readiness and prepare for future large-scale combat operations. U.S. Army senior leaders estimate the reduction of specialties will significantly improve the matching of assigned personnel to authorizations by rank, military specialization, and organization of assignment.[1] The Army's senior leaders' goal is to keep the operational force manned at the highest level possible. The personnel structure revisions reduce Soldier distribution challenges for Army units and joint organizations. GEN Stephen Townsend, U.S. Army Training and Doctrine Command (TRADOC) Commanding General, stated the Army must become "more lethal, more sustainable, and better integrated as part of the joint force."[2] The U.S. Army Intelligence Center of Excellence (USAICoE) submitted four military occupational classification structure (MOCS) documents to TRADOC, the Army Deputy Chief of Staff G-1, the Army Deputy Chief of Staff G-2, and the Army Deputy Chief of Staff G-3/5/7. USAICoE MOCS actions will modify the FY 2019 Military Intelligence (MI) Corps personnel structure (Figure 1). In accordance with DA PAM 611-21, *Military Occupation Classification and Structure*, a MOCS document standardizes future changes for the classifications of Soldiers and positions.[3] The MI Corps MOCS actions include—

- ✦ officer mergers for areas of concentration (AOCs).
- ✦ merger of the MI master sergeant ranks.
- ✦ establishment of skill level one authorizations for military occupational specialty (MOS) 35L, Counterintelligence.
- ✦ merger of the 35Q, Cryptologic Network Warfare Specialist MOS with the 35N, Signals Intelligence Analyst MOS.

Preparation for these revisions will take place between FY 2019 and FY 2020.

These changes will prepare U.S. Army professionals for multi-domain operations and large-scale combat operations against peer and near-peer competitors. FM 3-0, *Operations*, states, "Army forces must be organized, trained, and equipped to meet worldwide challenges against a full range of threats. The experiences of the U.S. Army in Afghanistan and Iraq in the early 21st century are not representative of the most dangerous conflicts the Army could face in the future."[4] During FY 2021, the U.S. Army and the MI Branch will implement the personnel structure revisions.

Officer Mergers

The officer authorization revisions will improve precision for the personnel distribution process, reduce redundancies between intelligence officers, and streamline the accessions process for the MI Branch. The intelligence discipline aligned AOCs are not career tracks and do not provide precise

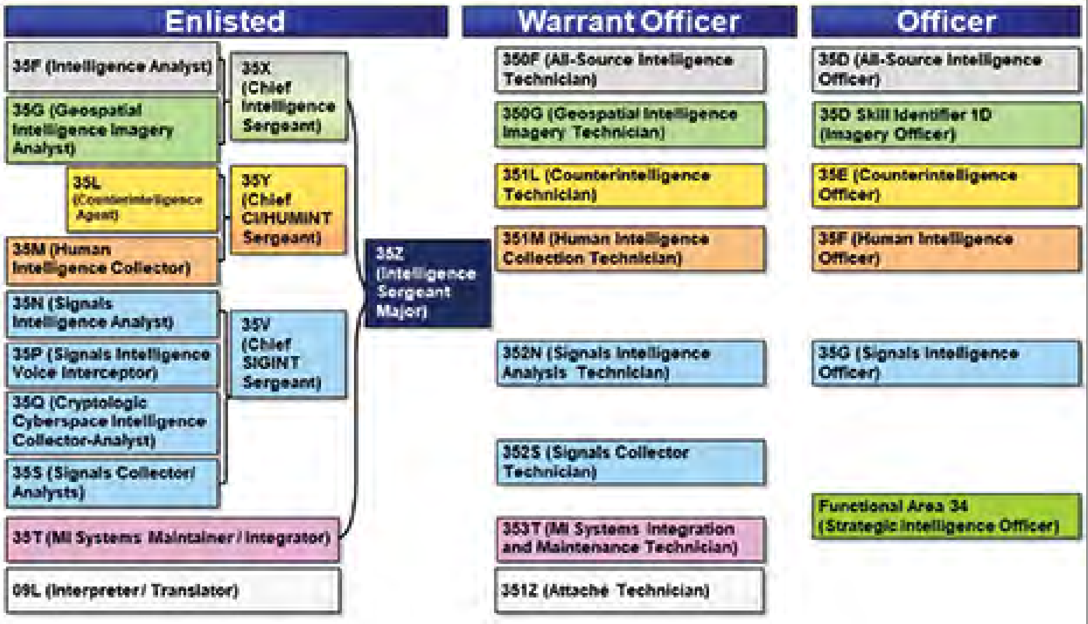

Enlisted
35F (Intelligence Analyst)
35G (Geospatial Intelligence Imagery Analyst)
35L (Counterintelligence Agent)
35M (Human Intelligence Collector)
35N (Signals Intelligence Analyst)
35P (Signals Intelligence Voice Interceptor)
35Q (Cryptologic Cyberspace Intelligence Collector-Analyst)
35S (Signals Collector/ Analysts)
35T (MI Systems Maintainer / Integrator)
09L (Interpreter/ Translator)
35X (Chief Intelligence Sergeant)
35Y (Chief CI/HUMINT Sergeant)
35V (Chief SIGINT Sergeant)
35Z (Intelligence Sergeant Major)
Warrant Officer
350F (All-Source Intelligence Technician)
350G (Geospatial Intelligence Imagery Technician)
351L (Counterintelligence Technician)
351M (Human Intelligence Collection Technician)
352N (Signals Intelligence Analysis Technician)
352S (Signals Collector Technician)
353T (MI Systems Integration and Maintenance Technician)
351Z (Attaché Technician)
Officer
35D (All-Source Intelligence Officer)
35D Skill Identifier 1D (Imagery Officer)
35E (Counterintelligence Officer)
35F (Human Intelligence Officer)
35G (Signals Intelligence Officer)
Functional Area 34 (Strategic Intelligence Officer)

Figure 1. FY 2019 Military Personnel Structure

distributions for 35E, Counterintelligence Officer; 35F, Human Intelligence Officer; and 35G, Signals Intelligence Officer authorizations. These three AOCs provide multiple broadening opportunities and a few key developmental opportunities for intelligence officers. The MOCS combines the All-Source Intelligence Officer AOC, the Counterintelligence Officer AOC, the Human Intelligence Officer AOC, and the Signal Intelligence Officer AOC into AOC 35A, the Intelligence Officer. The U.S. Army will track the intelligence discipline training for officers by skill identifiers. The MOCS does not change the authorization for these requirements, since this action converts previous AOC requirements to skill identifier authorizations. The MI Branch's consolidation of AOCs is similar to other branches such as the Infantry and Armor branches. This MOCS also merges functional area (FA) 34 with the MI Branch. FA 34 authorizations will convert to AOC 35B, the Strategic Intelligence Officer. The 35B authorizations will remain at the joint, strategic, and national levels. Officers will realign to 35A and 35B, while meeting requirements for multi-domain operations and preparations for large-scale combat operations.[5]

The MOCS eliminates certain officer distribution challenges, while increasing the precision in matching the officers to authorizations from company-level to national-level organizations. Field grade intelligence officers must understand the capabilities of personnel and systems within the intelligence warfighting function for decisive action in the land, air, maritime, space, and cyberspace domains. The consolidation of the officer authorizations and the officer inventories improves efficiency by reducing officer accessions and distribution challenges, since officer inventories have grown significantly over time. The U.S. Army filled Army requirements before filling joint requirements, since the Army decreased from a strength of more than 710,000 Active Duty Soldiers during 1992 to fewer than 508,000 Active Duty Soldiers during 1995.[6] MI Branch could not holistically fill Army and joint field grade authorizations for majors and lieutenant colonels. In 2000, GEN Dennis Reimer, then Chief of Staff of the Army, approved establishment of the FA for strategic intelligence officers as part of the Officer Personnel Management System XXI.[7] Understrength MI officer manning during the late 1990s necessitated the establishment of FA 34. HQDA established FA 34 in the Information Operations Division and reallocated MI Branch's 35B authorizations to FA 34.[8] Then in 2006, GEN Peter Schoomaker, then Chief of Staff of the Army, approved the inclusion of the MI Branch and FA 34 in the Operational Support Division. GEN Schoomaker also directed the implementation of position sharing for Branch 35 officers and FA 34 officers.[9] Since this period, conditions and the operational environment changed to include Russia's seizure of Crimea.

In the last 6 years, U.S. Army intelligence officer inventories for both FA 34 and Branch 35 field grade officers exceeded authorizations. Human Resources Command interchange fills for FA 34 officers and Branch 35 officer authorizations are based upon guidance from the Chief of Staff of the Army. During the last decade, FA 34 officers and Branch 35 officers performed the same duties, such as the Army Service component command (ASCC) Analysis and Control Element Chief, Corps G-2, and ASCC G-2. This realignment consolidates FA 34 within Branch 35 to reduce the redundancies between MI officers.[10] Merging FA 34 into Branch 35 establishes equitable opportunity for officers, affords greater flexibility in managing assignments, and aligns personnel to authorizations.

The MOCS will open additional opportunities for all intelligence officers to serve in joint organizations, thus earning joint experience and qualifications before selection and promotion to colonel. Additionally, the action enables joint assignment diversity for top-third MI officers rather than apportioning assignments between two similar officer categories. These personnel structure changes open opportunities for all accessed officers to receive the appropriate training and experience necessary to represent Army intelligence interests and successfully fulfill Army requirements from tactical to strategic echelons.[11] Finally, the action will ensure the efficient and effective preparation of the MI Corps officers for multi-domain operations in large-scale combat operations.

Master Sergeant Mergers

In response to HQDA Executive Order 048-18, USAICoE recommended a MOS merger at the master sergeant rank. The action will merge four of the MI Branch's master sergeant MOSs with the current 35Z MOS during FY 2021. The future 35Z MOS will consist of master sergeants, sergeants major, and command sergeants major. This merger provides additional organizational leadership experiences necessary for future sergeants major. FM 2-0, *Intelligence*, states, "many of the considerations necessary to achieve military success in the current operational environment remain fundamentally unchanged, but what has changed is important. Army forces cannot focus solely on large-scale ground combat operations at the expense of other missions, but they also cannot afford to be unprepared for large-scale combat operations in an increasingly unstable world."[12] The MI Branch's action establishes the 35Z5O MOS and formalizes master sergeants as organizational leaders across the intelligence warfighting function, thus improving their preparation to serve as sergeants major and command sergeants major.[13] The revisions in Figure 2 will affect all three U.S. Army components. All future MI master sergeants will conduct their transition earlier in their career from operating as single-discipline technical experts to experienced organizational leaders and advisors. Their responsibilities will emphasize the training and education of collective tasks and requirements across the intelligence warfighting function. The sooner the transition can occur, the easier the transition to senior roles and responsibilities.

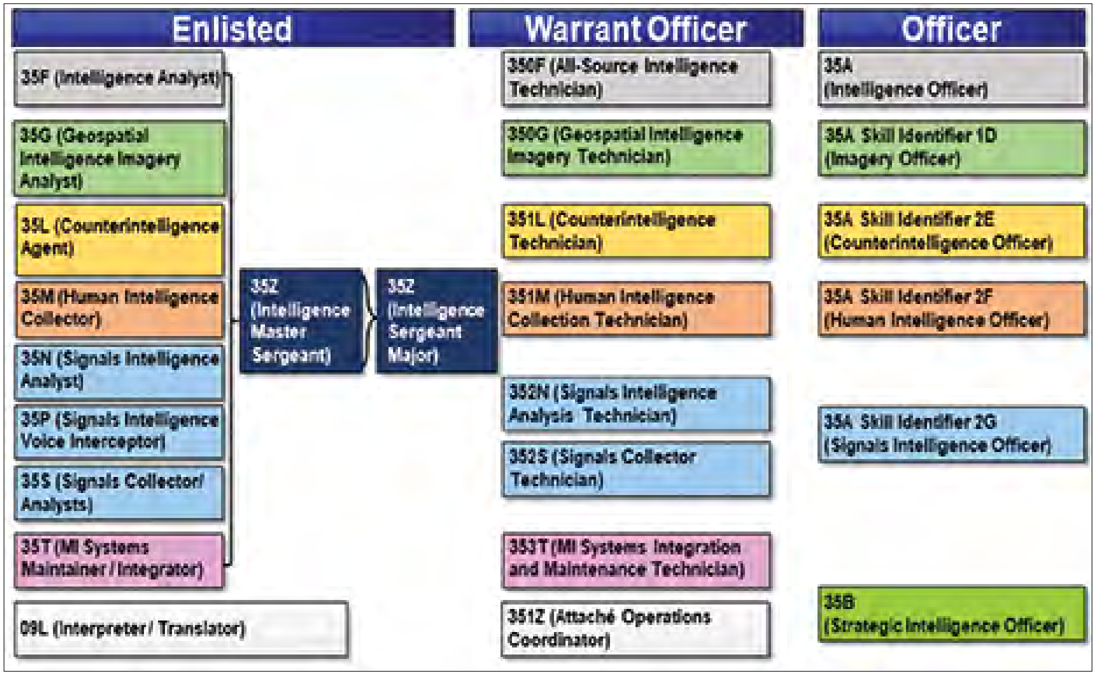

Enlisted
Warrant Officer
Officer
35F (Intelligence Analyst)
35G (Geospatial Intelligence Imagery Analyst)
35L (Counterintelligence Agent)
35M (Human Intelligence Collector)
35N (Signals Intelligence Analyst)
35P (Signals Intelligence Voice Interceptor)
35S (Signals Collector/ Analysts)
35T (MI Systems Maintainer / Integrator)
09L (Interpreter / Translator)
35Z (Intelligence Master Sergeant)
35Z (Intelligence Sergeant Major)
350F (All-Source Intelligence Technician)
350G (Geospatial Intelligence Imagery Technician)
351L (Counterintelligence Technician)
351M (Human Intelligence Collection Technician)
352N (Signals Intelligence Analysis Technician)
352S (Signals Collector Technician)
353T (MI Systems Integration and Maintenance Technician)
351Z (Attaché Operations Coordinator)
35A (Intelligence Officer)
35A Skill Identifier 1D (Imagery Officer)
35A Skill Identifier 2E (Counterintelligence Officer)
35A Skill Identifier 2F (Human Intelligence Officer)
35A Skill Identifier 2G (Signals Intelligence Officer)
35B (Strategic Intelligence Officer)

Figure 2. FY 2021 Military Intelligence Personnel Structure

The merger at 35Z5O emphasizes organizational leadership experiences earlier in a noncommissioned officer's career, which will enhance the capability of master sergeants to serve as future sergeants major and command sergeants major. The MI Advance Leader Course will include organizational leadership training. Additionally, all future promotable sergeants first class will attend the Master Leader Course before promotion to master sergeant. These two courses will provide baseline education for organizational leadership. The merger provides master sergeants with greater flexibility for assignments such as first sergeant, senior enlisted advisor, and senior staff section noncommissioned officer-in-charge. Master sergeants will promote to sergeants major and command sergeants major ready to provide advice and mentorship for matters across the intelligence warfighting function.[14]

Counterintelligence Agents

In FY 2007, the Army rescinded accessions for 97B10 (Counterintelligence Assistant) Soldiers and designated 35L, Counterintelligence Agent, as an in-service accessions MOS. Since FY 2010, the MI Corps faced challenges sustaining a sufficient level of in-service accessions to maintain counterintelligence capabilities and prevent readiness shortfalls. Seven years of varied initiatives for 35L20 in-service accessions yielded insufficient results. The in-service accession issue became a significant struggle by the end of fiscal year 2017. As a result, on 7 November 2017, LTG Scott Berrier, Army Deputy Chief of Staff G-2; MG Robert Walters, USAICoE Commanding General; and MG Christopher Ballard, former U.S. Intelligence and Security Command Commanding General, decided to return skill level one Counterintelligence Agent authorizations to the U.S. Army.

On 22 November 2017, USAICoE submitted a MOCS action for HQDA approval to implement the return of skill level one Soldiers (privates first class and specialists) to the 35L MOS. The Counterintelligence Critical Task Site Selection Board met from 27 November to 1 December 2017 to establish 35L10 critical skills. The members of this board also validated the rest of the counterintelligence critical skills (skill level two and above). On 13 September 2018, HQDA approved the 35L10 action and published the notification of future change informing leaders across the U.S. Army. The in-service accession issue for 35L20 remained prevalant during 2018. HQDA approved the conversion of 73 counterintelligence noncommissioned officer authorizations to 35L10 authorizations during FY 2021. Establishment of MOS 35L10 improves overall readiness by enabling a capable counterintelligence force to meet the Army's current and emerging requirements for multi-domain operations.[15]

35N MOS and 35Q MOS Merger

The activation of the Army Cyber Command on 1 October 2010 closely followed the Cyber Command's creation on 23 June 2009. The primary Soldiers used for this mission against emerging threats in the cyberspace domains were a combination of—

- 25D, Cyber Network Defender,
- 35N, Signals Intelligence Analyst,

- 35P, Cryptologic Linguist,
- 35S, Signals Collector, and
- 35T Military Intelligence Systems Maintainer/Integrator personnel.

On 1 October 2012, the U.S. Army established MOS 35Q, Cryptologic Cyberspace Intelligence Collector–Analyst, as the primary MOS for intelligence support to cyberspace operations. As Army Cyber Command expanded its role, the Cyber Center of Excellence activated on 28 March 2014 and the HQDA established the MOS 17C, Cyber Operations Specialist, in FY 2016. The 35Q MOS became a primary bill payer for the creation of 17C authorizations. Leaders in career management field 17 used many of the 35Q personnel, mission roles, responsibilities, and training. After the establishment of the 17C MOS, the U.S. Army reduced the 35Q MOS from 588 to 215 authorizations. The on-hand strength of the 35Q MOS fell from 546 Soldiers to 176 Soldiers after mandatory reclassifications to 17C. Authorizations for the 35Q MOS grew slightly by 40 authorizations between FY 2016 and FY 2018, thus limiting the growth opportunities and potential of the MOS.

In FY 2018, HQDA Executive Order 048-18 tasked USAICoE to assess MOS mergers and generalization within the career management field to increase promotion potential and ensure the proper match of personnel to authorizations. USAICoE submitted a MOCS request to merge 35Q and 35N authorizations. Analysis revealed that since the creation of 17C, multiple similarities existed between the 17C MOS and the 35Q MOS. The 17C and 35Q specialties attend identical training and have the same work role titles, but their utilization leads to different missions. Failure to clearly identify the differences in the utilization of the Soldiers, training, duty titles, and missions resulted in seemingly redundant mission sets without any doctrine to provide clarity. Additionally, the 35N and 35P specialties remain the primary specialties providing intelligence support to operations in the cyberspace domain.

This MOCS action allows for mission alignment within the MI Branch. This action also enables robust signals intelligence support in the cyberspace domain to meet the Army's current and emerging operational readiness requirements. Beginning in FY 2021, 35Q personnel will have 3 years to do one of the following:

- Attend the 35N transition course.
- Reclassify to another MOS.
- Separate from the U.S. Army.
- Transfer to another service.
- Retire.

During the 3-year period, the plan minimizes career impacts for Soldiers and affords mission sustainability. In this phase of transition, the 35Q Advanced Leader Course will continue to accept 35Q personnel to complete the Noncommissioned Officer Professional Development School's requirements for promotion. This proposal implements the methodical return of the cyberspace intelligence support billets and the majority of their mission sets to the 35N Signals Intelligence Analyst mission beginning in FY 2021.[16]

Conclusion

In summary, USAICoE submitted four MOCS actions for implementation during FY 2021 and beyond. These actions support MI Corps readiness by reducing redundancies. By 1 October 2020, HQDA will implement the changes and update tables of organization and equipment, tables of distribution and allowance, and joint duty assignment lists. The consolidation and reallocation of five intelligence officer AOCs into two AOCs benefits the U.S. Army by reducing Soldier distribution challenges and improving readiness for multi-domain operations. The realignment to the 35A AOC and 35B AOC establishes equitable opportunities among the Army's intelligence officers, while the U.S. Army ensures accessed officers receive the appropriate training and experience for advancement. The master sergeant merger will produce a more diverse and experienced senior noncommissioned officer population to serve as future sergeants major. The MI Branch will merge the 35Q MOS with the 35N MOS to reduce the redundancy of training and mission utilization between the MI and cyberspace career fields. The revisions to career tracks will provide intelligence professionals who represent U.S. Army intelligence interests and fulfill Army requirements from the tactical to the national levels. The transition from 14 MOSs to 10 and the reduction of 5 officer AOCs to 2 will support the U.S. Army senior leaders' goal to reduce personnel distribution challenges. The establishment of 35L10 authorizations improves the accession model and returns the 35L MOS to a healthy strength. These actions meet the intent of GEN Mark Milley, Chief of Staff of the Army, to reduce Soldier distribution challenges while maintaining readiness. The MI Corps and the Human Resources Command will improve the assignment of available Soldiers to units and organizations based on Army requirements and priorities.

Endnotes

1. Department of the Army, Training and Doctrine Command, Tasking Order IN180361, *Structure and Personnel Friction Analysis*, 2018.

2. Gina Cavallaro, "Townsend Takes Over at TRADOC: New Commander Emphasizes Constant Improvement," *Association of the United States Army*

online, 22 August 2018, https://www.ausa.org/articles/townsend-takes-over-tradoc-new-commander-emphasizes-constant-improvement.

3. Department of the Army, Pamphlet 611-21, *Military Occupational Classification and Structure* (Washington, DC: U.S. Government Publishing Office [GPO], 15 January 1991).

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

5. U.S. Army Intelligence Center of Excellence (USAICoE) Commanding General memorandum to Office of the Deputy Chief of Staff G-1, "Recommended Changes to DA Pam 611-21 for Branch 35 (Military Intelligence) and Functional Area 34 (Strategic Intelligence)," 15 May 2018.

6. Stephen L. Y. Gammons and William M. Donnelly, *Department of the Army Historical Summary Fiscal Year 1995* (Washington, DC: Center of Military History, 1995), https://history.army.mil/books/DAHSUM/1995/CMH_Pub_101-26-1.pdf.

7. Department of the Army, *OPMS XXI: Final Report* (Washington, DC: 9 July 1997), https://usacac.army.mil/CAC2/cgsc/carl/docs/OPMSXXI.pdf.

8. John M. Custer, "The Impact of OPMS XXI on MI Officers," *Military Intelligence Professional Bulletin* 23, no. 4 (October-December 1997): 29.

9. Barbara Fast, "Commanding General's Letter to the Field, April 2006," *Military Intelligence Professional Bulletin* 32, no. 2 (April-June 2006): 2.

10. USAICoE Commanding General memorandum, "Recommended Changes."

11. Ibid.

12. Department of the Army, FM 2-0, *Intelligence* (Washington, DC: U.S. GPO, 6 July 2018), vii.

13. USAICoE Commanding General memorandum to Office of the Deputy Chief of Staff G-1, "Recommended Changes to DA Pam 611-21, CMF 35 Master Sergeants," 15 May 2018.

14. Ibid.

15. USAICoE Commanding General memorandum to Office of the Deputy Chief of Staff G-1, "Establishment of 35L10, Counterintelligence Agent," 17 December 2017.

16. USAICoE Commanding General memorandum to Office of the Deputy Chief of Staff G-1, "Recommended Changes to DA Pam 611-21, Deletion of the 35Q MOS," April 2018.

LTC Brian H. Cunningham currently serves as the Director for the Office of the Chief of Military Intelligence (OCMI), Fort Huachuca, AZ. Before this assignment, he served as the Commander for the 2nd Military Intelligence Battalion in Germany. He also served as a Brigade Combat Team S-2 and the Analysis and Control Element Chief for the 1st Armored Division at Fort Bliss, TX. A 1997 graduate of the U.S. Military Academy, he holds graduate degrees in information technology and military studies.

MSG Mary Breslin is the 35N/35Q/35S/35V lifecycle career manager, OCMI, Fort Huachuca, AZ. She was previously Detachment Sergeant, 205th Military Intelligence Battalion, 500th Military Intelligence Brigade-Theater, at Fort Shafter, HI; and senior instructor, Senior Leader Course, Non-Commissioned Officers Academy, Fort Huachuca, AZ.

SFC Seth Nuckols is the 35L/35Y career management noncommissioned officer, OCMI, Fort Huachuca, AZ. Past assignments include counterintelligence platoon sergeant, 502nd Military Intelligence Battalion, 201st Expeditionary Military Intelligence Brigade; and senior enlisted leader for security, National Security Agency–Georgia.

SFC Demes Kilby is the 35T senior career manager, OCMI, Fort Huachuca, AZ. Previous assignments include career advisor and chief instructor writer.

How Lessons Learned Support Future Development of Army Intelligence

by Mr. Chet Brown, Chief, Lessons Learned Branch

Introduction

"The Army faces a unique set of challenges as it adapts to a world that has changed more broadly and fundamentally than at any other time since the end of World War II. The Army must continue to adapt to ensure success in a rapidly changing strategic environment. Now, more than ever before, it serves as a strategic Army, a land force that the United States and its allies rely on to meet global challenges."[1] Published a quarter-century ago in FM 100-5, *Operations*, this quote describes the current situation in which the Army finds itself operating.

LTG Michael Lundy, Commanding General of the U.S. Army Combined Arms Center, similarly discusses in the foreword of the Army's current operations manual, FM 3-0, *Operations*, the changing conditions that require an adaptive transformation in the Army's capabilities to meet "a challenge the joint force has not faced in twenty-five years."[2]

Adapting to Change

These two versions of operations doctrine, published 25 years apart, confirm the necessity of an Army to adapt to emerging and changing conditions. Both references declare that adaptability facilitates operational readiness. Adaptation is also necessary in order to prepare for conducting large-scale combat operations to defeat the predominant threat types mentioned in the operations manuals. Another enduring factor contributing to unit readiness is the Army Lessons Learned Program (ALLP). The most recent evidence supporting this appears in the latest version of FM 2-0, *Intelligence*, which advises military intelligence (MI) leaders to identify lessons learned and emerging tactics, techniques, and procedures that could support the unit better in the future.[3] The purpose of improving readiness is of such importance to the lessons learned effort that it is specifically mentioned in the opening paragraph of the ALLP regulation.[4]

Current and past doctrine confirms three enduring attributes:

- The world is constantly changing.
- The Army must adapt to changing conditions to remain operationally ready.
- The ALLP supports adaptability and readiness.

The MI Lessons Learned program has also adapted to meet recent challenges and become more relevant to supporting Soldiers and leaders as they work to improve their respective personal and unit performance.

Three years ago, the lessons learned article in the *Military Intelligence Professional Bulletin* (MIPB) was titled "ICoE's Lessons Learned Support to the Force in 2025 and Beyond."[5] This current MIPB issue's theme, "Intelligence in Large-Scale Combat Operations," provides an opportunity to describe how the U.S. Army Intelligence Center of Excellence (USAICoE) Lessons Learned program has improved the quality and speed at which lessons and best practices contribute to operational readiness and help facilitate future developments in the Army intelligence capability areas of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). Of all the DOTMLPF capability areas, changes to doctrine and training can be, and often are, accomplished more quickly and less expensively than changes to other capabilities.

Another quote from the operations manual of yesteryear (FM 100-5) concisely and accurately describes how lessons learned contribute to developing doctrine and future capabilities, "Never static, always dynamic, the Army's doctrine is firmly rooted in the realities of current capabilities. At the same time, it reaches out with a measure of confidence to the future. Doctrine captures the lessons of past wars, reflects the nature of war and conflict in its own time, and anticipates the intellectual and technological developments that will bring victory now and in the future."[6]

The link between the Lessons Learned Branch and Doctrine Division at USAICoE is very strong. A constant flow of information between the two entities helps to inform each organization's respective efforts. A similarly continuous dialogue occurs between the Lessons Learned Branch and Concepts Directorates.

The continuous evolution of doctrine and concepts results in a very receptive audience for lessons and best practices identified by the practitioners of our profession. Whether identified by units, the Center for Army Lessons Learned, or various USAICoE elements, the comprehensive lessons learned enterprise feeds into MI concepts and doctrine development. This audience also includes those who are working to effect positive changes in all of the DOTMLPF capability areas. The systems described in the MIPB Lessons Learned article of 2015 remain intact.[7] What has changed is the manner in which lessons learned information is packaged, provided, discussed, and used by the organizations identifying, forming, equipping, staffing, fielding, and training the intelligence force of the future.

Changes to the MI Lessons Learned Program

The most significant and beneficial change to the MI Lessons Learned program occurred 2 years ago when the Lessons Learned Branch became part of the organization now known as the Directorate of Training. The move facilitated a more direct connection between lessons learned and the integration of appropriate lessons and best practices into training and the products used to present training at USAICoE. The Directorate of Training maintains a cadre of officers—discipline technical advisors (DTAs)—who are subject matter experts in their respective intelligence disciplines. The intelligence collection disciplines DTAs and maintenance DTAs are chief warrant officers who serve as the USAICoE Commanding General's primary advisors for analyzing, designing, and developing resident training within their respective disciplines. The DTAs ensure integration of doctrine, lessons learned, and other DOTMLPF considerations into training. Aside from informing organizational leaders of the most recent lessons learned observations, findings, or issues, the DTAs are the first personnel who receive lessons learned. Working closely with the Lessons Learned Branch, the DTAs assess lessons learned information for pertinence and potential integration into the range of underway or planned DOTMLPF activities. The DTAs provide an authoritative and responsive assessment on the best use for lessons learned information. Their knowledge and familiarity with the various organizations and personnel who participate in USAICoE's DOTMLPF activities identify the most direct channel to those who need the information.

Another revision made to the MI Lessons Learned program allows a more rapid and direct dissemination of lessons and best practices to MI Soldiers and leaders in the field through the monthly MI Lessons Learned Forum. *Dissemination* of lessons learned may not be the best word choice to describe the benefit of the MI Lessons Learned Forum—*discussion* is a better choice. During the first few years of the MI Lessons Learned Forum, the forum was conducted as a broadcast of validated information discovered by the USAICoE Lessons Learned Branch. The forum was predominantly a one-way presentation of problems identified by observing brigades and their subordinate units at combat training center rotations or the results of interviews with MI personnel recently returned from domestic or overseas training or operations. The forum changed for the better when personnel from the units we had observed began presenting their personal insights, challenges, and tips from success themselves. The forum now provides an unfiltered voice for MI leaders. Other than adhering to the appropriate operational and information security reviews and considerations, the forum provides an opportunity for personnel to speak as candidly as necessary to convey their ideas and experiences. Likewise, MI leaders who participate are able to receive information directly from the source without the successive levels or organizational filters. This point in no way suggests that any MI professional intentionally removes unpleasant or negative information—it is simply a description of avoiding the unintended transformation of information, such as demonstrated by the all-too-familiar telephone game.

Sharing Information to Help Others Succeed

The current success of the MI Lessons Learned Forum directly relates to the MI professionals who willingly and unselfishly share their successes, failures, and unsolved problems in an effort to help others succeed. Several times, often unexpectedly, someone in the forum audience will chime in with an idea, technique, or offer to help resolve a problem being discussed. Not surprisingly, many of the offers of assistance come from USAICoE personnel working in the various DOTMLPF capability area efforts that are forming the future of Army intelligence. Some of the articles in this issue of MIPB describe these efforts. The officers, noncommissioned officers, Civilians, and contractors who support DOTMLPF developments are an extremely valuable category of MI Lessons Learned Forum participants. Not only can these personnel provide an authoritative delineation of the information, from its origin to its current condition, but they can also identify how the information may be used to effect positive enduring change.

An example from a recent MI Lessons Learned Forum occurred when an MI captain asked why the geospatial engineers were assigned to the brigade combat team S-2 instead of the same section in the MI Company to which the geospatial intelligence Soldiers were assigned. The captain was given an explanation; but more importantly, solutions to help address the captain's immediate concerns were offered and continued to be provided after the session ended. The USAICoE personnel involved in geospatial intelligence DOTMLPF are committed to integrating the question into their current work in order to determine the most effective resolution.

While this was an example of how the forum can support the rapid integration of lessons learned, it also indicates how the forum is often the catalyst in forming mentoring relationships. Mentoring relationships often form during the Lessons Learned Forum from the interaction of Soldiers, noncommissioned officers, and officers.

Identifying New Areas for Lessons Learned Collection

Although the MI Lessons Learned Forum is experiencing a growing audience and relevance to the field as the force shifts to address large-scale combat operations, we must remain cognizant of, and react to, the sense of value that each participant receives from the forum. We too must embrace the enduring requirement to be flexible and adapt to remain useful and relevant to those we are committed to support. The forum experienced a similar situation as the Army moved its focus from Operation Iraqi Freedom to Operation Enduring Freedom. Much of the information and lessons from Operation Enduring Freedom were new to those who had not yet deployed to Afghanistan.

As familiarity with preparing and training for large-scale combat operations increases in the force, we have to prepare to identify other areas for lessons learned collection. We cannot wait until our information is obsolete to begin collecting and sharing new information. We must identify emerging lessons learned collection requirements now in order to provide the information needed to enable future developments in Army intelligence training, doctrine, and other capability areas. Thankfully, we do not have to develop our requirements unilaterally or in isolation. Commander's intent, desired end state, specified (and implied) tasks, and purposes are just as useful in guiding and directing the intelligence lessons learned enterprise as they are in leading tactical operations. We have an eye on some topics of importance to the future of Army intelligence and are currently involved in supporting efforts to address these topics.

Participate in the Process

If you want to participate in the discussion or see where we are going, dial in to the MI Lessons Learned Forum. Forum information is available on the common access card (CAC)-enabled side of the Intelligence Knowledge Network (IKN) main page https://www.ikn.army.mil/ in the Upcoming Forums box. Briefing slides from past forums are available on the Lessons Learned Portal. To access the portal, select the MI Training & References toggle box, and in the MI Reference Library box, click on the Lessons Learned link. Be sure to use your CAC email certificate when prompted. We also monitor the IKN Shout box, so leave a question or request there for us. We measure our success by how successful we make others. Sharing your lessons and best practices is one way we can help those driving the future of Army intelligence to be successful.

Endnotes

1. Department of the Army, Field Manual (FM) 100-5, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 14 June 1993 [obsolete]), 1-5.

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

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

4. Department of the Army, Army Regulation 11-33, *Army Lessons Learned Program* (Washington, DC: U.S. GPO, 14 June 2017), 1.

5. Chet Brown, "ICoE's Lessons Learned Support to the Force in 2025 and Beyond," *Military Intelligence Professional Bulletin* 41, no. 4 (October-December 2015): 64-65, https://www.ikn.army.mil/apps/MIPBW/MIPB_Issues/MIPBOct_Dec15IKN.pdf#page=1&view=fit.

6. Department of the Army, FM 100-5, *Operations*, v.

7. Brown, "ICoE's Lessons Learned."

> "Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity."
>
> —General George S. Patton, U.S. Army

Moments in MI History

Value and Handling of Prisoners in World War I

by Lori S. Stewart, USAICoE Command Historian

Prisoners or deserters constitute one of the most fruitful sources from which information of the enemy is obtained.
—Intelligence Regulations (1918)

By the time of the Armistice ending World War I on 11 November 1918, the United States held nearly 48,000 prisoners of war. The majority had been captured within the final months as the war moved out of the trenches. The American Expeditionary Forces (AEF) G-2, MAJ (later MG) Dennis Nolan put much emphasis on the information obtained from enemy prisoners. After the war, he remarked, "[A prisoner] can, as a rule, tell you much more than a spy… who is trying to get around and find out about the enemy. [A prisoner] knows and the other man is frequently guessing at it."

As Nolan shaped his formal intelligence organization in the early months of American involvement, he recognized prisoners could be captured anytime on any battlefield, and commanders at every echelon wanted to examine the prisoners they captured. He also realized that, because of a lack of personnel and the high operating tempo, in-depth interrogations at lower echelons were not practicable or effectual. Nolan developed a hierarchical system for the examination of prisoners at all echelons and outlined clear guidelines for handling prisoners in the 1918 *Intelligence Regulations and Instructions for Regimental Intelligence Service*. Those same guidelines appeared in the Army's first (provisional) *Combat Intelligence Manual*, also printed in 1918.

Nolan's system started at the regiment. The regimental intelligence officer, typically a first lieutenant, determined the name, rank, and organization of any prisoners, as well as the time and place captured. Prisoners were searched and then quickly transferred to division assembly points. The division G-2 sections, led by a lieutenant colonel or major, conducted limited questioning, with the help of commissioned linguists from the Corps of Interpreters. This questioning focused on necessary tactical information about the division sector to a depth of two miles behind the enemy front lines.

From the division, prisoners were transferred to the corps collecting centers, where more in-depth questioning began. The number of prisoners, especially during offensive operations, often stressed the corps G-2 sections. At those times, Army headquarters dispatched teams of four sergeants and one officer to augment the corps' interrogation efforts. During the St. Mihiel and Meuse-Argonne offensives in the fall of 1918, French interrogators also supplemented the U.S. interrogators.

The corps intelligence sections found that simple and direct questioning, combined with kindness and courtesy, were the most effective method for eliciting information. Many of the AEF's interrogators had been lawyers in their civilian lives and could coax information out of the most recalcitrant prisoner. Corps interrogators used a variety of other tactics to elicit information, as well. One interrogator found that he could get prisoners to talk openly if he showed them aerial photographs with landmarks they recognized. The II Corps G-2, COL (later GEN) "Vinegar Joe" Stilwell, recruited a drafted German soldier, who had previously lived in the United States and yearned to return there, to "work the prisoner cages" and glean information from his fellow prisoners. Additionally, U.S. interpreters donned German uniforms and wandered the collection points to eavesdrop on prisoners bragging about intentionally misleading their interrogators. This use of "stool pigeons" was common practice throughout the war.

The quality and veracity of the information varied with the rank of the prisoner. LTC Walter Sweeney, who served in the AEF G-2 during the war, claimed that "noncommissioned officers were by far the best sources for gaining information" and "few of them resisted insistent interrogation." About 60 percent of officers "invoked military honor" and refused to cooperate. A typical German soldier had little knowledge about the larger battlefield, but he provided details on his own unit, weapons, troop losses, and general morale. Enemy soldiers from Poland, Denmark, the Alsace-Lorraine region, and southern Germany were particularly cooperative. Unquestionably, the most important information obtained from prisoners was enemy order of battle, but they also gave up their routes of movement; the position and condition of trenches, dugouts, and wire entanglements; their capacity to attack; and how susceptible they were to being attacked.

Based on the preceding outline, it is clear that World War I was no different from any other war in U.S. Army history—prisoners of war have always proven to be valued sources of intelligence. However, formalizing and standardizing the process for handling and examining prisoners in the 1918 intelligence regulations and provisional manuals was one more step in modernizing U.S. Army intelligence. While field manuals published in 1940 provided more details on accepted interrogation techniques, the system for prisoner-of-war handling that Nolan developed for World War I continued, with minor changes, throughout the 20th century.

Epigraph

American Expeditionary Forces, *Intelligence Regulations*, October 21, 1918.

In mid-October 1918, CPT Ernst Howald (standing right), the lead interrogator for the 28th Division, Second U.S. Army, used prisoner statements to construct a detailed template showing the enemy facing the division. After the war, his estimates were proven highly accurate.

Contact and Article
Submission Information

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

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

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

When submitting articles to MIPB, please consider the following:

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

What we need from you:

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

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

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

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

PIN: 204309-000