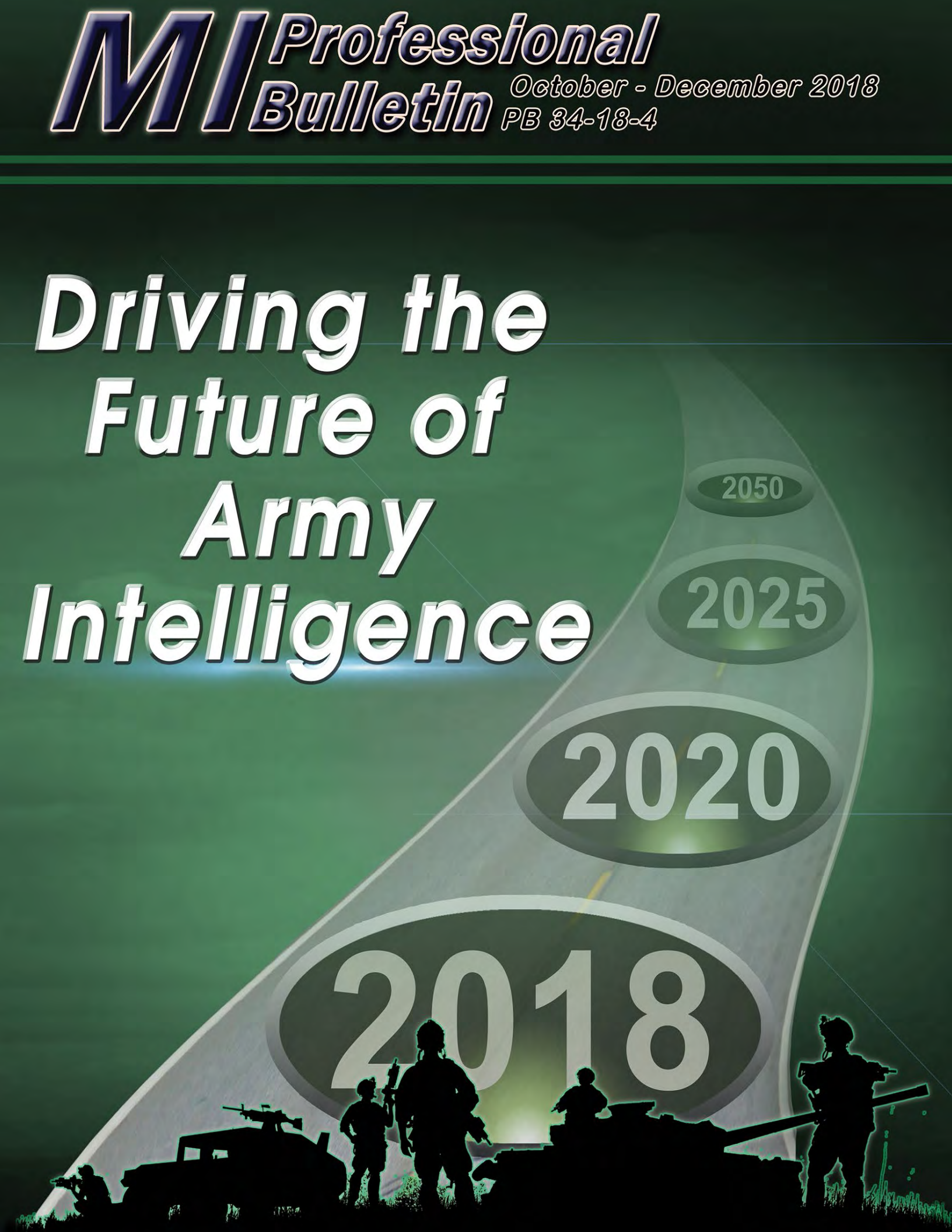
MI Professional Bulletin
October - December 2018
PB 34-18-4

Driving the Future of Army Intelligence



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

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

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

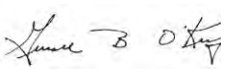
Our mailing address: MIPB (ATZS-DST-B), Dir. of Doctrine and Intel Sys Trng, USAICoE, 550 Cibeque St., Fort Huachuca, AZ 85613-7017

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
1819703

From the Editor

The following themes and deadlines are established:

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

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

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

October - December 2018
PB 34-18-4
Volume 44 Number 4

FEATURES

6 Accelerating Multi-Domain Operations: Evolution of an Idea
by GEN Stephen Townsend

9 Resetting Intelligence Doctrine
by Ms. Terri M. Lobdell

20 Assembly Required: The Building Blocks of ISR and PED Architectures
by Mr. John DellaGiustina, Mr. William Donner, and CW3 Otis Griffin III

25 Improving Intelligence Sharing
by Mr. Donald Beattie and Mr. Robert Coon

29 Military Intelligence Training Strategy Update
by MAJ Leah B. Haller

32 Adapting Multifunctional Intelligence and Electronic Warfare to Support Maneuver
by COL Mark Dotson, COL Jennifer McAfee, and COL Francesca Ziemba

35 The Future of Intelligence Analysis, Analytics, and Distribution
by COL Robert Collins, Ms. Lindsay Yowell, and Mr. Greg Hartman

38 Army Signals Intelligence Deep Dive: Developing a Strategy for the Future
by CPT Jason Boslaugh and Mr. Bryan Lasater

43 The Right Fit: Mission Command in the Twenty-First Century
by LTC Matthew T. Archambault, CPT Franklin G. Peachey, and CPT Jennifer P. Sims

55 Getting Intelligence to Move at the Speed of Decisive Action
by CPT Alex Morrow and CPT Michael Dompierre

59 Data Analytics to Win in a Complex World
by CW3 Garrett Hopp, CW3 Glenn Gleason, CW3 Nick Rife, and CW2 Ashley Muller

62 The Intelligence Warfighting Function: Rethinking Force Generation
by CW3 William J. Fann

65 Human Intelligence and Counterintelligence in the Brigade Combat Team
by CW3 Adam Hanson, 1SG Gary Vilano, and SFC Brendon Wiese

68 Developing Analytical Capabilities in Changing Environments
by CPT Christie P. Cunningham

72 Collecting in Vichy: Intelligence Operations in the French Resistance
by CPT Charles F. Nadd

75 Army Aviation Association of America Soldier of the Year
by Ms. Jocelyn Broussard

DEPARTMENTS

2 Always Out Front
3 CSM Forum
4 Technical Perspective
77 Culture Corner
82 Awards for Excellence in MI

Inside back cover: Contact and Article Submission Information

Always Out Front

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

The title of this quarter's *Military Intelligence Professional Bulletin* (MIPB) is "Driving the Future of Army Intelligence." The title captures the theme of this issue—topics addressed during the 2018 Intelligence Senior Leaders Conference (ISLC), which the U.S. Army Intelligence Center of Excellence (USAICoE) and Fort Huachuca hosted in March. The focus of the conference was military intelligence (MI) capability gaps identified last year by the Strategic Portfolio Analysis Review (SPAR). The SPAR process conducts value analyses to assess equipment capabilities, identify risks inherent to capabilities, and weigh potential resource implications. Three specific SPAR gaps were discussed at the conference—the ways to improve the Army's processing, exploitation, and dissemination (PED) architecture, intelligence sharing, and multifunctional intelligence supporting maneuver. Some of the articles in this MIPB issue address those capability gaps, while others provide a snapshot of the direction in which MI is heading.

Participation at the conference included leadership and commanders from across the globe—the Department of the Army (DA) G-2, the U.S. Army Intelligence and Security Command (INSCOM), USAICoE, U.S. Army Special Operations Command, Military Intelligence Readiness Command, and U.S. Army Forces Command. LTG Scott Berrier, DA G-2, and MG Christopher Ballard, then Commanding General of INSCOM, attended.

During his presentation, LTG Berrier talked about pacing threats and leveraging partnerships in the Army. He also gave senior leaders an opportunity to ask questions. One question was about the National Guard and Reserve Component intelligence readiness and the status of where these components are in relation to Active Duty units. LTG Berrier expressed the need to continually provide the necessary training to the right people. He also said that National Guard and Reserve Component units could use the Intelligence Knowledge Network for additional resources. The dialogue between LTG Berrier and the senior leaders was extremely helpful, allowing the DA G-2 to explain what he is doing for our warfighting function.

There were several presentations and breakout sessions at the two-day conference. Mr. DellaGiustina and CW3 Griffin, from the U.S. Army Training and Doctrine Command (TRADOC) Capabilities Development and Integration Directorate, led a discussion on the PED architecture in Europe and Korea. The Deputy TRADOC Capability Manager (TCM)–Sensor Processing, Mr. Beattie, briefed Army intelligence sharing and how we can improve it. The Directors of TCM–Terrestrial and Identity, TCM–Aerial, and TCM–Electronic Warfare gave a combined briefing about the improvement of multifunctional intelligence supporting maneuver. The presenters subsequently wrote articles, based on the briefings they gave, for this issue of MIPB.

Other articles include a piece about the MI Training Strategy, written by MAJ Haller, highlighting the certification plan to measure intelligence readiness across brigade combat teams. You will also find an article by Ms. Lobdell, titled "Resetting Intelligence Doctrine." It is important that everyone understands that we updated FM 2-0, *Intelligence*, in July 2018, to incorporate the foundational changes made by the recent revision of FM 3-0, *Operations.* These changes are essential to our warfighting function because doctrine is our professional body of knowledge.

ISLC provided an opportunity for a dialogue among the attendees. One of the long-term benefits of the conference will be that the doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) assessments will be updated based on the outcome of the discussions and collaboration between the intelligence leadership in attendance.

As MG Ballard said during his presentation, "Unless you identify our intelligence capability gaps, as a warfighting function we cannot move forward." He was absolutely right, and the conference was a great forum for this discussion. As a collective, we were able to help close some of the capability gaps. As we move forward, we must continue to collaborate, ensuring that *One Vision, One Voice, and One Vector* is shared among the intelligence corps.

Always Out Front!

CSM FORUM

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

The U.S. Army Intelligence Center of Excellence hosted the 2018 Intelligence Senior Leaders Conference at Fort Huachuca. During the conference, senior leaders made a decision that at first may seem minor but has huge implications for military intelligence (MI) noncommissioned officers (NCOs). I'm going to add a caveat, however, to say that the Department of the Army has not yet approved the decision.

The recommendation was made to combine the following military occupational specialties (MOSs) at the master sergeant (MSG) and first sergeant (1SG) ranks into a single MOS (35Z50) in order to meet a directive to merge as many MI MOSs as possible:

- 35T, Military Intelligence Systems Maintainer.
- 35V, Signals Intelligence Senior Sergeant.
- 35X, Intelligence Senior Sergeant.
- 35Y, Chief Counterintelligence/Human Intelligence Sergeant.

Up to this point, the norm across the MI Corps has been to stovepipe our NCOs in positions that flow along the career path of their particular MOS and discipline. There are advantages to this, as Soldiers build their knowledge, skills, and abilities within areas of technical and tactical competence while serving in iteratively more complex leadership positions. The problem is at the level of brigade command sergeant major (CSM) and beyond; we expect our senior NCOs to be diversified enough to ensure all disciplines are synchronized and offer educated recommendations to commanders on how to best provide intelligence enterprise support to warfighters. We have not been deliberate in offering our NCOs diversified experiences until they are already a sergeant major (SGM).

Approximately 24 months ago, we began diversifying our SGMs coming out of the U.S. Army Sergeants Major Academy by putting many of them in positions that require them to manage missions they were unaccustomed to dealing with based on their career trajectory. This was the first time our career management field (CMF) deliberately began preparing SGMs to move into senior level CSM and SGM positions with experience outside their MOS.

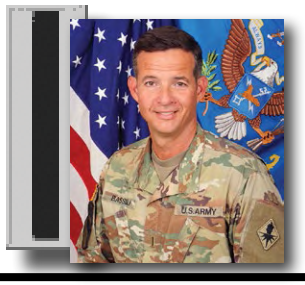
Merging at MSG will now allow our CMF to begin diversifying our NCOs one level earlier and further professionalize our NCO cohort. MSGs will primarily remain aligned with their MOS or serve in operations positions. We are highlighting 1SG positions as key and developmental to career progression. 1SGs will still be responsible for their customary roles, but will now have an opportunity to manage a mission they have not had an opportunity to oversee in the past. This plan will be even more beneficial for our 35Ts who do not typically perform a standard intelligence mission through the rank of sergeant first class.

If approved, the MOS merger will benefit the MI Corps by providing senior leaders another opportunity to assess and manage talent. In many cases, 1SG positions will require our senior NCOs to step outside their comfort zones and still perform to a high standard, which is what we expect of our CSMs and SGMs. We have now provided a great developmental opportunity for our NCOs while allowing our most agile and adaptive leaders to distinguish themselves from their peers.

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



To all my fellow military intelligence (MI) professionals, it is with great humility and extreme enthusiasm that I continue to serve our Army as the 7th Chief Warrant Officer of the MI Corps. To say that I have far exceeded expectations from the days when I was a young private first class at Fort Carson, Colorado, is a gross understatement. It is a testament to what dedicated leadership can accomplish when molding our youngest Soldiers. CPT (now retired LTG) Legere, SGT Good, MAJ Holly, SSG Kersh, and CPT Wilson… thank you all for taking the time to show me what it meant to be a Soldier and an MI professional. I would also like to thank all of the 1st Team troopers, Phantom Warriors, and Lightning Forward Soldiers who shaped the warrant officer I am today.

What most will likely take away from that list is the lack of any mentioned warrant officers who served as mentors or leaders in my development. Our Army today is much different from the one I grew up in as a young Soldier. I never had the opportunity to work directly for a warrant officer during my enlisted career; even when I decided to pursue becoming a warrant officer, I had to reach out to the greater U.S. Southern Command Joint Intelligence Center to earn a letter of recommendation. Soldiers today will be hard-pressed to serve in an organization without warrant officers—MI or other. It is a testament to the value we bring to the Army. We are leaders, advisors, trainers, integrators, and mentors to the entire force. I challenge each of you to embody these roles each day, as I do myself.

As I assume duties as the chief warrant officer of the branch, I'd like to lead all of us in congratulating CW5 Matt Martin on a successful tour of duty as the 6th Chief Warrant Officer of the MI Corps and his subsequent retirement from active duty. CW5 Martin has worked tirelessly to put our cohort on a path to increased proficiency in executing our core competencies of intelligence analysis; operations; synchronization; and processing, exploitation, and dissemination (PED). To name only a few, CW5 Martin—

- Led the effort along with our teammates at U.S. Army Forces Command (FORSCOM), U.S. Army Intelligence and Security Command (INSCOM), U.S. Army Special Operations Command (USASOC), and Human Resources Command (HRC) to adjust our grade plates across the force, ensuring balance and healthy life-cycle sustainment.
- Established the Distributed Common Ground System-Army Initiatives Group and Digital Information Systems Master Gunner course to increase proficiency in supporting ground force commanders with intelligence at the speed of mission command.
- Established the framework for how we conduct talent management to support commanders and senior intelligence officers and how we select our very best for attendance in our MI programs moving forward.

Thank you, Matt. We are better off for your efforts!

Like all of you, I too have a boss….his priorities are my priorities. Those priorities fall into the following lines of effort: training and education, capability development, organization and workforce development, and communication and strategic messaging. In conjunction with the Warrant Officer Training Branch, we will continue to build upon the world-class education each of our warrant officers receives during the Warrant Officer Basic Course, Warrant Officer Advanced Course, Warrant Officer Intermediate Level Education, and Warrant Officer Senior Service Education. This will ensure commanders and senior intelligence officers have capable and ready MI professionals grounded in doctrine and skilled in executing the intelligence warfighting function's core competencies, specifically focused on large-scale combat operations.

The focus of this issue lends itself to the second line of effort—capability development. MI warrant officers play a critical role in the development of solutions to our most critical capability gaps. We will work to improve lines of communication and transparency between those of you in the field and the dedicated capability developers resident at Fort Huachuca. While advances in technology will no doubt assist in solving these gaps in the long term, those of you working PED missions, leading Soldiers assigned to a multifunction team, and working with our Five Eyes and other host-nation partners possess invaluable tactics, techniques, and procedures and lessons learned. Right now, your knowledge can inform low- to no-cost doctrine,

organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) solutions!

Talent management is a delicate balance between Army requirements, career progression and development, and individual Soldier (and family) desires. The longer your career lasts as an MI warrant officer, the availability of authorizations by grade decreases—significantly. In the end, it's all about ensuring that commanders and senior intelligence officers are manned with the right warrant officer at the right time. In conjunction with FORSCOM, INSCOM, USASOC, Department of the Army G-2, and HRC, we will continue to ensure our talent management recommendations meet that goal. Simultaneously, we will continue to assess and make recommendations for changes to where our MI warrant officers serve by grade. Additionally, we need to increase our efforts in recruiting the next generation of MI warrant officers. This is a never-ending endeavor; though it is not a call to simply increase the number of applications we input. Never forget that the intent is for "highly qualified" candidates to seek appointment as a warrant officer. Not only should we be looking at those noncommissioned officers who have clearly demonstrated the highly qualified characteristics we are looking for, but also we all ought to be mentoring and shaping those privates first class and specialists who show the early traits that will develop with increased experience and opportunity.

Finally, I intend to find a balance between virtual and in-person presence throughout the force. This is not about personal preference, but deference to the position. Because readiness is the number one priority, I intend to accomplish this by focusing on attending combat training center and Mission Command Training Program/Battle Command Training Program training events. At these events, I will capture lessons learned for future initial military training/professional military education training development. I will also observe, mentor, counsel, and engage leaders and Soldiers where it matters…honing our skills to fight and win!

Again, I am excited and humbled by this opportunity. I look forward to ushering in the next 100 years of our cohort with continued progress and service to our nation!

Always Out Front!

ACCELERATING MULTI-DOMAIN OPERATIONS: EVOLUTION OF AN IDEA

by General Stephen Townsend, Commanding General U.S. Army Training and Doctrine Command

Editor's Note: This article was posted on July 24, 2018, on the TRADOC News Center website at https://tradocnews.org/category/frontpage/soldier-2020/.

Multi-Domain Battle has a clear origin.[1] Stemming from the idea that disruptive technologies will change the character of warfare, it recognizes that the way armies will fight and win wars will also change. It also reflects the desire to replicate the success of AirLand Battle, which is arguably the most significant case of developing a concept and then materializing capabilities across the DOTMLPF spectrum (Doctrine, Organization, Training, Material, Leadership Education, Personnel, and Facilities). Origin stories establish the foundation from which lasting ideas emerge. However, for ideas to have a lasting impact they must evolve.

For Multi-Domain Battle there are two things driving the need to evolve the concept.

First, ideas must evolve to ensure alignment with the strategic direction of the enterprise they serve. The 2018 *National Defense Strategy* lays out the missions, emerging operational environments, advances in technology, and anticipated enemy, threat, and adversary capabilities that the Department of Defense envisions for the foreseeable future.[2] It provides direction for how the joint force must evolve to compete, deter, and win in future armed conflict. To this end, Multi-Domain Battle must reflect this strategy.

Second, when I took the reins of US Army Training and Doctrine Command, I was specifically directed to *"operationalize Multi-Domain Battle"* by building upon the foundation created by my predecessor and accelerating its application. And what I found was an incredible foundation. Gen. Dave Perkins brought together partners across the joint force, driving development of the concept to an articulated idea and a vision of how the army fits into it. The key

players are all here and are committed to building and improving the concept and finding real solutions. The concept is ready to grow.

But for that to happen, we need to confront some of the problems others have noted. Over the last eighteen months that Multi-Domain Battle has been out there for debate, there have been four consistent critiques. Some noted that the idea was "old wine in a new bottle."[3] I think the iPhone analogy[4] articulates why that just isn't true. What the original iPhone *did* wasn't all that new, but *how* the iPhone did it fundamentally changed not just a market, but people's behavior. This is exactly what we seek to achieve with this new concept. Though the domains of warfare (air, land, sea, space, and cyberspace) are not new, how the US armed forces will rapidly and continuously integrate them in the future is new.

Another critique is that this is an Army-only concept.[5] However the Air Force and Marine Corps have been part of MDB from the start and recent reporting from numerous forums has made clear the Army's desire to listen, learn, and include our joint and multinational partners in the development of this idea.[6] Recently the Navy and the Joint Staff have also joined the discussion.

Albert Palazzo's series of articles in the fall of 2017 laid out a clear argument. To be successful, Multi-Domain Battle must translate into radical effects on the US military's culture.[7] The concept must force us to reconsider fundamental tenets, like our industrial-age means of promoting, training, and educating leaders. It must also pull us from the comfort of our tactical-level trenches to develop capabilities that inform up to the strategic level of war.[8] Putting "battle" into the name both confines the possibilities and limits the result.

In battles, combatants can win time and space and they allow one side to take ground but they do not win wars. The world we operate in today is not defined by battles, but by persistent competition that cycles through varying rates in and out of armed conflict. Winning in competition is not accomplished by winning battles, but through executing integrated operations and campaigning. Operations are more encompassing, bringing together varied tactical actions with a common purpose or unifying themes. They are the bridge between the tactical and the strategic.

In my first months of command at Training and Doctrine Command, it became clear that the use of the word "battle" was stifling conversation and growth of the concept. There are three concrete reasons why Multi-Domain Battle evolved to Multi-Domain Operations.

First, if the concept is to be truly joint and multi-service, we need clarity and alignment in how we talk. The Air Force talks of Multi-Domain Operations and Multi-Domain Command and Control, while we talk of Multi-Domain Battle—often covering similar, if not the same, ideas and capabilities. To this point, none of the many people I have talked to, including my predecessor, are wedded to the use of "battle"—it was what fit best in time, place, and circumstances. What they are committed to are the ideas of converging capabilities across the joint force with continuous integration across multiple domains.

Second, we cannot do this alone. The armed services can win battles and campaigns, but winning wars takes the whole of government. It helps the entire effort if our interagency partners are comfortable with and conversant in our warfighting concepts and doctrine. As highlighted to me by a former ambassador at a recent forum, talking in terms of operations instead of battles brings together those who want to get things done—whether they are civilians or the military.

And third, it is never just about the fight. When it comes to combat, there is no one better than the combined weight of the US military and our allies and partners. However, the operating environment is evolving and nation-state–level competition has re-emerged, as evidenced by recent actions by both Russia and China. Our National Defense Strategy highlights the importance of winning the "competition" that precedes and follows conflict. However, our use of "Multi-Domain Battle" seemed to indicate our concept was only for the conflict phase. While there are battles within competition, winning them is pointless if they are in isolation to the larger context of deliberate operations supporting national strategy.

Multi-Domain Battle served its purpose—it sparked thinking and debate and it created a foundation. But what we need now is Multi-Domain Operations, and the next revision of the concept to be released this fall will reflect this change.

Language is important. It conveys meaning. This change is not cosmetic—it is about growing an idea to its greatest potential in order to change the way we fight today and ensure overmatch against our adversaries of tomorrow. To do this we need clarity and alignment across the joint force, whole-of-government inclusion, and perspective that reinforces our need to compete effectively outside periods of armed conflict. Changing the name does not do this by itself, but it communicates a clear vision of what we need to accomplish and where we are headed.

Endnotes

1. Kelly McCoy, "The Road to Multi-Domain Battle: An Origin Story," *Modern War Institute*, October 27, 2017, https://mwi.usma.edu/road-multi-domain-battle-origin-story/.

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

3. Bob Scales, "Battle For Army's Soul Resumes: Lessons From Army After Next," *Breaking Defense*, March 28, 2017, https://breakingdefense.com/2017/03/battle-for-armys-soul-resumes-lessons-from-army-after-next/; and Shmuel Shmuel, "Multi-Domain Battle: AirLand Battle, Once More, with Feeling," War on the Rocks (Texas National Security Network), June 20, 2017, https://warontherocks.com/2017/06/multi-domain-battle-airland-battle-once-more-with-feeling/.

4. Nathan Finney, "Integration in warfare," *The Strategist* (Australian Strategic Policy Institute), 11 October 2017, https://www.aspistrategist.org.au/integration-in-warfare/.

5. Dan Goure, "Will the U.S. Army Tolerate a U.S. Air Force 'Bait And Switch' On J-Stars Replacement?" *The National Interest*, October 10, 2017, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwi2qsDlndbaAhXNz1MKHU-iCg8QFjAAegQIABAo&url=http%3A%2F%2Fnationalinterest.org%2Fblog%2Fthe-buzz%2Fwill-the-us-army-tolerate-us-air-force-bait-switch-j-stars-22662&usg=AOvVaw2CDXpMLqC5k6gW1D7_AUqR.

6. Mark Pomerleau, "In the move to multi-domain operations, what gets lost?" *C4ISRNET*, April 11, 2018, https://www.c4isrnet.com/c2-comms/2018/04/11/in-the-move-to-multi-domain-operations-what-gets-lost/.

7. Albert Palazzo, "Multi-Domain Battle: Meeting the Cultural Challenge," *The Strategy Bridge*, November 14, 2017, https://thestrategybridge.org/the-bridge/2017/11/14/multi-domain-battle-meeting-the-cultural-challenge.

8. Albert Palazzo, "Multi-Domain Battle: Getting the Name Right," *Small Wars Journal*, October 16, 2017, http://smallwarsjournal.com/jrnl/art/multi-domain-battle-getting-name-right.

Header photo: U.S. Army and British Army paratroopers shake hands before jumping from a C-17 Globemaster III over Latvia during Exercise Swift Response 18 June, 2018. (Credit: A1C Gracie I. Lee, U.S. Air Force)

Resetting Intelligence Doctrine

by Ms. Terri M. Lobdell

Introduction

For the past two decades, the U.S. Army and joint force have focused primarily on limited contingency operations against insurgencies and the fight against a global terrorist threat. The possibility of facing a peer threat in nation-state warfare was remote, but now the chances of facing a peer threat are greater because our world has changed. As a result, the Chief of Staff of the Army refocused the U.S. Army to address such a threat. While the U.S. Army must man, equip, and train its forces to operate across the range of military operations, large-scale combat operations against a peer threat represent the most significant readiness requirement.[1] Therefore, Army professionals must be knowledgeable of the new Army doctrine in FM 3-0, *Operations*, and FM 2-0, *Intelligence*. These new doctrinal changes are your future, and command of this doctrinal content will help ensure your credibility with your commanders/superiors, staff members, peers, and subordinates.

In October 2017, the Army released FM 3-0, *Operations*, to reset Army doctrine to focus on large-scale combat operations against a peer threat. "FM 3-0 does not change the Army's foundational operational concept, which remains unified land operations. What it does is better account for the reason behind the operations we conduct to clarify the interrelationship between strategic purpose, planning, readiness, and the tactical tasks assigned to units."[2] FM 3-0 introduces the Army strategic roles (shape, prevent, conduct large-scale ground combat, and consolidate gains) but clearly emphasizes and focuses on conducting large-scale combat operations against a peer threat.

With the release of FM 3-0, the U.S. Army Intelligence Center of Excellence Doctrine Division surged our doctrinal efforts to rewrite ADP 2-0 and FM 2-0 in order to nest them with FM 3-0 and reset Army intelligence doctrine. We viewed this revision of FM 2-0 as an urgent effort that we needed to expedite in order to get FM 2-0 to the field and update our institutional training as quickly as possible. Development of FM 2-0 included—

- Retaining time-tested doctrinal constructs.
- Improving the clarity and updating some portions of our existing doctrine.
- Describing the intelligence warfighting function within the context of FM 3-0.

Figure 1 captures our urgent need to update FM 2-0 and how that need drove the new focus and content in FM 2-0, as well as the fundamentals we maintained with only slight changes. It also shows why the concept of fighting for intelligence became our major point of emphasis for FM 2-0.

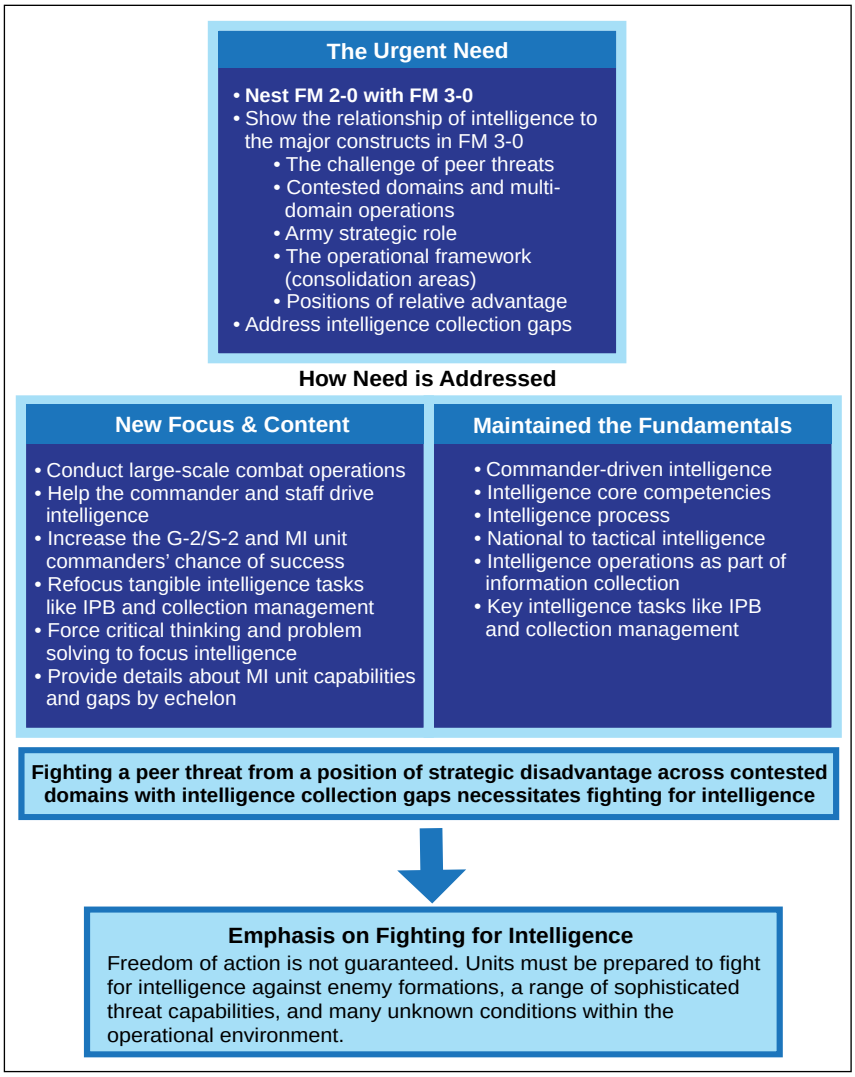


Figure 1. The Why and How of FM 2-0

New Scope of FM 2-0

This version of FM 2-0 is very different from the last version. The last version focused solely on intelligence operations and our contribution to information collection. This version of FM 2-0 represents an important step toward changing the Army culture and improving Army readiness by addressing the fundamentals and tactics associated with intelligence during large-scale combat operations.

FM 2-0 discusses intelligence that is networked, synchronized, and collaborative from national to tactical echelons. It highlights how "intelligence supports the Army operational concept of unified land operations and the conduct of operations. Intelligence supports commanders and decision makers by leveraging national-level to tactical-level capabilities to seize, retain, and exploit the initiative. Intelligence and the intelligence preparation of the battlefield (IPB) process assist in developing an in-depth understanding of relevant aspects of the operational environment and the threat. Based on IPB results, commanders visualize the desired end state and a broad concept of how to shape current conditions into that end state."[3]

Some of the key changes include updating our threat discussion to incorporate peer threats, intelligence across the Army strategic roles, large-scale combat operations and what that means to national to tactical intelligence, and intelligence support to multi-domain operations. Changes also include a new articulation of how intelligence supports the operational framework. While not an entirely new topic, FM 2-0 culminates with a more in-depth discussion on fighting for intelligence to overcome information collection gaps. The rest of this article focuses on a basic discussion of these key topics. However, it is important for intelligence professionals to read FM 2-0 in order to master the basics of Army intelligence and to develop proficiency in our common professional language. Figure 2 shows the structure and location of the key topics in FM 2-0.

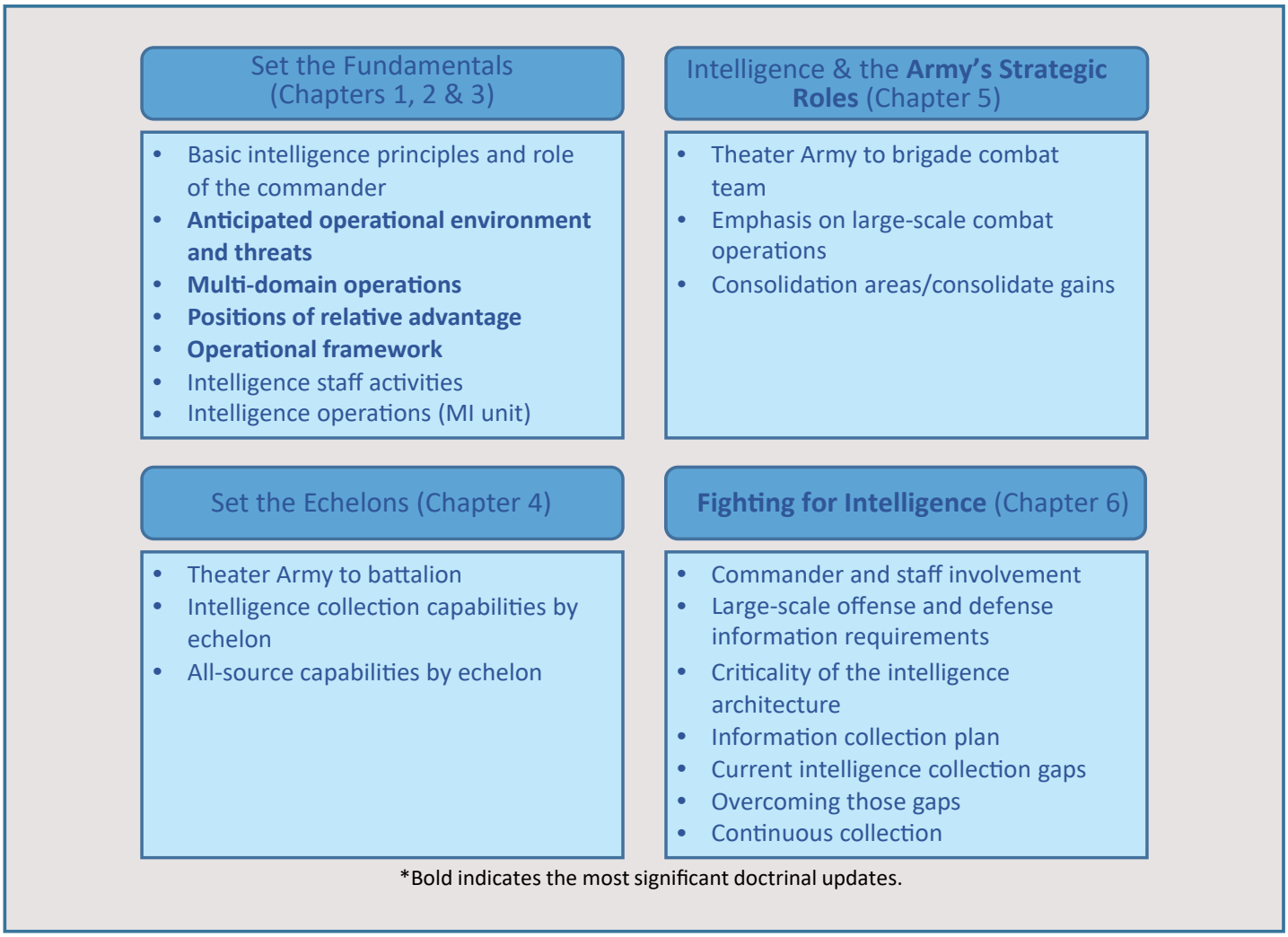


Figure 2. FM 2-0 Structure

Peer Threat

Peer threats are "adversaries or enemies with equal or superior capabilities and capacity to oppose U.S. forces across multiple domains worldwide or in a specific region where they enjoy a position of relative advantage. Some examples include Russia, China, Iran, and North Korea." A peer threat will most likely operate closer to their territory than U.S. forces, employ information warfare well in advance of ground operations, and share a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary. "Peer threats generate tactical, operational, and strategic challenges that are, in order of magnitude, more challenging militarily than those the Army has faced since the end of the Cold War…Peer threats believe they have a comparative advantage because of their willingness to endure greater hardship, casualties, and negative public opinion."[4]

When operating against a peer threat, commanders aggressively conduct decisive action to achieve positions of relative advantage. Intelligence supports the commander by visualizing the threat and detecting possible threat courses of action (COAs).[5] Supported by the most accurate and timely intelligence possible, Army forces must strike a peer threat unexpectedly in multiple domains and from multiple directions, denying freedom of maneuver by creating multiple dilemmas that the enemy commander cannot effectively address.

Army Strategic Roles

"The Army's primary mission is to organize, train, and equip its forces to conduct prompt and sustained land combat to defeat enemy ground forces and seize, occupy, and defend land areas. The Army accomplishes its mission by supporting the joint force in four strategic roles:

- Shape operational environments.
- Prevent conflict.
- Prevail in [Conduct] large-scale ground combat.
- Consolidate gains."[6]

The strategic roles clarify the enduring reasons for which the U.S. Army is organized, trained, and equipped.

"The goal through all four roles is to win. To win, intelligence operations must provide threat warnings, identify threat capabilities, and describe how threat capabilities will be employed and how they will impact friendly operations. This intelligence support must occur across the conflict continuum and through the range of military operations."[7] Each strategic role presents a unique set of intelligence requirements, as shown in Figure 3.

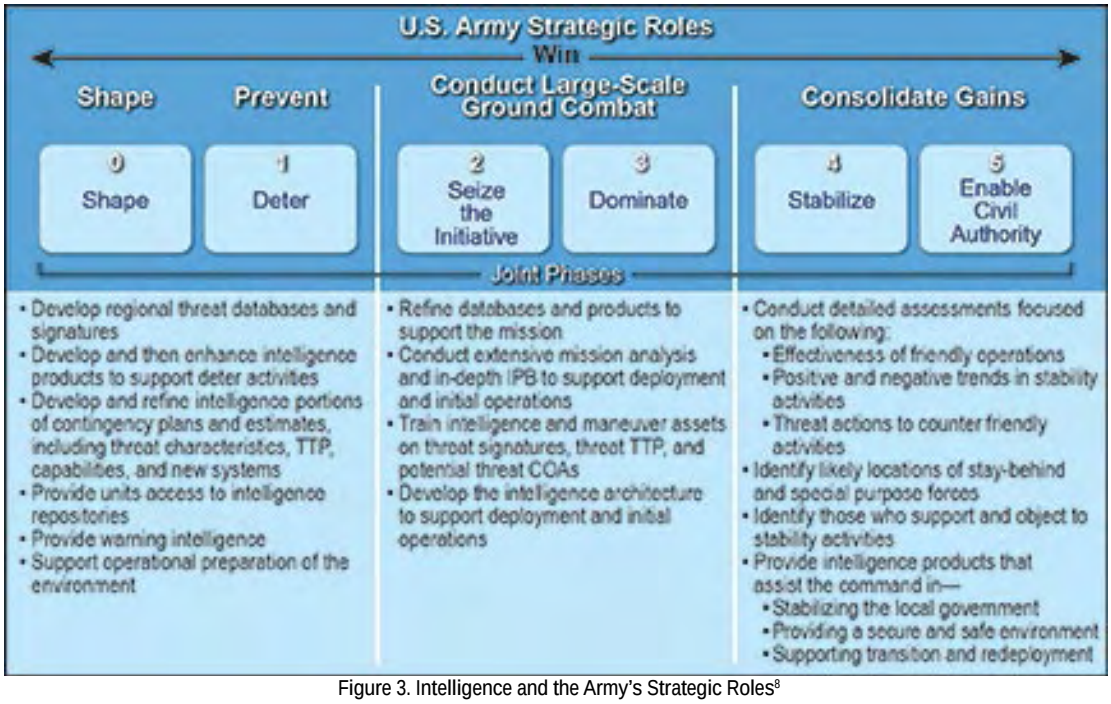


Figure 3. Intelligence and the Army's Strategic Roles[8]

Shape. "Intelligence is integral in supporting operations to shape. During operations to shape, the intelligence staff must establish a baseline intelligence architecture to meet a broad range of requirements. Intelligence products assist the commander in countering actions by adversaries that challenge the stability of a nation or region and are contrary to U.S. interests. Intelligence provides the commander the ability to detect adversary warnings, analyze enemy intentions, and track enemy capabilities across all domains to inform decisions and realistic assessments of operational and tactical risk."[9]

Prevent. "The intelligence staff increases its knowledge of the threat and the specific operational environment, and it expands various intelligence capabilities as part of the intelligence architecture. With the shift from shaping to deterrence [prevention of conflict], the theater army shifts to refining contingency plans and preparing estimates for increasing ground forces and capabilities."[10]

Conduct Large-Scale Ground Combat. "During large-scale combat, intelligence operations are continually conducted

to provide commanders and staffs the detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute unified land operations. This intelligence supports the unit's battle rhythm, such as commander update briefs and various staff processes. The demands of large-scale combat operations consume all staff elements." [11] Another complexity of large-scale combat operations is the many simultaneous intelligence requirements spanning operations in the deep, close, support, and consolidation areas.

During large-scale combat operations, commanders designate a portion of their area of operations (AO) as a consolidation area to facilitate the security and stability tasks necessary for the freedom of action of the maneuver force. While somewhat confusing, this is different from the role of consolidate gains that is aligned with the joint phasing model of stabilize and enable civil authority (discussed below).

"Intelligence during consolidate gains primarily supports maintaining the momentum of battle across the AO. Establishing security and a limited amount of stability within the consolidation area may necessitate the augmentation of existing information collection capabilities as well as unique solutions to answer difficult requirements… Intelligence staffs in the consolidation area focus on" stay-behind or bypassed forces, "other threats, hazards, and, at times, key civil considerations in the consolidation area. These threats may range from insurgent groups infiltrating rear areas to hybrid or proxy forces with technologically advanced systems used to exploit vulnerabilities behind close battle areas. [Military intelligence] MI units in the consolidation area conduct a multitude of tasks."[12]

Consolidate Gains. The Army strategic role of consolidate gains makes enduring any temporary operational success and sets the conditions for a stable environment allowing for a transition of control to legitimate authorities. Consolidation of gains occurs in portions of the AO where large-scale combat operations are no longer occurring. "During operations to consolidate gains, intelligence plays an important role in assessing the environment to—

- Detect both positive and negative trends.
- Determine the effectiveness of friendly operations.
- Identify actions that could threaten hard won gains.

Essentially, this focuses the intelligence effort on situational understanding, warning intelligence, and support to force protection, as well as assists in determining termination criteria or when it is operationally acceptable to transition from large-scale combat operations."[13]

Large-Scale Combat and What it Means to Intelligence

"Producing intelligence and executing information collection differ significantly based on the Army strategic role… Of the four Army strategic roles…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."[14]

Multi-Domain Operations

"The interrelationship of the air, land, maritime, space, cyberspace, the information environment, and the [electromagnetic spectrum] EMS requires cross-domain situational understanding of the operational environment. Commanders and staffs must understand friendly and enemy capabilities and vulnerabilities that reside in each domain. From this understanding, commanders can better identify windows of opportunity during operations to converge capabilities for the best effects. Since many capabilities are not organic to Army forces, commanders and staffs plan, coordinate for, and integrate joint and other unified action partner capabilities in a multi-domain approach to operations. Intelligence plays an important role in situational understanding across all domains.

The Army conducts operations across all domains and the information environment. All Army operations are multi-domain operations and all battles are multi-domain battles. A multi-domain approach to operations is neither new to the Army nor to national to tactical intelligence. Rapid and continued advances in technologies and the military application of new technologies to the space domain, the EMS, and the information environment…require special considerations in intelligence, planning, and converging effects from across all domains."[15]

"During IPB, each staff element provides input, ensuring a holistic view of the operational environment. Subsequently, the IPB effort aids in identifying domain windows of opportunity to exploit threat vulnerabilities. For example, the air defense artillery staff element's input to IPB about enemy

integrated air defense system (IADS) capabilities and vulnerabilities may present the friendly commander with recommended timeframes and locations to conduct suppression of enemy air defense or deep strike. Additionally, the gaps identified during mission analysis and IPB will drive information collection requirements. The results of information collection may also identify domain windows of opportunity."[16]

The joint force isolates portions of the operational environment in one or more domains to allow a portion of the joint force to establish a decisive point for the cross-domain convergence of capabilities, which must be supported by continuous intelligence operations across the domains. "During large-scale combat operations against a peer threat, ground-force commanders may be required to conduct tactical activities, such as a deliberate attack, to shape the environment to gain a position of relative advantage for activities, such as joint fires, within the other domains. Once that position is achieved, operations would continue to increase the position of advantage in order to create a longer window of superiority [opportunity] to facilitate follow-on missions and operations across the domains,"[17] as shown in Figure 4.

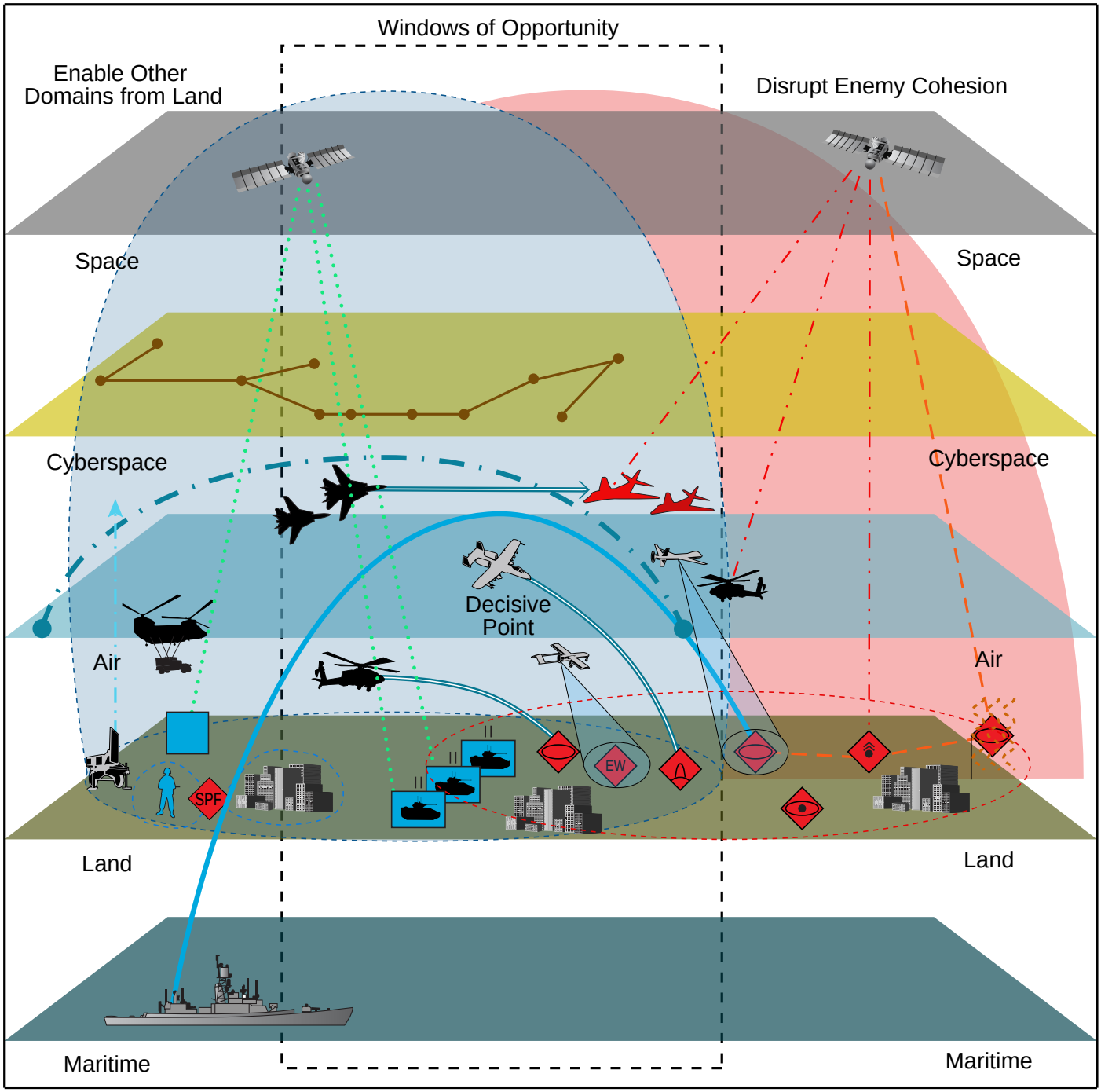


Figure 4. Windows of Opportunity in a Multi-Domain Extended Battlefield[18]

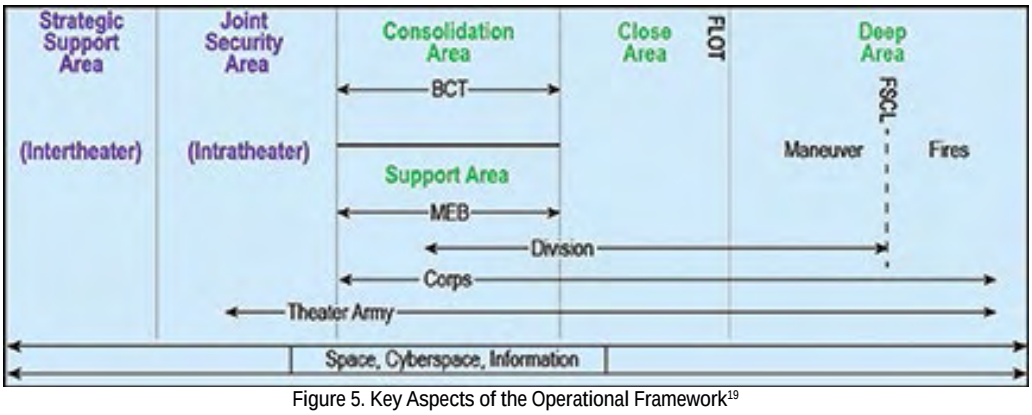


Figure 5. Key Aspects of the Operational Framework[19]

Operational Framework

"An *operational framework* is a cognitive tool used to assist commanders and staffs in clearly visualizing and describing the application of combat power in time, space, purpose, and resources in the concept of operations."[20] "Within the operational framework, commanders are assigned AOs, they designate the physical arrangement of forces on the battlefield, further articulate an operation in terms of purpose, and designate main and supporting efforts."[21] An important change in FM 3-0, which FM 2-0 reinforces, is the change to the physical arrangement of an AO by designating the close, deep, support, and consolidation areas, as shown in Figure 5.

FM 3-0 also identified four "operational framework considerations (physical, temporal, virtual, and cognitive) [to] provide commanders and staffs a way to look at multiple domains and the information environment within the context of land operations. The G-2/S-2 assists the commander and staff in understanding and accounting for these considerations through a number of processes and different types of intelligence products.

Intelligence is inherent in all staff planning activities. The IPB process provides information for most of the operational framework considerations to support long-term and short-term operational planning. During IPB, the intelligence staff leads the rest of the staff through the IPB process to thoroughly identify significant aspects of the operational environment, analyze how these aspects affect operations, and identify enemy COAs.

A thorough IPB and intelligence analysis assist each echelon in focusing operations on all significant aspects of the operational environment in time and space across multiple domains. This prevents each echelon from focusing only on the close fight and current operations. A broad focus across the operational framework considerations assists commanders and staffs in better identifying friendly windows of opportunity and threat windows of vulnerabilities within and across each domain and the information environment. This illustrates one way that intelligence is critical to operational planning."[22] Figure 6 shows a list of the operational framework considerations, as described in FM 3-0, and how IPB and subsequent intelligence analysis support each consideration.

Operational framework considerations	*IPB and intelligence analysis support*
Physical considerations include geography, terrain, infrastructure, populations, distance, weapons ranges and effects, and known enemy locations.	• Intelligence support begins well before the deployment of forces, through the generate intelligence knowledge intelligence warfighting task, which addresses the operational variables (PMESII-PT). Information gained during generate intelligence knowledge is used by commanders and staffs to assist in framing the operational environment during the Army design methodology. • IPB provides detailed analysis of the mission variables of enemy, terrain, weather, and civil considerations to determine their effects on operations. • IPB and intelligence analysis assist in determining relevant aspects within an area of operations—such as civil considerations characteristics (ASCOPE)—that are critical in determining how friendly operations may be impacted during the consolidation of gains. • Intelligence analysis is critical to the designation of a deep area, the fire support coordination line, and an engagement area.
Temporal considerations are related to time, including when capabilities can be used, how long they take to generate and employ, and how long they must be used to achieve desired effects.	• IPB is a process that is both geographically and temporally specific. • Developing threat courses of action during IPB is based on identifying threat objectives, goals, timelines, and end states. • IPB provides a temporal context using rates of movement, time phase lines, phases of enemy fires, and other templates to capture enemy timing.
Cognitive considerations relate to people and how they behave. They include information pertaining to enemy decision making, enemy will, the Nation's will, and the population's behavior.	• IPB accounts for aspects associated with the center of gravity and the enemy's morale and willingness to continue operations. • Intelligence support to continuous operational assessments considers many relevant aspects of the operational environment, including sociocultural factors. • IPB also considers all significant aspects of the operational environment associated with the various civil considerations.
Virtual considerations pertain to activities and entities, both friendly and threat, residing in cyberspace.	• IPB and intelligence analysis, in coordination with the cyberspace electromagnetic activities section, provide intelligence on the threat's likely activities within the information environment, which includes cyberspace.
ASCOPE areas, structures, capabilities, organizations, people, and events IPB intelligence preparation of the battlefield PMESII-PT political, military, economic, social, information, infrastructure, physical environment, and time	

Figure 6. IPB and Intelligence Analysis Support to Operational Framework Considerations[23]

Fighting for Intelligence

Fighting for intelligence, while not completely new, is a strong articulation of the many challenges we face during information collection against a peer threat and how to overcome the challenges. 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.

"Operational success requires a successful intelligence effort. Fighting for intelligence encompasses the basics of establishing an effective intelligence architecture, synchronizing the intelligence warfighting function, and planning and conducting information collection. The commander and staff need to understand the doctrinal fundamentals of fighting for intelligence and maintain proficiency in integrating the intelligence warfighting function into operations."[24]

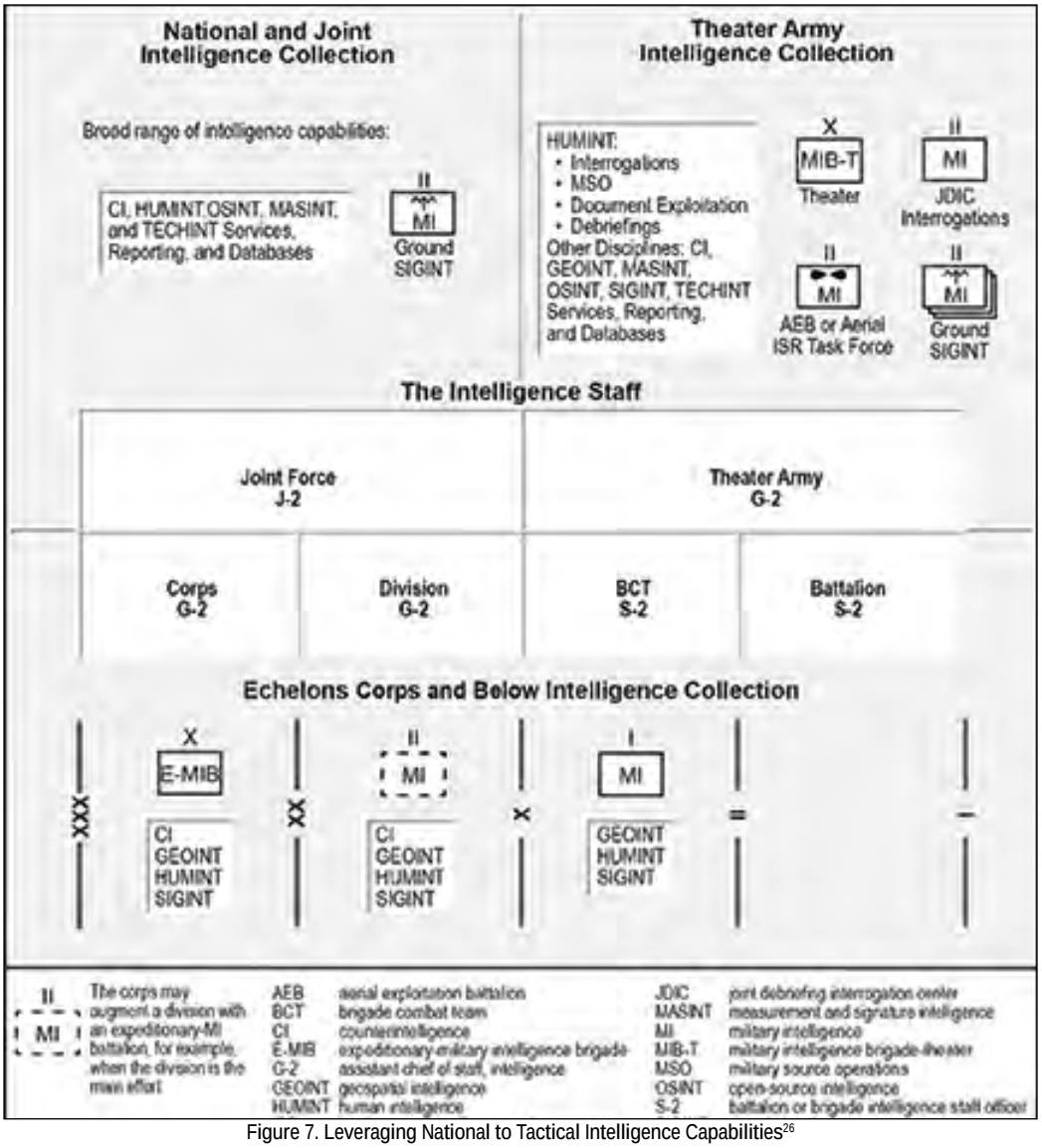


Figure 7. Leveraging National to Tactical Intelligence Capabilities[26]

"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."[25]

Intelligence Architecture

"The intelligence architecture begins with understanding intelligence capabilities. Intelligence capabilities broadly fall into the categories of intelligence collection capabilities (by intelligence discipline) and all-source intelligence capabilities. However, understanding capabilities is more complex than simply knowing the broad categories. Each intelligence collection capability comprises specific collectors/collection platforms with one or more specific capabilities or associated sensors."[27]

FM 2-0 provides a "general list of the organic and supporting intelligence collection and all-source intelligence capabilities by echelon." It highlights that "each echelon receives and depends on intelligence from higher and lower echelons and lateral units. They can receive this intelligence through various means on a number of different networks." Figure 7 "illustrates how leveraging national to tactical intelligence capabilities can support tactical operations down to

the [brigade combat team] BCT level through organic and supporting collection, as well as dissemination through intelligence broadcast dissemination systems and other intelligence systems, such as [Distributed Common Ground System-Army] DCGS–A, down to the battalion level."[28]

Information Collection Gaps

"Commanders and staffs use the principles of information collection, IPB and other key staff products, and knowledge of information collection capabilities and limitations to develop the information collection plan."[29] The fight for intelligence is difficult because friendly forces must contend with peer threat long-range and precision fires, cyberspace and electronic warfare capabilities, deception and threat counter-measures, counter reconnaissance forces, and especially in some situations, threat IADS. Intelligence collection gaps often occur due to—

- Peer threat advanced capabilities (e.g., IADS, cyberspace, and electronic warfare).
- Rules of engagement.
- Insufficient networks, systems, or personnel/linguists.
- Lack of technical capabilities.
- A high operating tempo and constant maneuver.
- Threat countermeasures.
- Unacceptable risk for the employment of specific assets.
- Unfavorable terrain.
- Movement in preparation for operations.[30]

Overcoming Gaps and Continuous Information Collection

"Information collection and intelligence analysis are integral to developing the situation. The intelligence staff conducts synchronizing activities to assist the unit in developing the situation and adjusting information collection. There are many requirements for the G-2/S-2 and rest of the intelligence staff to participate in unit battle rhythm activities to synchronize intelligence support and the information collection effort. The intelligence staff provides updates on the situation and briefs changes to the information collection plan during various commander updates, boards, cell meetings, and other meetings. Additionally, the corps and division intelligence staffs may attend or watch theater-level collection management boards, giving them insight into national and joint priorities and coverage. This insight, coordination, and preparation create opportunities for tactical units to leverage national and joint capabilities.

The theater army, corps, and division G-2s convene an operations and intelligence working group, or some form of synchronization meeting, with key staff and subordinate units. These intelligence synchronization meetings (normally conducted via video teleconferencing) create a common understanding of the enemy, ensure information collection plans address changes in the situation, and coordinate continuous information collection across echelons and units.

For example, the G-2 might anticipate an enemy unit designated as an [high-payoff target] HPT will cross a key phase line in the next 24 to 48 hours. The predicted movement of the HPT could cause the corps G-3 and G-2 to coordinate with the division G-3 and G-2 to ensure there is continuous tracking of the HPT with no loss of coverage. During the intelligence synchronization meeting, the corps G-2 and division G-2 could coordinate or adjust an intelligence hand-over line to ensure continuous coverage of the HPT. Another information collection technique is to coordinate for complementary/supporting coverage. For example, the theater army could simultaneously conduct suppression of enemy air defense and [unmanned aircraft system] UAS collection for the corps while the HPT moves into a corps deep engagement area. At the BCT and battalion levels, there is no requirement for an operations and intelligence working group but the operations and intelligence staff must still synchronize intelligence support and the information collection effort.

Information collection is continuous through the execution of operations and transition to consolidate gains. The all-source analytical effort is key to informing the commander and staff, who in turn support the continued fight for intelligence. Therefore, G-2/S-2s, all-source analysts, and collection managers must collaborate closely. Intelligence analysis assists in discovering collection gaps, generating more information requirements, and driving all operations. As with initial planning, information collection requirements can be answered immediately or designated as [priority intelligence requirements] PIRs by the commander or validated as information requirements in order to drive information collection. Additionally, analysis assists in determining the effectiveness of the information collection effort. That assessment leads to adjustments in the information collection plan, making it more efficient and effective. Thorough planning allows continuous collection planning through all phases, branches, and sequels of an operation."[31]

Conclusion

FM 2-0 now nests closely with FM 3-0, as shown in the logic chart in Figure 8. The left side of the figure contains the FM 3-0 logic chart in its entirety except for some wording at the bottom of the chart. On the right side are all the various intelligence doctrinal concepts that align to support operations.

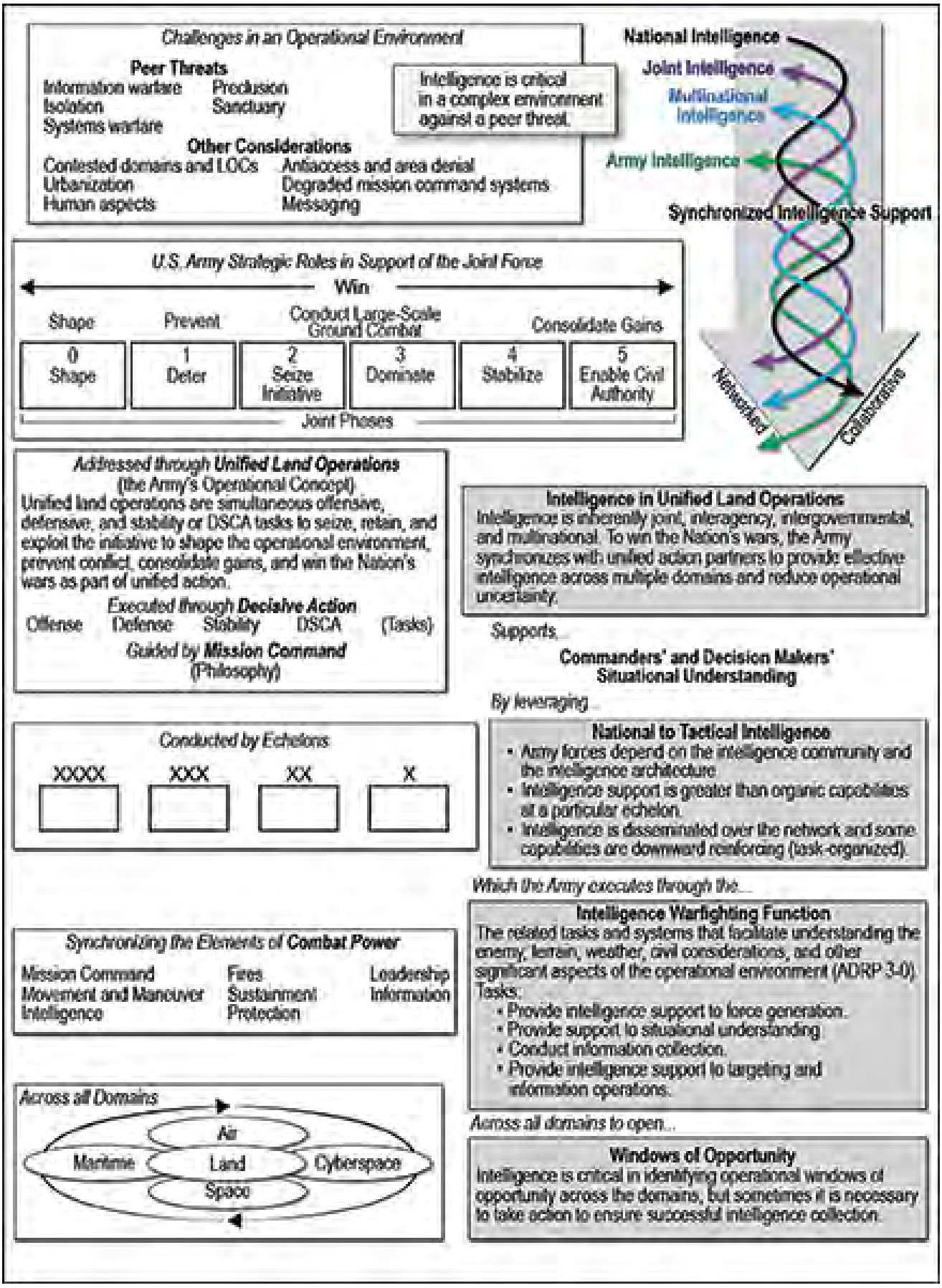


Figure 8. FM 2-0 Logic Chart[32] (Continued on next page)

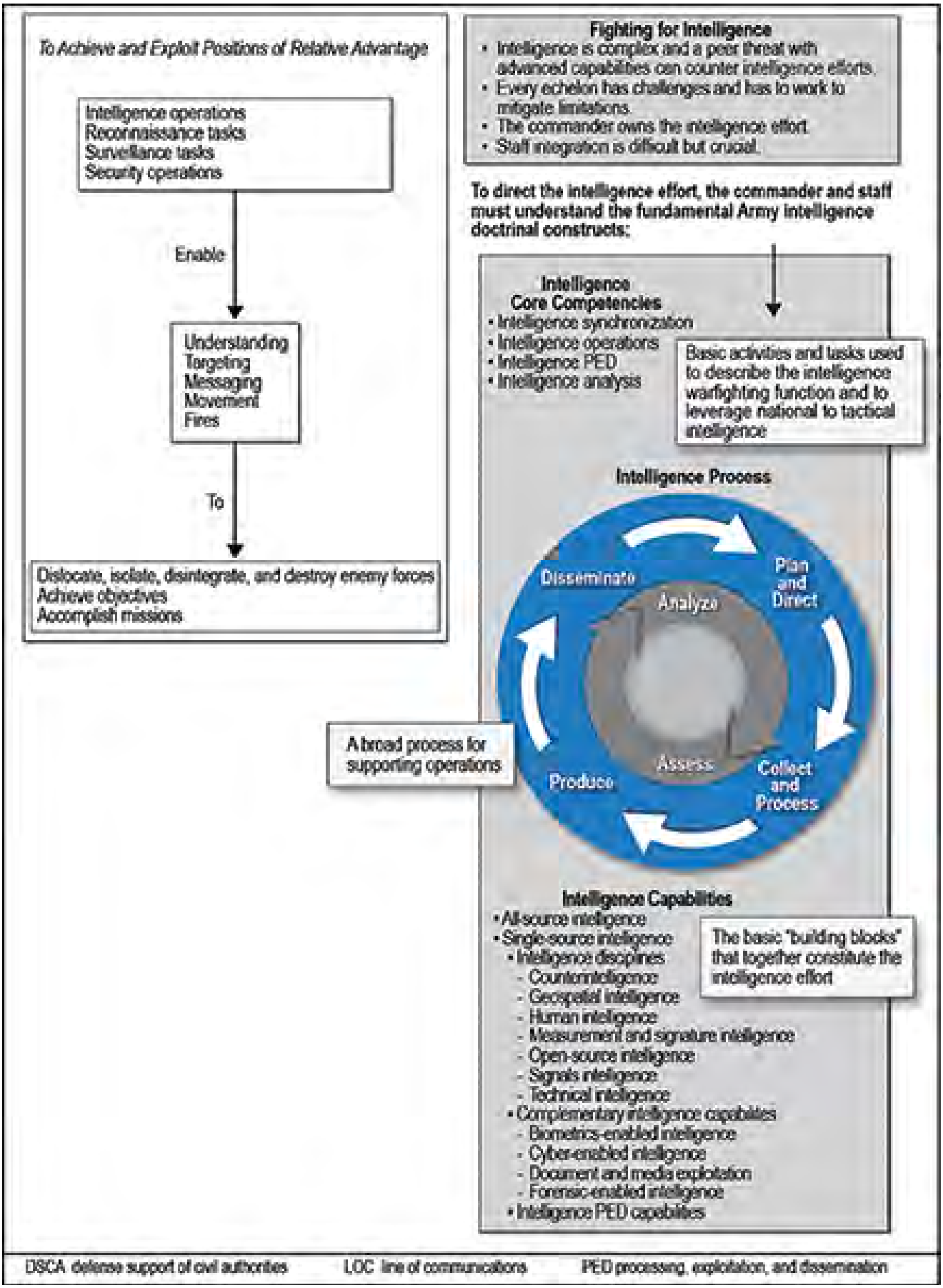


Figure 8. FM 2-0 Logic Chart

FM 2-0 provides clear doctrine on how—

- Army forces operate and develop intelligence as a part of a joint team and in conjunction with unified action partners.
- Intelligence as a warfighting function operates using current Army capabilities and units in today's operational environment.
- Intelligence is critical in a complex operational environment against a peer threat.
- Commanders and staffs need timely, accurate, relevant, and predictive intelligence to understand threat characteristics, goals and objectives, and COAs 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 a detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics to plan for and execute unified land operations.

For a more in-depth understanding of the change to the organizational construct of Army operations you can view LTG Lundy's discussion of FM 3-0 and large-scale combat operations at https://www.youtube.com/watch?v=JZcdvwKyTU4&t=519s.

Endnotes

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

2. Mike Lundy and Rich Creed, "The Return of U.S. Army Field Manual 3-0, Operations," *Military Review* (November-December 2017), https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/The-Return-of-US-Army-Field-Manual-3-0-Operations/.

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

4. Ibid., 1-19.

5. Ibid., 5-6.

6. Ibid., 1-19.

7. Ibid.

8. Ibid., 1-21.

9. Ibid., 5-3.

10. Ibid., 5-5.

11. Ibid., 5-6.

12. Ibid., 5-15.

13. Ibid., 5-18.

14. Ibid., 6-1.

15. Ibid., 1-16.

16. Ibid., 1-17.

17. Ibid.

18. Ibid., 1-18.

19. Department of the Army, FM 2-0, *Intelligence*, 1-15.

20. Department of the Army, Army Doctrine Publication 1-01, *Doctrine Primer* (Washington, DC: U.S. GPO, 2 September 2014), 4-8.

21. Department of the Army, FM 3-0, *Operations*.

22. Ibid., 1-13–1-14.

23. Ibid., 1-14.

24. Ibid., 6-1.

25. Ibid., 6-1–6-2.

26. Department of the Army, Army Doctrine Publication 2-0, *Intelligence* (DRAFT), 2-10.

27. Ibid., 6-10.

28. Ibid., 6-11.

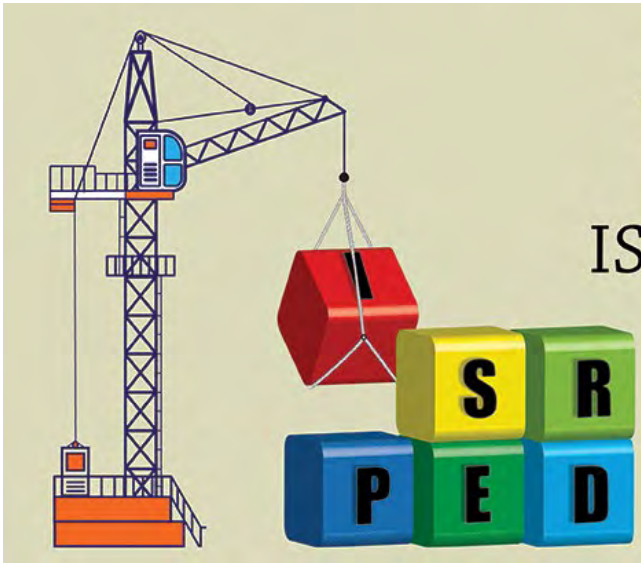
29. Department of the Army, FM 2-0, *Intelligence,* 6-13.

30. Ibid.

31. Ibid., 6-17–6-18.

32. Ibid., viii.

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



Assembly Required: The Building Blocks of ISR and PED Architectures

by Mr. John DellaGiustina, Mr. William Donner, and Chief Warrant Officer 3 Otis Griffin III

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

***–ADRP 2-0,* Intelligence**

Introduction

In December 2014, senior military intelligence (MI) leaders designated processing, exploitation, and dissemination (PED) as the fourth core competency of the intelligence warfighting function based on the significant amount of Army personnel, training, and resources dedicated to this key function. Although the MI Corps has made substantial progress implementing intelligence PED solutions since 2014, the Army's transition to focus on large-scale combat operations has revealed additional challenges that must be resolved to integrate the PED core competency across the force.

One major issue in integrating PED capabilities has been the need to establish the requisite architectures that seamlessly link the Army's intelligence, surveillance, and reconnaissance (ISR) assets to PED and intelligence analysis centers with supported mission command nodes. Identifying architecture shortfalls is critical in optimizing MI support to dynamic large-scale combat operations. The need to implement vertically and horizontally integrated PED architectures using common data links, networks, and interfaces for similar capabilities within and across intelligence disciplines summarizes this shortfall.[1]

In March 2018, the U.S. Army Intelligence Center of Excellence (USAICoE) hosted the Intelligence Senior Leaders Conference (ISLC) to address and resolve high-risk MI gaps in large-scale combat operations support. One focus area included a briefing and breakout session describing how the Army's ISR and PED architectures ingest collected data and exploit information that answer commanders' priority intelligence requirements in specified theaters of operations. The session developed a common understanding of an ISR and PED architecture framework for planning and integrating intelligence operations into specified geographic combatant command/Army Service component command theaters of operations.

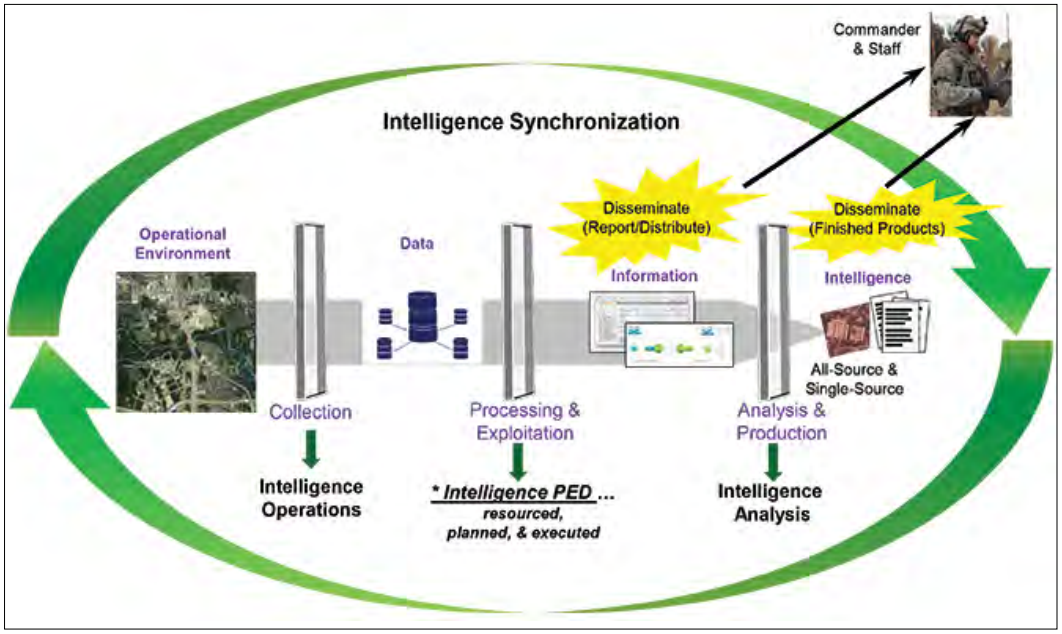


Figure 1. Intelligence Core Competencies

The purpose of this article is to describe the ISR and PED architectures that feed the broader intelligence architecture and inform supported commanders' situational understanding of the operational environment. To start, however, we summarize the evolution of the Army and ISR PED enterprise to highlight the need for intelligence leaders and planners to focus on developing architectures that support commanders' operational priorities.

Background—Recent Evolution of the Army ISR and PED Enterprise

PED is a widely used term that describes the process the U.S. military employs to convert data gathered by ISR assets into relevant information and intelligence useful to commanders, staffs, and intelligence analysts. Senior leaders at the Joint Staff, Service, and operational commands commonly refer to PED as a major consideration in determining if existing or emerging ISR capabilities are able to satisfy commanders' information needs in a timely and accurate manner.

Boots-on-the-ground reductions and a substantial increase in intelligence collection platforms, sensors, and their technological capabilities over the past decade have driven Army intelligence leadership to transition PED from a platform-centric capability to a holistic enterprise strategy. Although it remains best to tie a base capacity of PED resources directly to the collection asset they support, improvements in architectures and the need to colocate high-demand, low-density PED personnel to support multiple missions have led to the consolidation of Army PED capabilities at several key nodes.

In November 2014, a USAICoE-led capabilities portfolio review of PED provided a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) assessment to the Department of the Army's leadership panel. The assessment recommended major PED solutions across multiple domains in the near, mid, and far term to support objectives of the Army's future force. In parallel with the PED capabilities portfolio review, the Department of the Army G-2 published the *United States Army Processing, Exploitation, & Dissemination Concept of Operations* in December 2014. The document outlines the Army's PED strategy to support commanders from expeditionary, reach, and home station/combat training center locations. The Army staff then developed the Army PED execute order to implement solutions from the capabilities portfolio review, in addition to developing the PED concept of operations with formal tasks to the Army's major commands. In August 2015, the Department of the Army G-3 released the execute order delineating tasks and coordinating instructions as the initial roadmap for conducting Army PED operations, including reach architecture requirements.

One institutional accomplishment was the inclusion of dedicated PED personnel and equipment into the force structure of both the corps expeditionary-MI brigades and the U.S. Army Intelligence and Security Command's (INSCOM) 116th MI Brigade (Aerial Intelligence). As the primary tactical intelligence organization with an organic PED capacity, the expeditionary-MI brigade performs expeditionary operations in support of echelons corps and below units based on mission priorities. The 116th MI Brigade, headquartered at Fort Gordon, Georgia, plans and executes manned and unmanned aerial ISR missions and PED support for theater and Department of Defense (DoD) global requirements.

Another significant achievement was incorporating PED principles into Army doctrine. In addition to designating it a core competency, MI Corps leadership approved the definition of PED and incorporated it into the updates to ADP/ADRP 2-0, *Intelligence*, and ADRP 1-02, *Terms and Military Symbols*. To mirror joint intelligence doctrine, "collect and process" was added as a distinct step in the Army intelligence process. A PED MI Publication is pending approval, as is an appendix titled "Integrating Collection and PED Architectures" for an update to MI Publication 2-01.2, *Intelligence Architecture*. For the first time in one document, this appendix captures the multiple building blocks necessary to establish viable expeditionary and/or reach PED architectures in support of warfighting commanders.

INSCOM established its aerial ISR PED center at Fort Gordon in late 2013 to consolidate intelligence PED resources to support global mission sets from reach. Using Distributed Common Ground System-Army (DCGS–A) fixed site systems, INSCOM established the Army Global PED Center to centralize disparate worldwide aerial ISR PED operations. After the Army published its PED execute order in 2015, INSCOM designed and implemented an architecture to extend the PED enterprise to corps and Reserve Component PED nodes. From these locations, the U.S. Army Forces Command's expeditionary-MI brigade PED capacity can be allocated to support corps and below PED priorities, such as division combat aviation brigade Gray Eagle geospatial intelligence and terrestrial signals intelligence (SIGINT) PED operations. Initially, 12 of the 24 Active Component expeditionary-MI brigades' PED platoons were stationed at Fort Gordon, but with the installation of dedicated terrestrial circuits, the remaining 12 expeditionary-MI brigades rotated back to their parent corps' expeditionary-MI brigade sites in mid-2018.

Building Blocks of ISR and PED Architectures

The focus of the ISLC briefing was to describe the multiple building blocks that together comprise ISR and PED architectures. As delineated below, eight primary capabilities, each with several components, must be integrated to build the MI unit architectures necessary for intelligence operations support to mission command:

- **Collection Asset Communications:** tactical radios, line-of-sight and beyond-line-of-sight datalinks, PED/CrewCom (chat, voice), and Blue Force Tracker.
- **Sensor Processing Ground Stations:** Universal Ground Control Station, Tactical Intelligence Ground Station, Operational Intelligence Ground Station, and DCGS–A Intelligence Processing Center Version 2.
- **Expeditionary PED Locations:** supported unit command post, brigade combat team, combat aviation brigade/Gray Eagle company, division, corps, and 116th MI Brigade/Theater airfield.
- **Sensor Data Transport Capability Options:** Warfighter Information Network-Tactical (WIN–T), INSCOM Operational Intelligence Ground Station satellite communications, theater-provided solutions, and TROJAN data network.
- **Army and DoD/Defense Information Systems Agency (DISA) Communications Hubs:** WIN–T regional hub nodes, DISA teleports/gateways, Defense Enterprise Computing Center sites, and DISA-leased terrestrial fiber.
- **PED Service Centers/Converged Infrastructure:** Fort Gordon, Georgia; Europe; Pacific—all with DCGS–A Intelligence Processing Center Version 1 software; and TROJAN data network for routing terrestrial information.
- **Reach PED Nodes—INSCOM, U.S. Army Forces Command, U.S. Army Special Operations Command, Combat Support Agency:** Fort Gordon, area exploration battalion locations; expeditionary-MI brigade sites; corps, U.S. Army Reserve, and Army National Guard locations; and special operations forces PED node.
- **Dissemination Methods:** broadcast, push time-sensitive reporting, post products (e.g., Geospatial Intelligence Enterprise Tasking, Processing, Exploitation, and Dissemination Services), and archive for accessibility and discoverability.

Understanding the capabilities and technical capacity of each system listed in these components is necessary to plan and coordinate the architecture required to support ISR and PED operations. Many systems offer similar or redundant capabilities to satisfy architecture requirements and thus offer multiple options for developing primary and alternate means of routing collected sensor data to designated PED node(s).

One key PED architecture initiative has made considerable progress in forging consensus across the Army—the U.S. Army Training and Doctrine Command's PED tasking order. The order fostered collaboration between the USAICoE PED Team, U.S. Army Cyber Center of Excellence, U.S. Army Aviation Center of Excellence, INSCOM, and U.S. Army Special Operations Command to determine the requirements and develop recommended solutions for the Army's aerial sensor data transport capability gaps. Recommendations from the Gray Eagle and PED capabilities portfolio review led to a decision briefing to analyze courses of action for the Army's three Gray Eagle formations that have a common and dedicated expeditionary capability to transport sensor data to designated intelligence PED nodes.

In May 2016, the commanding general of the U.S. Army Cyber Center of Excellence endorsed a program of record solution—a pooled expeditionary signal brigade WIN–T capability (consisting of the upgraded command post node and satellite transportable terminal)—as a bridging strategy to support Gray Eagle data transport. Additionally, during the two 2017 MI-cyberspace home-on-home sessions, senior MI leaders directed an end-to-end architecture analysis assessment across the existing ground station, satellite communications terminals, PED service center, regional hub nodes, and terrestrial architectures. The stakeholder consensus led to publishing the Army's *Aerial Sensor Data Transport Concept of Operations* to serve as the basis for integrating new capabilities that satisfy end-to-end Army ISR and PED architecture requirements, including a four-part,

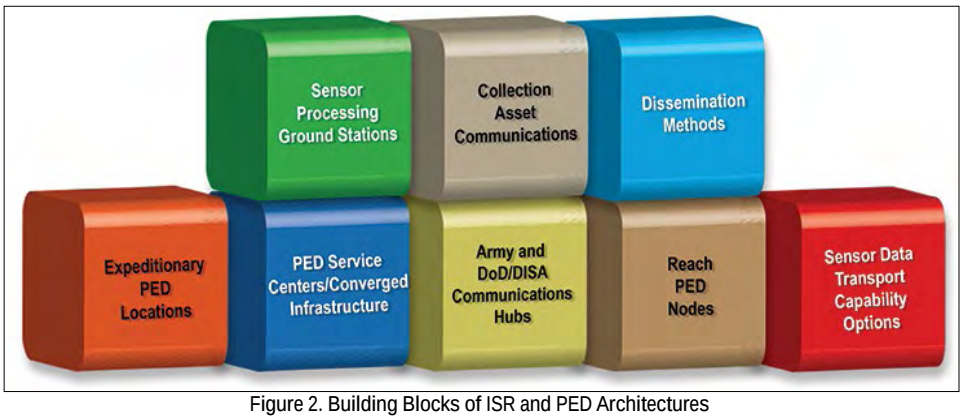


Figure 2. Building Blocks of ISR and PED Architectures

near-term funding request to resolve current architecture needs.

Lessons—Transition of PED Operations from Steady-State to Large-Scale Combat Operations

One of the Department of the Army G-2's modernization imperatives is to expand and evolve PED. During ISLC's breakout session to discuss the Korean and European theaters, it became apparent that steady-state (phase 0/1) and major contingency operations (phase 2/3) architectures may be much different from one another as a theater transforms to support large-scale combat operations. To address this, the following framework was devised to understand the distinction between the PED architectures in each. The framework provides an Army PED operations concept to transition from a phase 0/1 focus to large-scale combat operations support.

Figure 3. Army Strategic Roles and their Relationship to the Joint Phases[2]

Phases 0 and 1 primarily use reach PED operations based on a deliberate planning process to establish the architecture necessary to support "steady-state" DoD and combatant command ISR and combat aviation brigade globally validated requirements. These end-to-end ISR and PED architectures use a mix of INSCOM, Army, and theater-provided communications capabilities as delineated in the previous section titled "Building Blocks of ISR and PED Architectures."

During phases 2 and 3, PED for the terrestrial, aerial, and space layer ISR capabilities that support multi-domain operations will transition to a focus on expeditionary PED operations to provide a flexible and dedicated capacity for forward-deployed warfighters. The 116th MI Brigade and corps expeditionary-MI brigade PED elements can deploy to locations in the theater army area of operations that optimize support to the designated coalition joint task force and land component command operational priorities and main effort. Deployment of the PED elements will depend on the ISR and PED architecture established during "set the theater" activities.

These expeditionary PED operations minimize the operational risk to deployed warfighters in two key ways:

- The expeditionary PED force structure attached to, or in direct or general support of, commanders provides a dedicated and flexible capacity that effectively responds to the changing priorities of the unit, especially in dynamic on-the-move operations.
- Due to proximity, expeditionary PED architectures are able to incorporate a variety of line-of-sight and beyond-line-of-sight communications systems to assure communications between the mission command and PED nodes when they are not colocated. The ability to establish an effective expeditionary primary-alternate-contingency-emergency communications plan between PED nodes and their supported command is critical throughout an operation but especially so during periods of disrupted, intermittent, and limited communications.

As the duration of the deployment timeline before and during a large-scale combat operation lengthens, MI leadership must simultaneously plan and coordinate to extend the expeditionary ISR and PED architecture to incorporate reach PED operations. This is important for multiple intelligence disciplines but is especially so for SIGINT. For example, in a large-scale combat operation, terrestrial SIGINT capabilities must leverage the global SIGINT enterprise and its linguist and analyst capacity to answer supported commanders' priority intelligence requirements in a timely manner. Collaboration and access to this reach PED enterprise maximize commanders' situational understanding of their operational environment.

Throughout a large-scale combat operation and its aftermath in phases 4/5, it is paramount to continue to improve and extend the ISR and PED aspects of the intelligence and mission command architectures. This concerted effort expands the intelligence warfighting function's ability to leverage additional intelligence community capabilities and resources that directly address commanders' requirements.

A second key lesson from the ISLC discussion was the need to incorporate PED products and reporting into coalition networks for both intelligence and mission command purposes. Since the U.S. military will rarely act unilaterally, understanding the policies and procedures for establishing coalition architectures is critical to operational effectiveness

in all phases of a mission. Thus, when planning MI operations in a given geographic theater, commanders need to coordinate not only unique intelligence and communications architecture capabilities, but also the integration of multinational partners in the direct and general support of the region's operations.

Conclusion

ISLC 2018 provided participants with an understanding of why members of the MI community must work diligently with one another to establish and sustain ISR and PED architectures that support the full range of operational settings and scenarios. Although the INSCOM-led PED service center effort has matured to adequately support global ISR and PED operations, continued Army, DoD, and intelligence community convergence efforts are necessary to optimize this capability across the intelligence and mission command enterprises, especially to support dynamic large-scale combat operations.

In sum, MI leaders gained a better perspective of the Army's architecture capabilities and challenges in each respective theater. The useful dialogue helped establish a common understanding of the components and complexities involved in developing viable PED architectures. Every MI leader—officer, warrant officer, and noncommissioned officer—must master the critical task of coordinating to integrate the multiple building blocks of end-to-end expeditionary and reach PED intelligence and communications architectures. Becoming proficient in this skillset is essential for MI units' support to mission command in the complex 21st century information environments where the Army and our joint and multinational partners will fight.

Epigraph

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

Endnotes

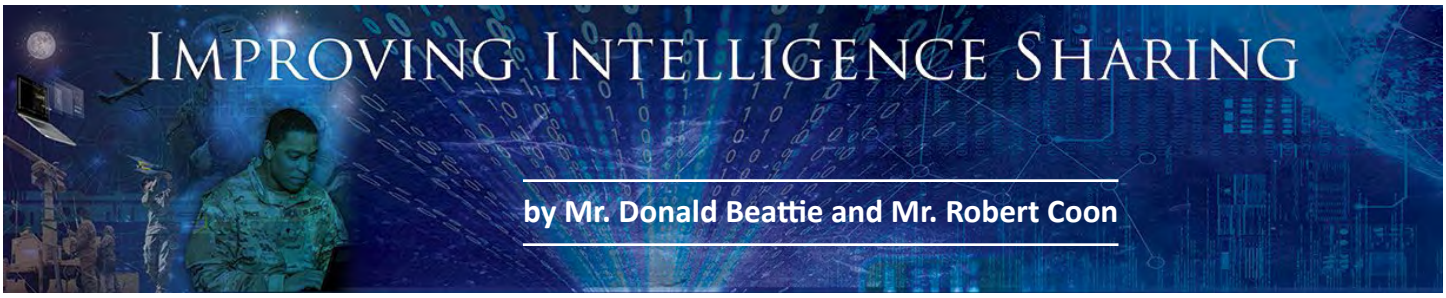
1. U.S. Army Training and Doctrine Command, *Capabilities Needs Analysis (CAN) FY17/18 Results Supporting SPAR-20, General Officer Steering Committee*, 14 July 2017.

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

Mr. John DellaGiustina is a retired military intelligence officer who is the contract task lead for the Processing, Exploitation, and Dissemination (PED) Team in the Requirements Determination Directorate (RDD), U.S. Army Intelligence Center of Excellence (USAICoE) at Fort Huachuca, AZ. After a decade in tactical intelligence leader positions, he planned and executed operational Army and joint aerial intelligence, surveillance, and reconnaissance/PED missions in Joint Task Force/North, 12th U.S. Air Force/U.S. Air Force, Southern Command, and Task Force Observe, Detect, Identify, and Neutralize (ODIN) Iraq. He was the Deputy Training and Doctrine Command Capability Manager Sensor Processing/Distributed Common Ground System-Army for Joint Surveillance Target Attack Radar System/Common Ground Station capabilities and served as the Coalition Forces Land Component Command/Combined Joint Task Force-7 Command and Control Joint Air Control Element and Term Fusion Chief during Operation Iraqi Freedom. He is a graduate of the Command and General Staff College, the Armed Forces Staff College, and the Joint Command, Control, Communications, Computers, and Intelligence and Joint Space Intelligence/Operations courses.

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

CW3 Otis Griffin III is a capability developer and team chief for the RDD PED Team at the USAICoE. He is currently deployed to Afghanistan as the Joint Intelligence Support Element Chief in support of the North Atlantic Treaty Organization Special Operations Component Command-Afghanistan and Special Operations Joint Task Force-Afghanistan. CW3 Griffin has served in numerous intelligence positions throughout his more than 19-year career from tactical through strategic. Previous assignments include the 470th Military Intelligence Brigade-Theater, brigade production manager; Defense Intelligence Agency, Syria Crisis Cell Team officer in charge; and 1st Infantry Division G-2, analysis and control element, fusion team chief. He holds a master of science in public safety and emergency management from Capella University.



Improving Intelligence Sharing

by Mr. Donald Beattie and Mr. Robert Coon

Introduction

The *Distributed Common Ground/Surface System (DCGS) Enterprise Concept of Operations (CONOPS) 2016–2019* outlines the primary objective of all its digital systems to "deliver intelligence to the decision maker. To achieve this objective three key enabling concepts exist to support this effort: Data and Service Standards, Enterprise Wide Data Management, and Integrated Analysis and Analytics."[1]

Army intelligence elements, at all echelons, have a limited capability to exchange accurate and actionable intelligence across security domains and among designated providers and consumers. These include—

- Supported S-2s and G-2s.
- Joint, intergovernmental, and multinational partners, including the Five Eyes nations.
- Host-nation partners.
- Special operations forces.
- Medical.
- Civil affairs.
- Other services.

This is especially true when consumers operate for an extended period in a disconnected, intermittent, limited, and contested electromagnetic and cyberspace environment. Data refinement is therefore critical to intelligence sharing in order to provide the decision maker with timely, accurate data.

Objectives of Improving Intelligence Sharing

Intelligence sharing has three centers of gravity:

- Competitive advantage—the speed at which we can exploit data and information.
- Support to decision making—how we make information palatable for leadership (at all levels).
- Data value—how we increase the value of data, or what we can do with data.

One of our more complex challenges with today's intelligence structure is to mitigate data growth and complexity at the tactical level. To do this, we must approach the challenge as a three-dimensional problem that consists of volume, velocity, and variety. Volume increases and sustains the amount of data we process. Velocity increases the speed of data processing, in and out of systems. And variety increases the range of data types and sources.

To realize greater returns on our exploitation investments, we must consider evolving where we enrich data. This would result in performance of data analytics at division and above, with a greater focus on dissemination at the tactical level, i.e., brigade combat team (BCT) and below.

Efforts at the tactical level should enable a lightweight, low-bandwidth, centrally managed ontology that enables intelligence sharing between the United States and its coalition partners. In addition to providing an advanced capability within an agile framework, the capabilities should reside on the current infrastructure and be adaptable to changing data requirements that directly facilitate mission planning and execution.

Intelligence Sharing in a Peer/Near-Peer Decisive Action Environment

Battlefield geometries are relative to your location on the battlefield, and the effects on intelligence sharing differ between operating environments. We can define the threat through three primary effects:

- Destroy (fires and direct attack).
- Disrupt (nonlethal fires and electronic warfare).
- Manipulate (cyberspace attacks).

Our current architecture complexity complicates data interoperability and dissemination. The standard U.S. Army corps/division/BCT architecture contains more than a dozen systems, each with "niche" data silos and no central control mechanism. Our intelligence architectures have become overly complex with multiple points of failure and data exchange bottlenecks. We face daily challenges that include analysis, search, sharing, storage, transfer, visualization, and information security. Therefore, intelligence sharing must derive from suitability and survivability. Simplicity then becomes a key enabler, while speed and availability of services remain essential.

Proposed Ways to Maximize Intelligence Sharing

Ultimately, we must invest in the enrichment of information at all levels—turning data into knowledge. In order to maximize the return on that investment, intelligence sharing must reduce or eliminate any added overhead at the BCT and below. Our system designs must enable intelligence contributions from all sources without boundaries, allowing the distribution of not only single-source but also all-source information.

Database contribution cannot be restricted to hardware- and software-specific platforms; every organization must have the ability to contribute within a crowdsourcing construct—similar to the Every Soldier is a Sensor program and every analyst is a processor. The U.S. Army is extremely competent at distributed single-source intelligence operations, while it is a little less confident in its ability to conduct "distributed" all-source operations on a modular battlefield.

The current threat, coupled with guidance from the U.S. Army Chief of Staff GEN Mark Milley, directly decreases physical footprints at the BCT and below. In turn, our tactical operations centers must reduce their setup and teardown times and enable multiple "jumps" without degrading any capability for long periods. An extensive evaluation of our current architecture is essential, to include reducing the number of connection points, ontologies, and schemas. Available technology (mainly ecommerce) used by industry can help determine how geographically separated elements collaborate, disseminate, and enable their leadership. Where we process data could cause a fundamental change in our current force structure.

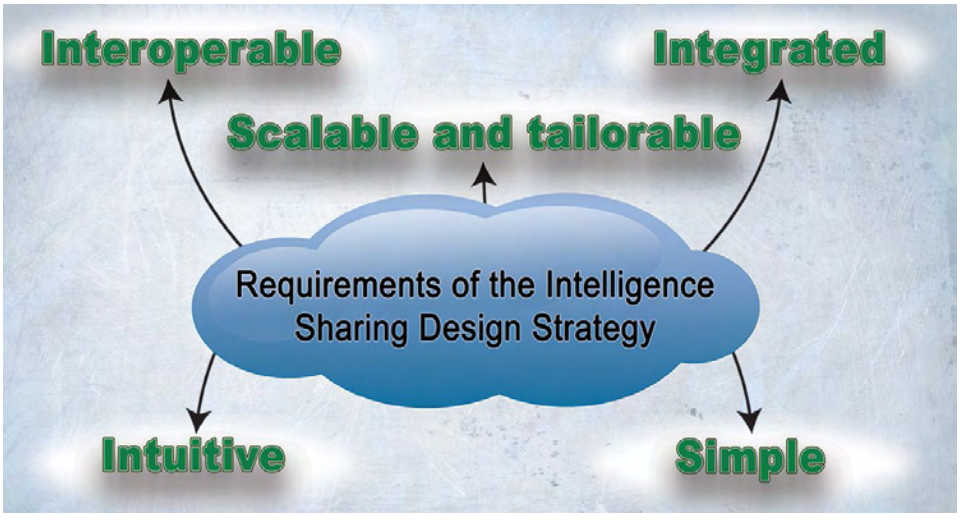
Traditionally, division and corps elements tactically deploy their Analysis and Control Element (Block II) structure only to experience—

- A loss of capability with inclement weather.
- Bounding command nodes.
- A loss of or degraded digital connectivity.
- Electronic warfare.
- Reduced manning.
- Simple system failures.

Tactical command and control nodes are consumers of data and information; there is no benefit in forward deploying an overhead-intensive enrichment capability. Centralizing processing nodes regionally increases reliability, quality, and redundancy between nodes.

The U.S. Army Intelligence and Security Command's *Data Vision 2017-2025*, published in May 2017, provides a starting point to enable this strategy.[2] This vision would consolidate our current ingestion and enrichment structure to three primary sites. This strategy, coupled with the right technology, would reduce overall costs and allow us to see an exponential decrease in maintenance and sustainment challenges. Our design principle must be—

- **Simple:** Be able to leverage mission command network capabilities in intense, time-constrained situations; enable the significant cognitive requirements on leaders and soldiers; and provide for a common user experience across all echelons, formations, and phases of the operation.
- **Intuitive:** Have an overall ontology and topology that is simple to understand and execute while allowing for dynamic changes. Tools cannot take 3 weeks to learn; we must take cues from commercial capabilities that do not require training to operate (e.g., Amazon, eBay, and Facebook).
- **Integrated:** Provide a common strategy that reduces the systems' overhead at the tactical edge; and centralize a schema for standardization and consolidation, allowing us to make surgical decisions of how data is received, processed, shared, and (more importantly) interoperated.
- **Interoperable:** Provide for interoperability across all echelons, formations, and unified action partners while remaining system-agnostic. Data transformation into various object models must be seamless.
- **Scalable and tailorable:** Have the ability to adapt to a wide variety of situations; and enable operators, analysts, and leaders to tailor capabilities to their needs or requirements.



What Does Fully Mission Capable Intelligence Sharing Look Like?

In simple terms, intelligence sharing is fully mission capable if it can exchange and leverage disparate data and information from higher, lower, adjacent, and joint, intergovernmental, and multinational partners and allies. As an example, a battalion can receive and exchange data, information, and intelligence with its companies, as well as with its higher brigade headquarters from BCT through echelons above corps units. To provide this capability it is necessary to use organic communication means in a net-ready environment while being able to interoperate, manage, and communicate through a degraded network.

Enhancing capabilities at division allows for an evolution in how we process, normalize, correlate, associate, and enrich data. Ultimately, these improved capabilities would enable timeliness of actionable intelligence and reduce the volume of unprocessed data flowing through any given network, thereby improving communications across the force.

Finally, we need to visualize the data through object-based production (OBP). OBP is the creation of conceptual objects (i.e., people, places, and things) that are used as "buckets" to store tokens that make up attribute collections. The object becomes the single point of convergence for all information and intelligence, as the "object" is enriched throughout a workflow, architecture, or topology. OBP is not a tool or technology but rather a deliberate way of doing business.

Historically, the intelligence community and Department of Defense arrange and prioritize information/intelligence based on the organization that produced it. Retrieving all available information about a person, place, or thing was performed primarily by accessing the individual repository of each data producer and conducting free-text searches. Standards and formatting differ between organizations and create "silos of excellence" for data discovery.

The cornerstone of OBP is the object model. For example, the Tactical Entity Database is an object model. It is a standard collection of artifacts that make up a unit, facility, person, etc. Interoperability between systems is based on transformations between object models—mapping one attribute to another. Examples of systems with a defined object model are the Modernized Integrated Database, the Global Command and Control System, and the Command Post of the Future.

Contemporary analysts and decision makers comprehend information visually. In almost every modern command and control node, the operations focus on a visual representation of the battlefield, such as a map. Therefore, the evolution of intelligence sharing must include—

- Improving visualization of the operational environment (terrain, weather, civil considerations, and threat).
- Supporting course of action development and the decision-making process.
- Leveraging a true common operational picture across echelons.

Enhancement of the common operational picture occurs by improving support to information collection, which includes planning, execution, and assessments. Finally, we must evolve the availability of predictive intelligence capabilities to better hypothesize and predict threat actions and activities.

When is Intelligence Sharing Fully Mission Capable?

Intelligence sharing is fully mission capable when it has met its net-ready requirements and is able to provide fusion and visualization capabilities.

Net-Ready Requirements. To be net-ready, a system must be interoperable with 80 percent of its identified national agencies and multinational, Department of Defense, and Army organizations. It must have the capability to enter and be managed in the network, and it must be able to transmit and receive 80 percent of its identified core functions.

Fusion. Through fusion, systems provide processes to transform observational data into refined information, knowledge, and understanding that involve both automation and human cognition. Fusion has three process categories: normalization, correlation, and association. Normalization is the initial process that organizes the collected data into a usable form. Correlation determines if an entity is new or already exists and associates the entity with the existing instance of the entity. It then updates the knowledge about that entity. Association determines how entities are related and how they work together.

Visualization. This capability accesses and provides relevant battlefield and situational understanding that supports the commander's common operational picture, allowing visualization of the operational environment. It also allows analysts to support course of action analysis; develop and visualize the common operational picture; support information collection (plan, execute, and assess); support targeting (plan, execute, and assess); and hypothesize future threat actions.

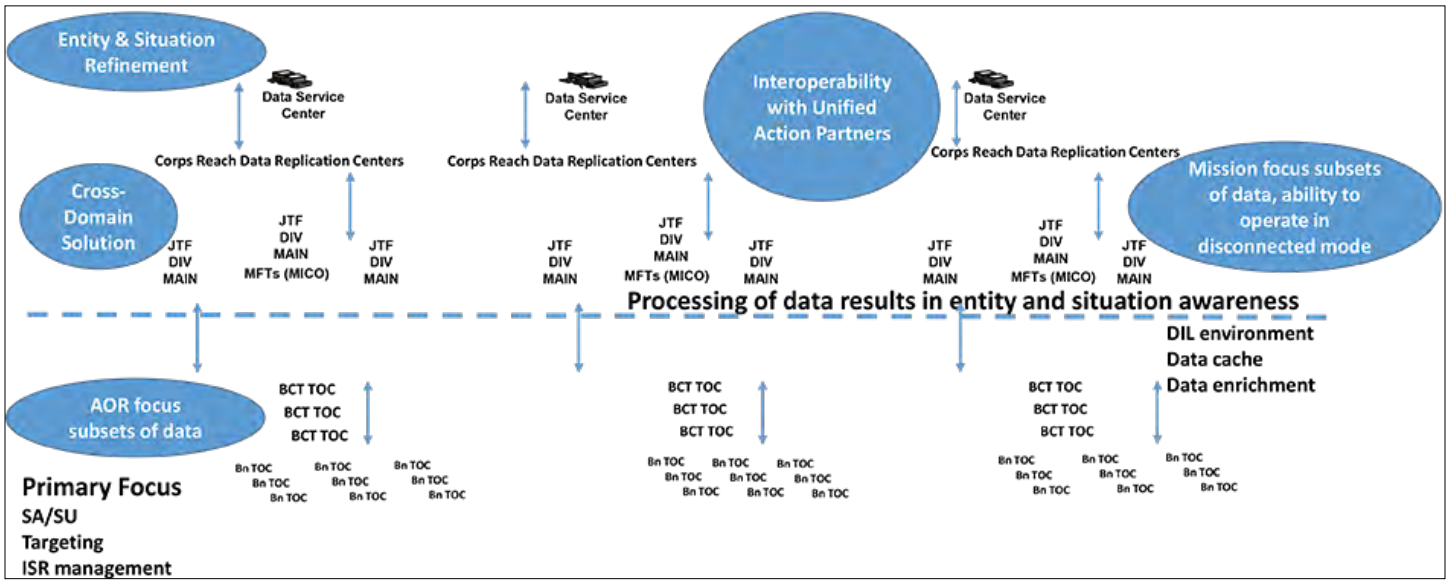
Intelligence Sharing Considerations

The intelligence environment will be a continuum of Army operations, operating in complex multi-domain and multi-security domains in a dispersed disconnected, intermittent,

and limited environment. Intelligence missions will take place at home station and throughout the deployed areas of responsibility while using a scalable and tailorable communications architecture to obtain, process, and disseminate intelligence products. Our intelligence sharing architecture must enable the intelligence analyst to operate seamlessly in this multifaceted environment.

A New Architecture Strategy to Enable Intelligence Sharing

As we purchase and enable new technology, we must be prepared to adapt our force structure to maximize the gains. Laying new technology over our current intelligence template may not yield the results we need.



As we integrate new technology, we need to be open to where we are best postured to process data that will result in an enhanced situational awareness while accelerating data enrichment. Issues of where we employ a cross-domain solution, conduct interoperability with unified action partners, and conduct entity and situation refinement must enable tactical command posts to function in consolidated and distributed configurations, thereby providing the capability to deploy quickly and then scale to the desired capacity. Commercial industry provides us a glimpse of what is possible and how to employ the technology. The underlying question is—are we as open-minded as we need to be to employ it?

Endnotes

1. Undersecretary Secretary of Defense for Intelligence, *Distributed Common Ground/Surface System (DCGS) Enterprise Concept of Operations (CONOPS) 2016–2019, Version 1.0* (2 October 2014), ii.

2. The U.S. Army Intelligence and Security Command's *Data Vision 2017-2025* is a companion to *Army Intelligence 2017-2025—Intelligence at the Speed of Mission Command*, expanding on line of effort 3, titled Enabling Technology.

Mr. Donald Beattie is a retired Army military intelligence officer who currently serves as the Deputy for the U.S. Army Training and Doctrine Command Capability Manager–Foundation, Distributed Common Ground System-Army, at the United States Army Intelligence Center of Excellence, Fort Huachuca, AZ. He has a bachelor of science from Canisius College and a master of arts in education from the University of Colorado.

Mr. Robert Coon currently works for the U.S. Army Intelligence and Security Command as the G-3 Integration lead under Foundry. He has a bachelor of arts in political theory, a bachelor of science in computer science, and a master of business administration from Colorado State University.

Military Intelligence Training Strategy Update

by Major Leah B. Haller

Introduction

At the 2018 Intelligence Senior Leaders Conference, the U.S. Army Intelligence Center of Excellence (USAICoE), Directorate of Training, Director, COL Eric Larsen briefed the latest information on the Military Intelligence Training Strategy (MITS). This article summarizes four key areas of COL Larsen's presentation:

- MITS.
- Objective-T.
- MITS pilot results and lessons learned.
- Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT).

Military Intelligence Training Strategy

The purpose of MITS is to develop a tiered certification plan that can provide an objective approach to measure intelligence readiness across the brigade combat team (BCT) intelligence structure. Standardization of military intelligence (MI) certification is based on one basic principle—to objectively rate how a unit is able to answer a brigade commander's priority intelligence requirements. For units to be successful at this certification, the MI company commanders must plan and set up training for their sections before the MITS certification to ensure their sections are proficient at their individual and collective tasks. Once a unit is ready to conduct MITS certification, it should be familiar with all the tasks required to certify. Training circular 2-19.400, *Military Intelligence Training Strategy for the Brigade Combat Team*, provides information about the Army's approach to training and highlights training considerations and enablers which, when mastered, will make the certification process successful.[1]

MITS requires a coalition of organizations to make the certification process a reality. The proponent, USAICoE, is responsible for developing the standards for certification, based on critical task lists by military occupational specialty (MOS). USAICoE will also publish training circulars and other literature for the BCT MITS tiers 1 through 4. Publication of the training circulars is ongoing: tier 3 (MI crew certification) and tier 4 (individual MOS proficiency on programs of record) were published in May 2018. Training circulars for tiers 3 and 4 are available on the Army Publishing Directorate website. These are prescriptive "how to" documents that will guide units through the execution process and methods to certify their organizations.[2] Training circulars for tier 1 (intelligence warfighting function certification) and tier 2 (MI platform certification) will be published no later than third quarter 2019.

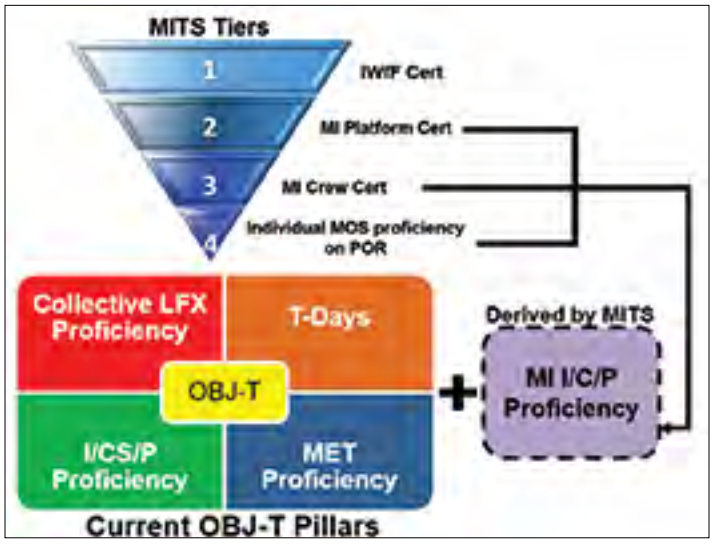


Figure 1. Current Objective-T Pillars and MITS Tiers

The U.S. Army Training and Doctrine Command G-27 Operational Environment Training Support Center delivers complex operational environment products and services by leveraging real-world data, information, and knowledge to enable learning across all training, education, and leader development. In Army forums, it also advocates solutions to key operational environment capability gaps, as the responsible Army operational environment opposing force project office.[3] Using the decisive action training environment, G-27 overlays this scenario on any terrain to enable the digital range to provide a realistic MI-focused scenario for every BCT, light and heavy. G-27 also has developed division- and brigade-level products, such as operational orders, fragmentary orders, collection plans, and graphic intelligence summaries to provide Soldiers with training at the collective crew and platform levels.

IEWTPT creates the digital range that Soldiers use to conduct certification. IEWTPT consists of a suite of user interfaces designed to mimic the operational environment using

the MI-assigned systems or programs of record. For instance, the Intelligence Low Overhead Driver (iLOD) system interfaces with the Distributed Common Ground System-Army through the Intelligence Fusion Server stack to populate the graphics and reporting that an all-source team would normally see and use to analyze the battlefield and answer a commander's priority intelligence requirements. IEWTPT is an integral part of the certification because the crews and platforms must be able to fulfill both analog and digital requirements in order to answer a commander's priority intelligence requirements, and thereby report themselves as ready. The last members of this coalition are from the—

- Home station.
- Foundry facility that hosts IEWTPT and runs units through individual tasks and training.
- Mission training complex that is responsible for all other training conducted in station.
- Unit conducting the training itself.

Once the policies, literature, descriptions, and exercise materials are completed, they are pushed out to every home station in order to provide each unit an opportunity to conduct a certification. The units must lock in their certification training dates and coordinate with Foundry and the mission training complex early enough to ensure they will receive IEWTPT and product support. IEWTPT is integral to the conduct of the tier 2 and 3 certifications; however, USAICoE has designed the certification to be as simple as possible so that each BCT can execute MITS certification with minimum external support. Initially, some challenges may exist when planning and executing MITS certification, but as the digital trainer evolves and Foundry 3.0 is implemented, this process will be streamlined.

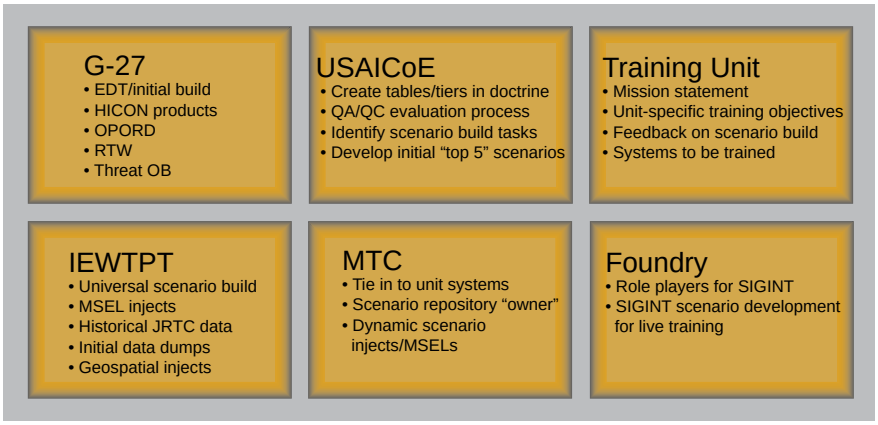


Figure 2. Key Elements of MITS

A parallel effort exists at U.S. Army Forces Command (FORSCOM) and U.S. Army Intelligence and Security Command to develop and implement training strategies for MI unit's echelons above corps. These strategies are loosely based on the BCT certification process but will have to deviate in certain areas where the crew and platform composition does not align or the tasks conducted at BCT level do not match up. (The modified tables of organization and equipment and the tables of distribution and allowances provide the basis for this determination.) USAICoE is supporting this effort with its MITS and certification expertise.

Objective-T

Army senior leaders have directed phased implementation of objective assessments of training proficiency. The current Army regulations that denote how units will track and report their readiness to higher headquarters are FM 7-0, *Train to Win in a Complex World*; AR 220-1, *Army Unit Status Reporting and Force Registration–Consolidated Policies*; and AR 350-1, *Army Training and Leader Development*. The four components/pillars of objective evaluation of units are—

- Weapons system proficiency.
- Mission essential task proficiency.
- Collective live-fire task proficiency.
- Continuous training days.

The only metric that provides a unit's "T" rating is the mission essential task proficiency.[4] Currently, we have no capacity to add an MI-specific readiness component, or "pillar"; therefore, the training and evaluation outline will include MITS requirements as part of the task conditions and standards. Thus, an MI unit's "T" rating will be affected if it has not conducted MITS training through tier 1. One key ingredient to success for this strategy is the ability to account for, and track readiness for, each BCT as it conducts every tier of training up until its final certification at the combat training center rotation.

As we continue to determine the most effective method to measure readiness, the MITS itself is an ongoing progression to create, test, and validate the process of planning and executing tiers 1 through 4. Our intent is to stay ahead of FORSCOM units' requirements and provide assistance when needed. So far, USAICoE has observed and supported the certification efforts of the 82nd Airborne Division, 4th Infantry Division, 10th Mountain Division, and Indiana National Guard training site, along with numerous outreach efforts at the MI, BCT, and brigade engineer battalion pre-command courses; MI warrant officer and officer forums; and various other venues.

MITS Pilot Results and Lessons Learned

The 82nd Airborne Division recently conducted two pilot exercises and a third exercise with observers from USAICoE. As with any pilots, participants raised concerns during the exercises, many of which USAICoE was able to address on the spot. Bottom line: We have learned that in order to run a successful MITS certification tier, units will need to incorporate training and certification timing into their annual training plan.

Another major lesson learned is that in order to conduct the certification, there must be regular maintenance and use of the systems; and a pre-certification communications check is vital to making sure the certification is not a failure due to administrative reasons. There have been some requests to allow an analog exercise to provide partial credit, but the requests were not granted because the certification is meant to ensure readiness—not just for personnel but also for equipment.

Intelligence and Electronic Warfare Tactical Proficiency Trainer

As stated earlier, IEWTPT is the digital range for MI units to conduct training and certification. IEWTPT is constantly evolving to support new technologies, improve the current user interface, and add capabilities. USAICoE is working on a non-dynamic, fully incorporated exercise scenario for tiers 2 and 3 of training that will test and validate the crews' and platforms' ability to answer priority intelligence requirements. For this initiative to be successful, we will need every BCT in FORSCOM to have access to IEWTPT support in order to accomplish the new readiness standards that are coming. IEWTPT is fundamental to the successful execution of MITS, and though the Army has made significant improvements to the system and its capabilities, IEWTPT still needs a fair amount of work before it can fully support MITS. Tracking of these requirements occurs through the regular meetings of the Requirements Control Board and the Capabilities Control Board Governance. In order for MI training to continue to be successful, the Army must continue to fund IEWTPT, incorporate it into Foundry 3.0, and support it through the mission training complexes.

Conclusion

The role of the MI company is to provide timely, relevant, accurate, and synchronized information collection, surveillance, and reconnaissance support to maneuver units within the BCT, the BCT commander, staff, and subordinates during the planning, preparation, and execution of multiple, simultaneous decision actions on the battlefield. MITS, supporting scenarios, and increased functionality of IEWTPT will work together to enable a clearer picture of intelligence readiness across the BCT intelligence structure. Ideally, we will be able to fully implement MITS tiers 1 through 4 certifications, with supported exercise scenarios for tiers 2 and 3 as early as fiscal year 2020.

Endnotes

1. Department of the Army, Training Circular (TC) 2-19.400, *Military Intelligence Training Strategy for the Brigade Combat Team* (Draft).

2. Department of the Army, TC 2-19.403, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 3* (Washington, DC: U.S. Government Publishing Office [GPO], 30 May 2018), and Department of the Army, TC 2-19.404, *Military Intelligence Training Strategy for the Brigade Combat Team Tier 4* (Washington, DC: U.S. GPO, 10 May 2018).

3. U.S. Army Training and Doctrine Command website, "G-27 OE Training Support Center" page, http://oetsc.tradoc.army.mil/.

4. Department of the Army HQDA G/3/5/7, *Leader's Guide to Objective Assessment of Training Proficiency (Initial Operating Capability)* (29 September 2017), https://atn.army.mil/unit-training-management-(utm)/leader-s-guide-to-objective-assessment (common access card required).

MAJ Leah B. Haller accepted an Army Reserve Officers' Training Corps scholarship to the University of Utah and commissioned as a military intelligence (MI) officer. Her first assignment was to 501st Corps Support Group, direct support to 2nd Infantry Division on Camp Red Cloud, Korea. From there, she moved to a platoon leader position with A Company, 102nd MI Battalion and deployed with 2nd Brigade to Ar Ramadi, Iraq, for one year of targeting support. Her other assignments include Joint Surveillance Target Attack Radar System deputy mission crew commander; 1st Armored Division G-2 operations officer; 11th Air Defense Artillery Brigade S-2; 8th Army G-2 deputy analysis and control element chief and Countering Weapons of Mass Destruction officer in charge; U.S. Forces Korea Special Troops Battalion S-3 and executive officer; and U.S. Army Intelligence Center of Excellence Directorate of Training executive officer. She is a graduate of the Command and General Staff College.

Adapting Multifunctional Intelligence and Electronic Warfare to Support Maneuver

by Colonel Mark Dotson, Colonel Jennifer McAfee, and Colonel Francesca Ziemba

Introduction

Warfare is becoming more challenging with each passing generation. In no facet of warfare is this more relevant than in our struggle to maneuver in today's cyberspace domain, specifically in the electromagnetic spectrum (EMS). Increasingly contested and congested with more complex and numerous signals, the EMS has become an essential component of our peer adversaries' attempts to present operational dilemmas to the U.S. Army. Operating in this complex environment has created challenges for intelligence collection within a net-dependent force. To address some of these challenges, the Chief of Staff of the Army directed the U.S. Army Intelligence Center of Excellence (USAICoE) and U.S. Army Cyber Center of Excellence (USACCoE) to integrate their signals intelligence (SIGINT) collection and electronic warfare (EW) capabilities. These efforts are currently under way.

2018 Joint Operational Integration Assessment

In February and early March 2018, Army and Marine Corps (USMC) SIGINT, EW, and EMS management professionals met at the Electronic Proving Ground at Fort Huachuca, Arizona, to take an initial step toward greater integration and interoperability. The event was the first in a series of joint operational integration assessments (JOIAs) and was made possible with funding from the Department of the Army's operations and intelligence staffs, as well as the Program Executive Office for Intelligence, Electronic Warfare, and Sensors. The purpose of the JOIA is to discover best practices and identify doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) implications for greater sensing and effects on capability and interoperability in joint multidomain operations. The intent is to demonstrate how the Army and USMC would jointly conduct SIGINT and EW support operations across a congested and contested EMS environment to open windows of opportunity for maneuver forces and provide those forces a decisive advantage.

The objectives of the initial JOIA event focused on observing and documenting Army and USMC staff procedures, staff interactions, and the execution of SIGINT and EW support/electronic attack operations. The complete findings are documented in the *JOIA Report.*[1] This article will focus on three of the most significant DOTMLPF-P findings of the assessment:

- Army and USMC lack the necessary materiel to face the full complement of threat signals of interest.
- Army needs to reevaluate how it staffs its SIGINT and EW forces.
- Current facilities are not conducive to realistic operations in the EMS.

Lack of Necessary Materiel. First, the Army and USMC lack the necessary materiel to face the full complement of threat signals of interest. Currently fielded materiel solutions are not state of the art and the basis of issue is not adequate, leaving commanders without the organic equipment densities required to fight and win in the EMS.

The military does not have the capability required to fight and win in the EMS. Given the changing nature of our threats and the capabilities of our peer competitors, the military needs reinvigorated SIGINT and EW systems that can detect and exploit the full complement of threat signals. These systems will be required to communicate via line of sight and beyond line of sight in order to account for the varied size, terrain, infrastructure, and supporting networks associated with current and future battlefields.

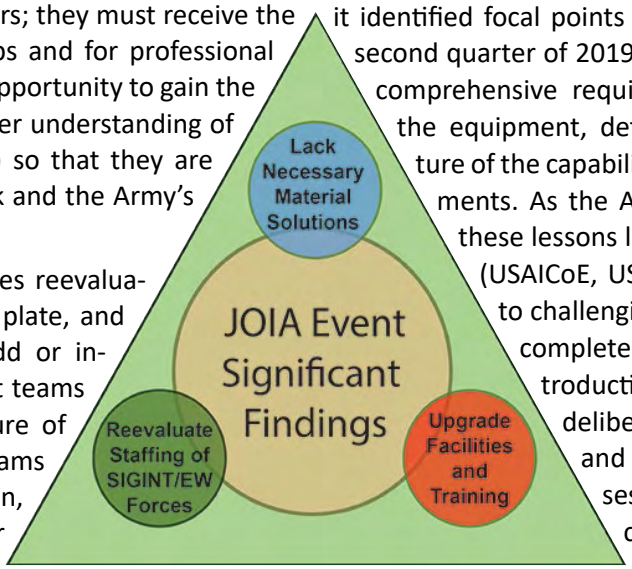
SIGINT and EW are inseparable. EW relies on SIGINT for accurate target decks, and SIGINT exploits the EW sensor data to vastly increase its collection opportunities. Because of this relationship, it is critical that SIGINT and EW systems work together and communicate. Given our reduced forward posture and the great diversity of threats, the SIGINT and EW materiel solutions need to be easily deployable and tailorable to the mission. One of the high points of the initial JOIA event was related to the effectiveness of the Army's Raven Claw,[2] a risk reduction effort for the Electronic Warfare Planning and Management Tool (EWPMT). Raven Claw showed great promise as a means to plan and control effects in the EMS and gained interest as a planning and synchronization possibility for the USMC.

Staffing of SIGINT and EW Forces. Second, the Army needs to reevaluate how it staffs its SIGINT and EW forces. The current designated SIGINT and EW organization is not effective

at the tactical echelon, nor is it sufficiently manned to conduct sustained 24-hour operations.

The Army's EW force is not mature. As it grows and begins to have greater capability, the U.S. Army Training and Doctrine Command must review its overall structure. It is not a simple matter of increasing numbers. There must be a viable career path for the Soldiers; they must receive the necessary education for their jobs and for professional growth; and they must have the opportunity to gain the experiences necessary for a greater understanding of SIGINT and EW (and cyberspace) so that they are prepared for each successive rank and the Army's expectations of that rank.

The tactical SIGINT force requires reevaluation in terms of structure, grade plate, and strength. The Army needs to add or increase SIGINT cryptologic support teams at all echelons. The rank structure of the current SIGINT collection teams also requires careful consideration, as it currently consists of junior grade Soldiers. While acknowledging the JOIA event was limited to normal duty hours, it was clearly evident that tactical SIGINT collection teams are not designed for continuous 24-hour operations. The Army needs to rethink its tactical SIGINT and EW structure to effectively support a range of military operations.



Facilities and Training. Third, current facilities are not conducive to realistic operations in the EMS. The military needs more locations where it can train its forces to operate across EMS and in multi-domain operations. The military also needs tools to enable virtual and constructive training when or where live training is not feasible.

As the SIGINT and EW force grows in capability, it will need space to train. The assessment at the Electronic Proving Ground was the first opportunity for many of the Soldiers and Marines to use their equipment in a live environment. Unintentional effects on civilian communications often constrain most military training areas from being able to fully employ their SIGINT and EW systems in the EMS. This results in too few locations for our military to learn how to fight in the EMS. A mitigation for this shortfall is the Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT). As it continues to develop, the goal is to have IEWTPT interface with EWPMT and other mission command systems and become the premier tool for Army training in the EMS. Additionally, all new SIGINT and EW equipment will come with a certain level of embedded training capability. Despite these near-term advances, the military cannot rely solely on virtual and constructive training; it must find ways to incorporate the EMS into live training events at its combat training centers and home stations.

Lessons Learned. The first JOIA event in February 2018 provided pertinent documented lessons learned information needed for joint integrated SIGINT and EW operations, and it identified focal points for the second JOIA event in the second quarter of 2019. Key among those are identifying comprehensive requirements needed in modernizing the equipment, determining proper manning structure of the capabilities, and defining training requirements. As the Army and USMC begin to address these lessons learned, the organizers of the JOIA (USAICoE, USACCoE, and USMC) look forward to challenging the Army and USMC to a more complete assessment next year with the introduction of aerial SIGINT and EW, and a deliberate emphasis on tactical planning and target synchronization. Future assessment events may include the challenge of combined movement and maneuver—if our recent operations are any indication, the U.S. military is unlikely to fight alone anytime soon.

Aerial Layer Challenges and Initiatives

While the first JOIA focused exclusively on the integration of the terrestrial layer of SIGINT and EW, USAICoE is simultaneously working in collaboration with the community of interest to solve the significant challenge of conducting aerial intelligence, surveillance, and reconnaissance and EW in an antiaccess/area denial environment. The challenges primarily revolve around capability gaps in deep sensing, survivability of platforms, data transport in contested environments, and the speed and volume of processing, exploitation, and dissemination requirements in high-intensity operations.

Today's aerial layer is generally built for unchallenged air superiority and is optimized for collection against targets unlike those of peer competitors in large-scale combat operations. The desired end state is a relevant and effective aerial intelligence, surveillance, and reconnaissance layer that directly supports shared understanding in antiaccess/area denial environments. This will include collection systems with improved survivability, extended range, and leap-ahead technology that address current sensing gaps. It also requires the right doctrinal foundations, institutional training, force mix, and military occupational specialties.

USAICoE concluded its aerial DOTMLPF-P analysis in mid-2018. The results will help inform an aerial layer

modernization strategy and a future sensor systems initial capabilities document. In turn, this documentation will support larger modernization efforts.

In particular, significant potential exists for the future integration of SIGINT, EW, and cyberspace sensors in the aerial layer. Tentatively dubbed the Aerial Layer Intelligence-Electronic Warfare System, this future capability will complement the Terrestrial Layer System. Ultimately, this aerial modernization effort will permit the Army to field an organic, multimodal family of integrated collection capabilities, effective at all altitudes and echelons, in order to support a shared understanding and targeting in depth.

These initiatives in both the aerial and terrestrial layers are nested within the national defense strategy as well as in the guidelines of intelligence operations described in FM 2-0, *Intelligence*:[3]

- Maintain readiness.
- Ensure continuous intelligence operations.
- Orient on requirements.
- Provide mixed and redundant coverage.
- Gain and maintain sensor contact.
- Report information rapidly and accurately.
- Provide early warning.
- Retain freedom of movement.

Conclusion

The operational challenge posed by the advent of the antiaccess/area denial battlefield environment, as well as the identified shortcomings in the existing SIGINT and EW enterprise, necessitates deliberate change in order to gain and maintain a position of relative advantage over peer adversaries. The successful reintegration of these capabilities on the battlefield requires unity of effort with the total Army across all components, commands, and staffs.

Endnotes

1. U.S. Army Intelligence Center of Excellence, *Army/USMC Signal Intelligence (SIGINT), Electronic Warfare (EW), and Cyber Joint Operational Integration Assessment (JOIA) Doctrine, Organization, Training, Materiel, Leadership & Education, Personnel, Facilities – Policy (DOTMLPF-P) Report*, 15 June 2018.

2. The Army's Raven Claw was designed "to work networked or in a Disconnected, Intermittent or Latent (DIL) environment…it doesn't depend on a host server or external data, but rather can function on its own with last known data and real-time feeds from sensors providing electronic support to do its work. Raven Claw is contained in a ruggedized military laptop—for now—that integrates with other Army systems until an appropriate hosting environment is introduced into Army formations." John Higgins, "Raven Claw Augments Battle Management for Electronic Warfare Operations," *U.S. Army Worldwide News*, January 22, 2018, https://www.army.mil/article/199368/raven_claw_augments_battle_management_for_electronic_warfare_operations.

3. Department of the Army, Field Manual 2-0, *Intelligence* (Washington DC: U.S. Government Publishing Office, 6 July 2018), 3-7.

COL Mark Dotson, COL Jennifer McAfee, and COL Francesca Ziemba currently serve as the U.S. Army Training and Doctrine Command Capability Managers for Electronic Warfare, Terrestrial & Identity, and Aerial, respectively.

The Future of Intelligence Analysis, Analytics, and Distribution

by Colonel Robert Collins, Ms. Lindsay Yowell, and Mr. Greg Hartman

Introduction

The Distributed Common Ground System-Army (DCGS–A) is a major automated information system, with the Army Acquisition Executive serving as its milestone decision authority. The system provides foundation capabilities to support the Army's intelligence, surveillance, and reconnaissance (ISR) mission for the processing, exploitation, and dissemination (PED) of information and intelligence data across echelons. Within the Project Manager DCGS–A portfolio, DCGS–A comprises two acquisition category I major automated information system programs—the Product Manager for Fielding and Training and the Product Manager for Capability Drop—and three acquisition category III programs.[1]

DCGS–A entered fiscal year (FY) 2018 poised to make momentous strides in updating the capability provided to more than 40,000 Soldiers and Civilian employees globally. A substantial change of direction in acquisition strategy was implemented, in which the large-scale incremental updates were replaced with smaller, more agile capability drops that focus on specific requirements. The strategy uses the best of breed industry has to offer for each set of capability updates, while also allowing the program management office to operate with maximum efficiency and agility. This new direction involves an emphasis on troop feedback, improved market research, and better cooperation with industry, all of which will expedite getting cutting-edge capabilities into the hands of Soldiers faster.

The revised acquisition strategy for DCGS–A is in alignment with the Army Intelligence Plan, in particular with line of effort three, Enabling Technology. This line of effort includes major objectives incorporating "develop DCGS–A as an agile system," "modernize relevant platforms," and "reduce cognitive burden for analysts," which DCGS–A is presently taking action on through the capability drop strategy, current software fielding, and in cooperation with Project Maven. DCGS–A strives to meet Army modernization, which uses a process to leverage commercial innovations, cutting-edge science and technology, prototyping, and warrior feedback. Specifically, DCGS–A aligns with modernization priorities of the Army's network, command, control, communications, and intelligence, and Soldier lethality.

Fielding and Training

The Product Manager for Fielding and Training manages DCGS–A Increment 1, which achieved full deployment fielding in 2015, with 96 percent of the Army having been fielded this capability. The second iteration of this capability, Release 2, completed a follow-on operational test and evaluation during the Network Integration Evaluation 15.2 event at Fort Bliss, Texas. An Army fielding decision on Release 2 occurred in November 2015 and fielding began in early 2016. As of May 2018, Release 2 is fielded to 50 percent of the force, with full deployment scheduled for 2019.

DCGS–A Release 2 provides all-source fusion, higher classified networks, and Cross Domain Solution Suite capability down to the brigade combat team level, which increases situational understanding, data accuracy, collaboration, and a common operational picture. Release 2 also brings back the electronic intelligence analysis capability and allows users to reach national databases and repositories. Additionally, Release 2 provides a smaller size, weight, power, and cost battalion solution with tailorable configuration and a common software baseline, which reduces training, maintenance, and operator learning times. Release 2 also enables units to displace the legacy All Source Analysis System Analysis and Control Element Block II, Prophet Control, and Digital Topographic Support System-Light, which reduces sustainment costs.

Going forward, the Product Manager for Fielding and Training will focus on continued fielding of Release 2 and displacing the Analysis and Control Element Block II. This is needed to continue, and improve upon, connecting Soldiers to multiple joint ISR platforms and sensors, the intelligence community, and the U.S. Armed Forces mission command systems. At the same time, the system must provide commanders the ability to view ISR information in one place and integrate that information into tools that can support intelligence development.

Capability Drops

The DCGS–A Product Manager for Capability Drop is pursuing Capability Drop 1 by navigating a series of carefully designed events to determine the best solution for the warfighter to support the Army's intelligence planning

functions at the battalion echelon. The goal of these events is to find a commercial solution that can meet the requirements, which include increased usability and operating while disconnected from servers and with intermittent tactical communications. The approach that the Product Manager for Capability Drop used to achieve the expectation for this system included market research, a request for proposal-driven source selection with a product demonstration, and a series of user trials, in addition to a formal operational test at the Network Integration Evaluation in late 2018. This test-fix-test concept, which incorporates Soldiers' feedback and incremental system of systems integration, has been and continues to be a critical factor in all the steps of this acquisition.

The capability drop initiative marks a distinctly different acquisition strategy path for DCGS–A. With an open system architecture guide, the process to pursue commercially available solutions began with an initial "capability drop" requirements analysis. Next, market research and vendor demonstrations were conducted, followed by a multiple contract award. The next steps for the capability drop acquisition are minor software modifications to meet user requirements, integration with the broader DCGS–A and mission command enterprise, user trials and operational assessments, accreditation to operate on deployed/fielded networks, and, lastly, down-select to a single vendor and fielding to Soldiers.

The Product Manager for Capability Drop completed the first round of user trials in June 2018, after a multiple contract award, and will proceed through the follow-on test events. Then, with support from Soldiers, the U.S. Army Test and Evaluation Command, and the Department of Defense (DoD) community, the Product Manager for Capability Drop will determine where to procure the needed quantities. The objective is to rapidly proceed and fully field a commercial battalion configuration system to the warfighter in 2019.

Capability Drop 1 will replace the current DCGS–A solution at the battalion echelon. Moving forward, Capability Drop 2 will replace the Enterprise Data Warehouse, otherwise known as the "Fusion Brain" at the DCGS–A fixed sites. Capability Drop 3 will replace the data management architecture at the tactical echelons. Capability Drop 4 will replace the all-source (user-facing) solution. Capability Drops 5 through 7 will replace the "functional" applications such as counterintelligence/human intelligence, geospatial intelligence, and signals intelligence, and do so while fully aligned with congressional language in the National Defense Authorization Act for FY 2017 (sections 113 and 220).

The Product Managers for Field and Training and for Capability Drop work collaboratively to ensure the force is fielded with the new tactical level system, and receive the training required to operate it, once Capability Drop 1 completes testing and a final contract is awarded.

Artificial Intelligence, Machine Learning, and the Future

Using an open architecture allows DCGS–A maximum agility to take advantage of emerging technology and rapid leaps in the advancement of current technologies, not the least of which are artificial intelligence and machine learning.

Presently, Project Manager DCGS–A is a key partner with the Algorithmic Warfare Cross-Functional Team's (AWCFT) Project Maven working to integrate the computer vision algorithms in the system for testing. Project Maven's goal is to augment or automate PED by reducing the human factors burden of mid-altitude full motion video by using algorithms for object detection, classification, and alerts.

In coordination with the U.S. Army G-2 and the U.S. Army Intelligence and Security Command, the DCGS–A program will begin a pilot of the Maven capability at Fort Gordon, Georgia. Installation completion is scheduled for the end of third quarter FY 2018, and the pilot will be conducted through fourth quarter FY 2018. This pilot will give the Army an opportunity to experiment with the Maven capability under realistic conditions and allow operators to provide direct feedback on the utility and capability provided. This pilot will help to shape how the Army extends this capability across the force.

Along with the efforts of Project Maven, DCGS–A continues its collaboration with Army and DoD research laboratories. DCGS–A also continues engagements with vendors in commercial industry on their artificial intelligence and machine learning efforts. As these capabilities prove their maturity and value, the DCGS–A program will continue to seek opportunities to insert these capabilities into the DCGS–A portfolio and deliver them to the Army.

Going forward, the AWCFT will consolidate, create, and apply similar capabilities to enhance PED across the military intelligence spectrum of capabilities and the DoD. DCGS–A is always prepared to take advantage of not only what the AWCFT produces but also next generation analytics, deep learning (machine learning), and other technological changes, all in keeping with the Army's modernization priority.

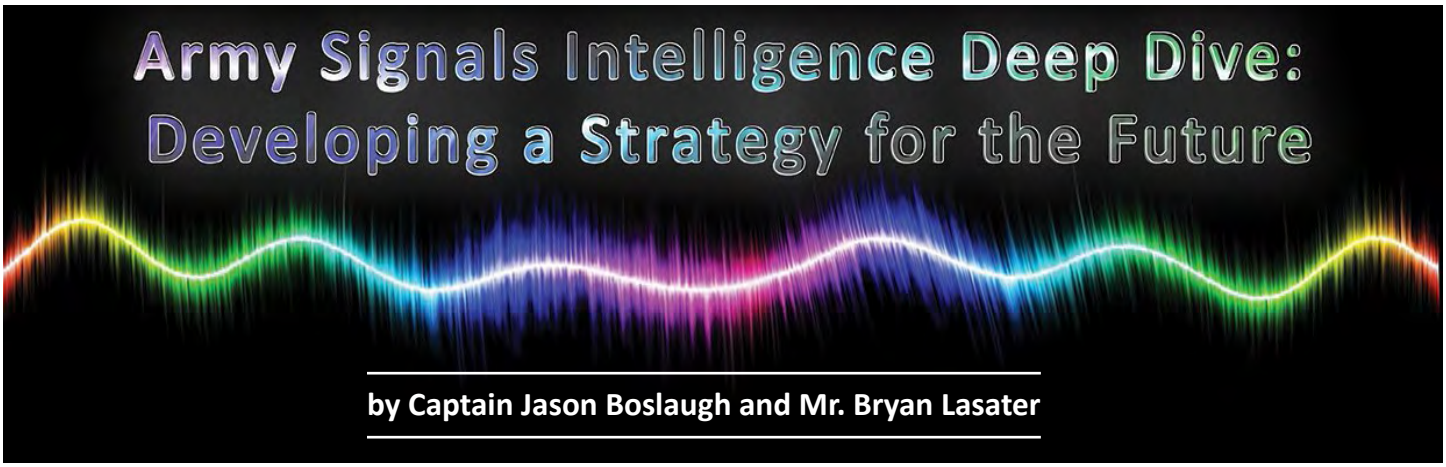
Endnote

1. Acquisition categories are "categories established to facilitate decentralized decision making and execution and compliance with statutorily imposed requirements. The categories determine the level of review, decision authority, and applicable procedures." "Acquisition Encyclopedia," Defense Acquisition University website, last modified 28 February 2018, https://www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=a896cb8a-92ad-41f1-b85a-dd1cb4abdc82.

COL Robert Collins, Project Manager (PM) for the Distributed Common Ground System-Army (DCGS–A), was commissioned into the Army in 1992 and served in several signal assignments before his selection into the Acquisition Corps in 2000. He took command of DCGS–A in 2014 and has spearheaded the efforts to modernize the capability and to do so through an inventive and revolutionary acquisition strategy.

Ms. Lindsay Yowell has worked for PM DCGS–A since 2013 and as the Deputy Project Manager for the past 3 years. With a background in engineering, testing, and program management, she distinguished herself as an effective leader during the successful testing of the currently fielded software and management of the program office. In 2017, she received the Knowlton Award for her contributions to the intelligence community.

Mr. Greg Hartman, the Chief of the Systems Engineering Division, has distinguished himself as an effective leader, skilled systems engineer, and consummate problem solver for DCGS–A. He received the Knowlton Award in 2016 for his contributions to the intelligence community.



by Captain Jason Boslaugh and Mr. Bryan Lasater

Introduction

In 2017, senior signals intelligence (SIGINT) leaders from across the U.S. Army recognized Army SIGINT was not optimized to compete in large-scale combat operations against a peer threat. Army "SIGINTers" have become very proficient in the precision targeting of individuals; unfortunately, the skills associated with fighting against a peer threat in a large-scale combat operation have atrophied. These skills are needed to support overall situational understanding of the enemy, to include building network diagrams and creating target folders to underpin the enemy's electronic order of battle.

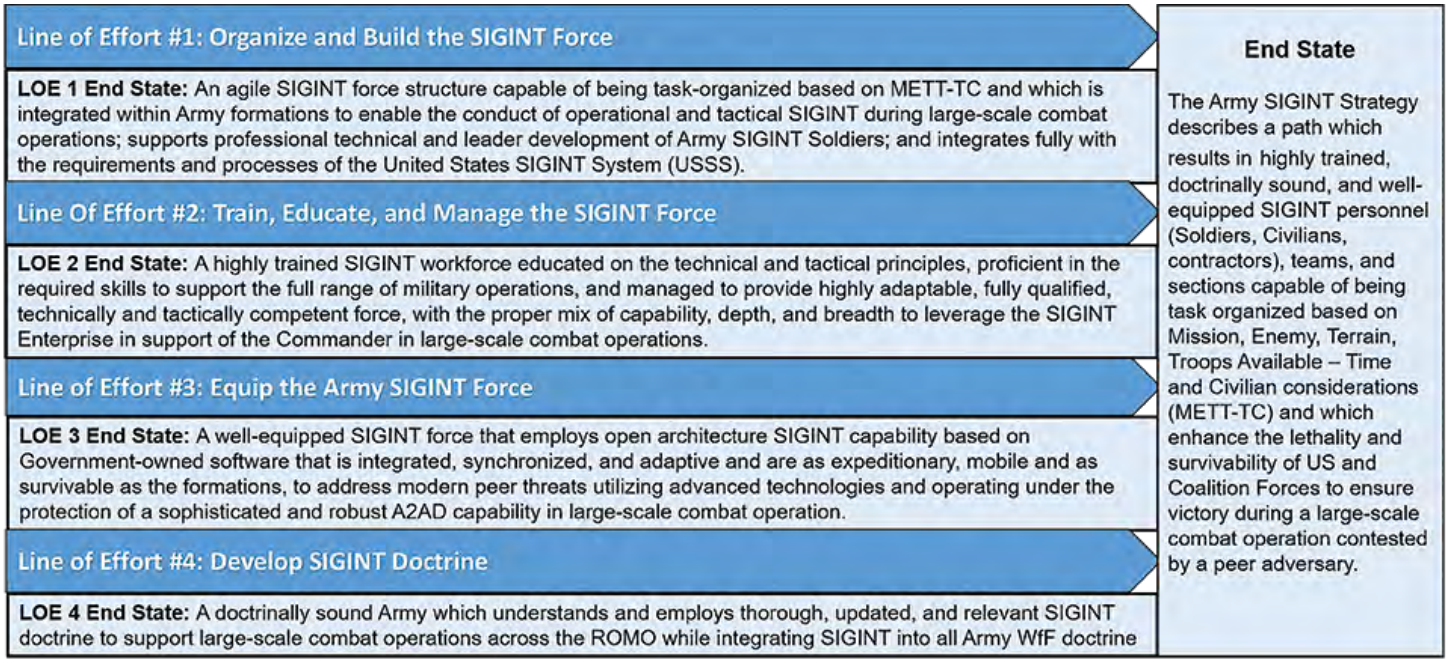
To establish a way ahead for Army SIGINT, the Deputy Chief of Staff G-2 directed a SIGINT deep dive to identify and develop ways to mitigate SIGINT capability gaps. In October 2017, the U.S. Army Intelligence Center of Excellence (USAICoE) hosted the SIGINT deep dive that brought together approximately 80 SIGINT subject matter experts representing various organizations across all Army echelons. The purpose of the deep dive was to achieve community consensus on a unified, feasible, and long-term SIGINT strategy. The *Army SIGINT Strategy*, completed in May 2018, ensures a well-equipped, well-led, professional force capable of achieving and maintaining the advantage in a multi-domain environment. The strategy uses a classic "man, train, equip" framework as lines of effort to concisely explain to Army intelligence leaders what we must do to reinvigorate the Army SIGINT force. The implementation of the *Army SIGINT Strategy*, in concert with the *United States Army Processing, Exploitation, & Dissemination Concept of Operations*, and the *Army Data Strategy*, will provide tailored expeditionary and reach SIGINT capability and enable a more holistic enterprise approach to support global SIGINT requirements. This article provides the Military Intelligence (MI) Corps with the major findings of the deep dive, which frame the *Army SIGINT Strategy* that provides the way ahead for Army SIGINT.

The Shift in Focus

Since 2001, the Army has been committed to fighting in a counterinsurgency environment. This led to decisions for optimizing the intelligence warfighting function's formations, training, and equipment to support the counterinsurgency mission. The decision makers included USAICoE, Department of the Army G-2, U.S. Army Training and Doctrine Command G-2, U.S. Army Intelligence and Security Command, and U.S. Army Forces Command G-2. With these decisions, the Army assumed risk to the intelligence warfighting function's ability to pivot effectively to conduct operations against highly competent and well-equipped peer adversaries. These changes, coupled with the high operational tempo of deploying Army units, resulted in an entire generation of MI leaders and Soldiers who have honed their skills operating in the counterinsurgency and limited contingency environments. The Army expertly adapted to the unique, unconventional challenges of counterinsurgency and demonstrated proficiency in asymmetric operations. However, peer and near-peer adversaries studied the U.S. military's evolution and adapted to counter the United States' advantages that had made us dominant in large-scale combat operations (e.g., Operation Desert Storm). As the Army transitions away from a focus on counterinsurgency-driven demands to focus on the highly kinetic, fast-paced large-scale combat operations, it is apparent the force must acquire new skills while maintaining the current scope of skills honed over the past two decades. Intelligence professionals must relearn and reintroduce many of the proficiencies from the pre-9/11 era, while adapting to enemy technological advances and managing exponentially increasing volumes of data. Although adaptability and flexibility are required across all warfighting functions, a case can be made that this transition will mostly affect the technical fields. Within the intelligence community, there is no discipline more impacted than SIGINT.

SIGINT Strategy Lines of Effort

Combinations of conventional state actors and unconventional non-state actors will likely affect the future operating environment. These actors will likely capitalize on technological advantages to enhance the command, control, communications, computers, intelligence, surveillance, and reconnaissance of their force structure. This increasingly complex environment includes a mix of modern communications and non-communications signals with a low probability of detection within the electromagnetic spectrum. On the future battlefield, the Army's ability to detect, collect, characterize, classify, locate, and attack these threat emissions is critical to force protection and enhanced lethality. To meet these requirements, the Army must meet significant objectives to ensure readiness against the full range of threats. The lines of effort that encompass these objectives serve as the framework of the *Army SIGINT Strategy*.



Lines of Effort and Desired End States

Success in these four areas involves building flexibility and adaptability into our force structure and developing our approaches to training. It also requires our equipping processes to remain state of the art while rapidly capitalizing on commercial and military innovation to sustain an advantage across the intelligence warfighting function. To achieve our goals, we must—

- ✦ Organize and build the SIGINT force.
- ✦ Train, educate, and more effectively manage the SIGINT force.
- ✦ Equip the SIGINT force in a rapid and agile manner.

SIGINT Collection Challenges

Over the past few decades, multiple iterations of force reductions and resource constraints (e.g., sequestration) have reduced the Army's SIGINT expertise, capability, and capacity at all Army echelons. Although the Army has been able to adapt to these limitations during crisis response and limited contingency operations, it must reassess and optimize the force design for current and future Army operational requirements. As the unit of action for large-scale combat operations shifts from the brigade combat team (BCT) to division, the intelligence warfighting function must ensure its organizational structure supports these changes. This occurs by accounting for national-to-tactical SIGINT integration and implementing a grade plate that supports professional development and mentorship of all intelligence personnel at all echelons.

Currently, SIGINT collection and processing, exploitation, and dissemination (PED) elements for echelons corps and below are allocated to expeditionary-MI battalions and BCTs as PED platoons, multifunction teams, and cryptologic support teams optimized for counterinsurgency operations. The allocation occurs using modified tables of organization and equipment. There is also limited SIGINT capability organic to our warfighting divisions and corps, performing primarily collection management, intelligence oversight/information assurance, and single-source analysis functions. BCT SIGINT operations

are critical because of the increased number of SIGINT sensors, as well as their vastly improved technical capabilities, and the close access to robust signals environments. This has resulted in substantially more data/information collected than ever before.

These factors have led to a significant shortfall in PED capacity at the tactical level, resulting in a focus only on high-priority SIGINT collection. Specifically, terrestrial layer SIGINT collection will typically exceed the assigned cryptologic linguist capacity at a BCT. The cryptologic support team provides SIGINT technical control, tasking, and analysis to support up to four multifunction teams. The cryptologic support team also performs SIGINT analysis functions for the BCT S-2 in coordination with requirements of the division G-2 analysis and control element SIGINT section. However, given the tactical focus on providing combat information and intelligence to the BCT commander and staff, the SIGINT focus is primarily on timely reporting rather than detailed analysis. The shift from BCT to division as the unit of action for large-scale combat operations and the operational convergence of SIGINT with cyber-electromagnetic activities may affect future force structure and concepts of employment; however, it will not affect the enduring requirement for MI units to perform SIGINT PED.

To further the issue of having too few SIGINT Soldiers at the tactical level, lessons learned and combat training center rotations suggest the BCT grade plate is too junior and provides a narrow window for SIGINT noncommissioned officer leadership, specifically cryptologic linguist sergeants, to mentor junior SIGINT Soldiers in tactical and technical tradecraft. This is due to the prolonged initial entry training for SIGINT Soldiers, particularly the linguists who reside at the BCT MI Company, combined with generally fast promotion rates to staff sergeant for those same cryptologic linguists.

Lastly, the elimination of the technical control and analysis element (TCAE) at echelon has limited the ability to provide the technical control and coordination of SIGINT enterprise assets. The TCAE structures previously provided numerous functions, such as ensuring legal compliance with the National Security Agency's policies and procedures, as well as synchronizing SIGINT analysis operations to derive intelligence required for technical steerage of SIGINT and electronic warfare collectors. The TCAE also provided direction that enabled collectors and analysts to answer a commander's priority intelligence requirements and provided support to indicators, warning, situational understanding, target development, and targeting. These tasks are complex and manpower-intensive, which further exacerbates organizational challenges.

Revitalizing SIGINT to Meet the Challenges

Army commanders require adept support from teams of SIGINT Soldiers and leaders capable of understanding, adapting to, anticipating, and exploiting experienced and sophisticated threat forces. Essential tasks that Soldiers must be able to perform include—

- Conducting focused information collection and PED.
- Providing warning intelligence.
- Providing intelligence support to situational understanding.
- Delivering support to kinetic and non-kinetic targeting during large-scale combat operations.

To meet these challenges and revitalize SIGINT, the Army must re-examine and make required changes regarding the SIGINT military occupational specialty allocation to Army echelons and the TCAE functionality at echelon. The Army must also re-examine opportunities for the mentorship of junior Soldiers and noncommissioned officers at the tactical level, and the integration of unique National Guard and Army Reserve capabilities to augment Active Duty SIGINT forces, such as using their robust linguist capability.

SIGINT Training

Organizing the force to keep Soldiers who are more senior "in the fight" and optimizing for a large-scale combat operation are only part of the equation. We must also train MI Soldiers and leadership to effectively employ and manage SIGINT assets for large-scale combat operations. The operational environment will only increase in complexity. SIGINT Soldiers face threats that are increasingly dynamic and sophisticated in their use of the electromagnetic spectrum. To gain and maintain proficiency, we must re-assess our approach to training and we must develop realistic training scenarios or bring real-world mission opportunities to home station, especially at echelons corps and below, so

U.S. Army photo by SGT Mark Miranda

Soldiers train on the PROPHET signals intelligence/electronic warfare system.

that SIGINT Soldiers can exercise their perishable skills and keep pace with the threat.

The Army's current approach to SIGINT training leverages joint institutional initial entry training, which does not address the Army's tactical SIGINT mission and equipment. This has resulted in Soldiers in tactical units having insufficient tactical SIGINT proficiency. Many SIGINT Soldiers do not understand their role. A greater concern is that they are unable to employ and operate their collection systems using proper field tradecraft. The transition to supporting combined arms maneuver in large-scale combat operations compounds this difficulty further when mobility is critical to survivability.

Lessons learned from combat training centers from 2012 to 2017 indicate a trend of consistent challenges. For example, SIGINT Soldiers receive ad hoc training and lack expertise on their systems. There is also reliance on BCT S-6 and intelligence and electronic warfare system maintainer personnel because of the complexity of intelligence systems. SIGINT training should incorporate the tasks performed and the equipment used at echelons corps and below. The creation of a tactical SIGINT course, currently under development at Fort Huachuca, Arizona, will seek to correct this shortfall. This training will be required for all Soldiers assigned to U.S. Army Forces Command units and will go a long way in increasing the knowledge base and proficiency of skill level 10 Soldiers as they arrive at their first duty station.

As Soldiers headed to the tactical edge receive increased training to operate effectively in large-scale combat operations, MI leadership must also be educated to effectively and consistently integrate SIGINT into the scheme of maneuver. Results from the intelligence 2025 bottom-up review survey indicate training is not adequately resourced to prepare Soldiers to conduct a mission. Lessons learned from combat training centers describe SIGINT resources as being inconsistently integrated into the BCT's concept of operations (CONOPS), creating a "chicken and the egg" scenario. According to this scenario, if MI leaders are unable to integrate SIGINT into the BCT's CONOPS, which includes describing the value SIGINT provides to a maneuver unit, then they are unlikely to receive adequate resources for training. On the other side of the coin, inadequately resourced SIGINT assets will likely not provide enough value to a commander to be fully integrated into the BCT's training CONOPS.

Platoon and company leadership must be well versed in ground SIGINT assets, as well as the employment of SIGINT assets in accordance with Army doctrine. Prior to the employment of Soldiers and assets, MI leaders must know how to effectively advocate for and manage resourcing. They must also understand the criteria to validate and certify their SIGINT sections. Most importantly, MI leaders at all echelons must be able to translate SIGINT technical capability into a practical explanation that describes exactly how SIGINT will enhance the lethality and survivability of a commander's maneuver units on the battlefield. Enabling our tactical MI leaders to improve their knowledge of SIGINT integration by investing in career-long training opportunities, in conjunction with a professional military education, provides an approach to increase SIGINT expertise within our formations. Leader training must cover the management of SIGINT collection, describe various training resources available to SIGINT Soldiers, and explain how to advocate for time and resources to train and certify SIGINT Soldiers. Additionally, the development of certification requirements for tactical SIGINT (parallel to existing intelligence community certifications) should be used to ensure training opportunities on a unit-training calendar.

Without specified requirements for SIGINT military occupational specialty proficiency, the subjugation of SIGINT training to other priorities will continue. By developing validated tasks, leaders can plan their unit training and take advantage of the Military Intelligence Training Strategy and Intelligence and Electronic Warfare Tactical Proficiency Trainer, which can provide realistic training opportunities and can help sustain the SIGINT Soldiers' technical and tactical proficiency.

U.S. Army photo by SSG Tamika Dillard, 2nd BCT, 1st ID Public Affairs

SGT Jacob Butcher, a squad leader in the 1st Infantry Division, troubleshoots a system during an electronic **warfare certification course at Fort Riley, Kansas.**

Optimizing SIGINT Equipment

In addition to an effectively organized and well-trained force, we must ensure that our Soldiers have the best equipment we can provide. Global threat actions; equipment; tactics, techniques, and procedures; and spectrum utilization are dynamic and varied. In order to address the evolving threat, U.S. Army SIGINT equipment needs to be sufficiently flexible, agile, and rapidly adaptable. The Army must optimize SIGINT equipment to support large-scale combat operations against peer adversaries by taking an approach using scalable hardware with an open architecture that runs government-owned software, algorithms, and standards. This method supports the intelligence warfighting function's ability to evolve rapidly to address changes to the threat. By creating systems in a well-informed and forward-looking fashion, we could ensure that software and minor hardware upgrades quickly identify and address the majority of changes to adversaries' tactics, techniques, and procedures; signal parameters; and electronic order of battle.

The Department of Defense's (DoD) "IT Box"[1] acquisition rules allow great flexibility and delegated approval authorities to address the need for agile fielding of an upgraded capability in software-heavy acquisition programs. Additionally, rapid development and fielding organizations within the DoD and intelligence community can be used to fill additional gaps in a reduced timeline. If we leverage the expertise of the entire intelligence community to identify the highest priorities, make smart hardware choices, and use agile acquisition and rapid fielding processes, we can ensure that our Soldiers have the best equipment available to accomplish the mission.

Conclusion

The Army faces a significant challenge adapting to the complex, dynamic, unpredictable, and highly variable global threats. It is critical to have an effective SIGINT capability to support a commander's ability to see, understand, decide, and act to "win in the unforgiving crucible of ground combat."[2] SIGINT is a linchpin for overall situational awareness in a large-scale combat operation, as there are many second- and third-order effects that arise from ineffective SIGINT collection. For example, many other ongoing efforts are dependent upon a robust SIGINT capability to be successful, such as PED and the use of data science to enable predictive analytics. Without SIGINT data, those two functions are degraded.

Just as retired GEN Ray Odierno referred to SIGINT as the coin of the realm in counterinsurgency operations, a well-trained and well-equipped SIGINT force can exponentially increase the ability for Army and strategic intelligence organizations to succeed against a peer threat. To improve SIGINT and the Army's intelligence warfighting function, intelligence leaders at all levels must work together to develop a "lethal, professional, and technically competent force"[3] while taking care of the troops. The *Army SIGINT Strategy* that the SIGINT community of interest developed is a step in the right direction to ensure SIGINT is postured to support the Army's priorities. However, the successful implementation of the strategy will require hard work, support, and expertise from Department of the Army staff, the SIGINT community, the MI Corps, and Soldiers and Civilians across the Army.

Endnotes

1. Recognizing the difficulty in keeping up with technology, the Joint Chiefs introduced the "IT Box" concept "to ensure programs meet cost, schedule and performance goals and focus on rapid and small increments. The IT Box approach also is trying to solve well-documented problems with how the Pentagon buys and implements technology." Jason Miller, "How an 'IT Box' is making it easier for DoD to do business," *Federal News Radio*, February 27, 2014, https://federalnewsradio.com/defense/2014/02/how-an-it-box-is-making-it-easier-for-dod-to-do-business/.

2. GEN Mark A. Milley, "39th Chief of Staff Initial Message to the Army," *U.S. Army Worldwide News*, September 1, 2015, https://www.army.mil/article/154803/39th_Chief_of_Staff_Initial_Message_to_the_Army.

3. Ibid.

CPT Jason Boslaugh currently serves as a branch chief for Single Source Intelligence Capability Development, Requirements Determination Directorate at the U.S. Army Intelligence Center of Excellence (USAICoE). He recently co-authored the Army SIGINT Strategy Paper. *His team conducts assessments in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) and determines future Army requirements for signals intelligence (SIGINT), geospatial intelligence, space, counter-unmanned aircraft system, human intelligence, counterintelligence, and data science to help prepare the Army intelligence warfighting function for the envisioned threat. Before this assignment, CPT Boslaugh served at 7th Special Forces Group (Airborne) as a military intelligence detachment commander and battalion S-2.*

Mr. Bryan Lasater has served as an intelligence capability developer at USAICoE since 2007. He co-authored the Army SIGINT Strategy Paper *and a number of capability development documents for programs focused on SIGINT, measurement and signature intelligence, ground robotics, and counter-unmanned systems. He is a U.S. Army veteran and has a bachelor of arts in psychology and a master of science in computer information systems.*

The Right Fit
Mission Command in the Twenty-First Century

Lieutenant Colonel Matthew T. Archambault
Captain Franklin G. Peachey
Captain Jennifer P. Sims

Editor's Note: This article is reprinted with the permission of Military Review, the Professional Journal of the U.S. Army, Combined Arms Center, Fort Leavenworth, Kansas. It was originally published online in the January 2018 Military Review, Online Exclusive.

The Army needs to have a more precise and open conversation about mission command. As U.S. Army Europe's opposing force at the Joint Multinational Readiness Center (JMRC), 1st Battalion, 4th Infantry Regiment (1-4 IN), known as the "Warriors," practices Army core competencies, specifically mission command, more than most units based on its mission set. Five or more rotations per year with varied task organizations have enlightened the Warriors' approach to Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command*, which we strive to pass along with this article.[1]

Successful mission command requires the proper organization of individuals outlined in a standard operating procedure (SOP), repetitive iterations of the military decision-making process (MDMP), and leverage of the appropriate technologies to enable communication. The following sections articulate the underlying reasoning and processes for how the Warriors develop SOPs, employ the MDMP, integrate intelligence,

Photo by SPC Naiomy Gaviria, U.S. Army

CPT Franklin G. Peachey, 1st Battalion, 4th **Infantry Regiment intelligence officer, reviews his current analog** enemy situational template after a battle in exercise Combine Resolve 8, which took place 27 May 2017 to 12 June 2017 at the Joint Multinational Readiness Center in Hohenfels, Germany.

and incorporate technology judiciously so that readers may be able to develop a mission command mindset within their professional relationships.

Role of the Commander

(Written by LTC Archambault, 1-4 IN Battalion Commander)

ADRP 6-0 invokes mission command's German ancestry, *Auftragstaktik*, but misses an important component of the German concept for mission orders and decentralized execution. Auftragstaktik received its name mostly after the fact, as part of an explanation for how the German army functioned. In short, Auftragstaktik was cultural rather than top-down.[2] Every aspect of the German army organization, personnel systems, and education supported and reinforced the lived expression of this concept. The Warrior Battalion's aim was to create that culture, where mission command was pervasive, and everyone operated on a common vision.

Everything starts with the commander. The commander must feel the pulse of the lived experience of the mission command principles within his or her team. Commanders must

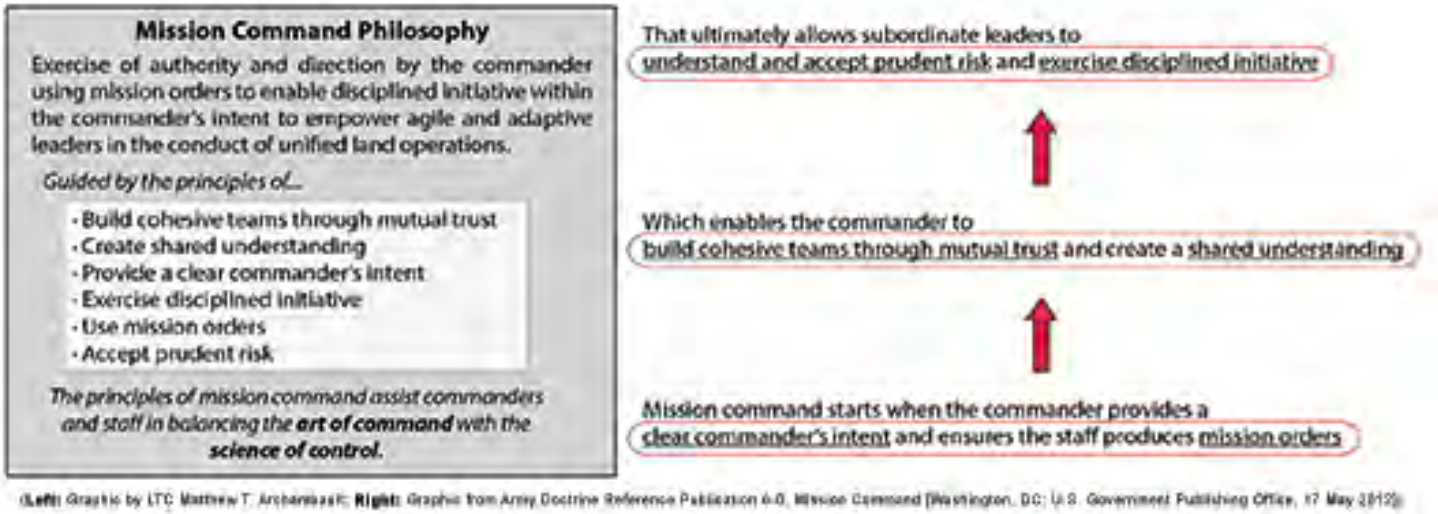
- know whether there is mutual trust between echelons,
- know whether they and their staffs have done everything to facilitate shared understanding,
- know their staffs and producing mission orders,
- be comfortable with and understand the disciplined initiative their subordinates take,
- communicate what prudent risk is for the formation, and
- provide clear commander's intent.

The Army is a people business, and the commander must emphasize the human dynamic with a nuanced and firm understanding of group communications and of how the group under his or her command understands and develops its particular processes and procedures.

Mission command philosophy at its best provides a lens for focusing energy, for deciding how to balance the art of command with the science of control. To focus energy properly, processes and procedures are not only important, they are also essential. ADRP 6-0 provides a graphic to explain its mission command philosophy. We revisualized the graphic into something more tangible. Figure 1 provides a side-by-side comparison. The revisualization establishes relationships between commanders at different echelons. For example, the disciplined initiative is crucial to the concept, but evinces itself in subordinate action as a result of mission orders, clear intent, and mutual trust.

Standard operating procedures and policies, when adequately written, establish relationships and expectations for the soldiers, noncommissioned officers (NCOs), and officers in the organization. The mission command SOP outlines how the battalion executes the MDMP, executes a combined-arms rehearsal, organizes its tactical operations center (TOC), and manages information and knowledge.

A mission command SOP is not a regurgitation of doctrine. It outlines and provides guidance on how



(Left: Graphic by LTC Matthew T. Archambault; Right: Graphic from Army Doctrine Reference Publication 6-0, Mission Command [Washington, DC: U.S. Government Publishing Office, 17 May 2012])

Figure 1. Mission Command Philosophy

subordinates should act, what their responsibilities are, and what they can expect from others depending on the situation. All SOPs should reduce stress and friction because people know, without being told, what is next. Effectively, the SOP organizes how the staff advises and informs the commander, and it assigns responsibilities among the staff, so the battalion commander does not have to be a staff officer. In large part, success in command includes developing and enacting successful processes for refining SOPs that are team-driven rather than top-down.

Culture builds around relationships. A battle captain, whether a captain, an extra lieutenant, or an NCO, must know what to expect of his or her radio operators and the operations sergeant major. The same is true for MDMP or any process the battalion executes. Everyone on the staff ought to know the position—not the individual because individuals come and go—that is responsible for leading course of action (COA) development.

lenge for those not afforded the opportunity of multiple combat training center rotations is to execute MDMP routinely at home station for annual training guidance, platoon live-fire exercises, and other events that usually fall into the hands of a single staff officer. Whatever the training constraints, it is incumbent upon the commander to treat development and refinement of SOPs as the standard-bearer of shared understanding and development of collective performance excellence.

In accordance with Field Manual 6-0, *Commander and Staff Organization and Operations*, the battalion commander takes mission analysis and COA development briefs from the staff.[4] These briefings are vital for MDMP and, as discussed above, the battalion's culture. These briefings might happen across days, or they might all occur within a single day; mission requirements drive the planning timeline. I never provide directed courses of action. This is the staff's opportunity to show me what I do not know, and

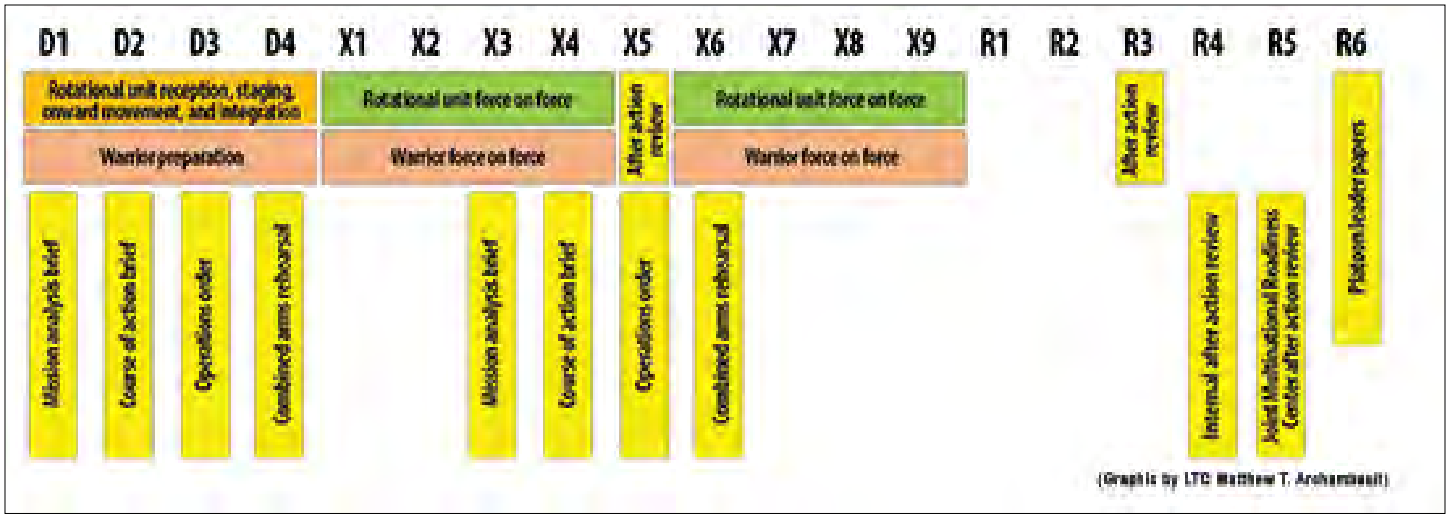


Figure 2. A Typical Military Decision-Making Process Schedule during a Rotational Exercise

The expectations for these relationships find expression in SOPs. When the SOPs are repeatedly used, the culture of the unit rises to a higher standard because everyone knows how the unit executes its systems.

The Warriors conduct MDMP at least twice during rotation, one for an offensive operation and one for a defensive operation, five to six rotations per year. That is an incredible amount of opportunities for the battalion commander, staff, and subordinate commanders to gain a shared understanding and transform that understanding and relationships into SOPs. Figure 2 illustrates the general timeline.[3] The challenge me with their ingenuity. Time-dependent, they will wargame both COAs and provide me a COA decision brief.

The dialogue that ensues from these briefs is invaluable. The staff gains an appreciation for how I think and see the battlefield. I am verbalizing my thoughts and creating a vision for what will happen. There are no unexplored assumptions. There can't be if a true dialogue is to occur, hence my organizing briefs so that the staff provides COAs.[5]

Ultimately, after the discussion, I decide on the COA, and the staff briefs the operation order to the company

commanders. The mission command SOP guides touchpoints for the commander, regardless of the mission set. The science of control, the SOPs, guides us through understanding, visualizing, describing, and directing. Throughout the entire synchronization issues that require a fragmentary order. We make the fix on the spot and rehearse the plan again. These are conversations with the subordinate commanders and principle staff. The augmenting commanders provide the greatest opportunity to challenge our way of business because they are new to the battalion. For them, this is all new. It is a training process of preparing my people for successful engagement in conflict, I am using twenty years of experience, the dialogue with staff and commanders, and finally, the combined-arms rehearsal to refine that visualization and share it.

The Warrior Battalion contends with uncertainty and complexity every rotation. Task organization is never the same, even changing between a single rotation's battle periods. We always have new teammates: a National Guard company, a U.S. Army Reserve company, and often a multinational company. We are also fighting a different enemy every rotation with different capabilities. Sometimes we are fighting a mechanized formation or Strykers, and it is always multinational. Executing battalion-level battle drills would not challenge our opponents, the rotational unit.

My commanders, organic and augmenting, provide me with a confirmation brief immediately following the operation order, and then a backbrief a day or two later. A combined-arms rehearsal follows on a terrain model, which enables leaders down to the platoon level to walk through the operation. Without fail, we discover changes to the plan or opportunity for both of us, which we do again, during the defensive planning cycle.

Now we go out to fight. Personal experiences and technology will influence the idea about how a commander fights on the field, where he should be, etc. However a commander conducts himself, the procedures must refine the process of information flow. Most of the time during the fight, my visualization of events comes from a radio transmission. Today, commanders do not "see" anything. Therefore, it is essential that battalion leadership, from the commander to the platoon leaders, understand and are comfortable with well-tested communication strategies so that nearly everyone continues to maintain shared understanding to the fullest extent possible.

We are a people business. Every aspect of our profession is about people. There is no getting away from people, and there is no getting away from Murphy's Law, friction, fog, and the general chaos of the battlefield. Warfare has not changed enough to preclude the requirement of the commander to place himself wherever he feels it is necessary to best influence the battle. Some may feel that is the TOC. For myself, it is a mobile tactical command post (TAC), with two HMMWVs, the operations officer's (S-3's) and mine.

Where we go changes every rotation. Sometimes I get an inkling during the combined-arms rehearsal that a company may need help so that I may follow them. Sometimes it will be the main assault. Other times it is with the breach. It is never the same. One way to cope with the friction is to develop this intuition through trial and error during training exercises.

I go that close to the front because it is necessary. Some might ask, what about Joint Capability Requirement (JCR)?[6] We have it, but it is not fast enough. It loses satellite links and goes stale during operations in the dense terrain of Europe. Analog maps continually prove to be faster. Below, the Warrior's signal officer discusses how our battalion integrates communication technology in greater detail.

What are we doing in the TAC during the fight? At this point in the process, we are placing trust in our refinement of the SOPs and relationships and opening up to the "art" of command. Sometimes we are evading enemy scouts. Most of the time, we are standing around, listening to the nets, looking at a map, and thinking. This is the best part. This is the payoff. After all of the preparation with MDMP and the conversations, after all of the visualization I have done, I now get to listen over the radio and see if I recognize what is going on. I do not have to troubleshoot procedure or clarify my intent—my focus is on staying with the information flow so that I can be at the right place at the right time to weigh in. My S-3 fights the battalion. He will come to me for the big decisions. I stay off the net. My intelligence officer (S-2) sits behind me. My truck has three radios, I listen to two nets, and my S-2

listens to the operations and intelligence net. I keep one ear on the battalion command net and the other jumping around on the company command nets, passively listening. My executive officer updates higher headquarters. This is a command. The S-3 is fighting and I am assessing my vision for the reality playing out in the field.

When the rotation is over, after we have experienced how the SOPs functioned, we refine as necessary. Every day, while we are going through preparation or execution, I am making notes about our SOPs, subordinate leaders, and warfare in general. The Army is rebuilding its combined-arms maneuver war machine, and no one really knows what it looks like. It will not be our grandfather's Oldsmobile, AirLand Battle, but it might not be far from it either. After-action reviews (AARs) are the principal method for refining these SOPs, and AARs must involve the commander to ensure the AAR is not a frivolous event.

What is the organization reviewing? Against what standard, and how do we judge the actions that our subordinates and we took? The answer ought to be our doctrine, our SOPs, and our policies. The organization cannot directly affect Army doctrine, but it owns its TACSOP and mission command SOP. The organization cannot change Command Post of the Future, but it does not necessarily have to use it when it does not make sense. Commanders must feel the pulse of the technology used within the formation and know its effects on mission command.[7]

This is the crux of a learning organization. Commanders support and guide the process of collective reflection and refinement. Commanders should ask, how do I know my organization is learning?[8] Where can I find evidence of that learning? From a different perspective, is my current organization or procedures to support that organization proper for the situation within which I find myself ? That is why SOP refinement is not the responsibility of a single staff officer, but an organizational responsibility led by the commander.

A leader azimuth check is a method for all the organization's leaders to come together, discuss their SOPs, and determine how to make them more effective. That annual conference helps impart several principles of mission command to include the obvious shared understanding and mutual trust. When the commander creates these events and is involved in the process, subordinates are learning how he or she communicates—the meaning behind his or her words, gestures, and idiosyncrasies. Giving subordinates the opportunity to develop this understanding of their commander creates the conditions for mission command philosophy to permeate the group culture.

As brilliant as commanders like to think they are, the reality is that no commander speaks clearly, concisely, or brilliantly all the time. Once SOPs are functional—maybe not perfect but good enough—the AARs for exercises and training events can be elevated to a much higher level. Now, the organization can stop trying to figure out how to do something, and it can begin figuring out how to do it better than anyone else, to realize something new.[9] This—the collective reflection and refinement of processes—is the opportunity to appreciate intangibles on the battlefield like time, terrain, and friction. Those three things affect every unit, but the unit with sound mission command, whose SOPs are effective, will not succumb to them. Some concluding recommendations for commanders follow:

- Get numerous and honest repetitions at MDMP. You do not want your focus to be how you are going to do MDMP. You want to focus on what you have learned from MDMP.
- Do not pretend you know everything. Listen to your staff. Challenge them, but allow them to challenge you. You might know how best to run a motor pool or live-fire exercise, but on a combined-arms maneuver battlefield, it takes a team effort. You need practice with understanding, visualizing, describing, directing, leading, and assessing.
- Check your SOPs. Are they being used? Do they make sense? The SOP prevents you from having a conversation about how to do the process and instead maximizes the process so you can focus on the end state.
- Task organize for every mission. One size does not fit all. The result is a new team at every echelon, which demands you ensure you have communicated clearly and that shared understanding exists.

Intelligence Warfighting Function

(Written by CPT Franklin Peachey, 1-4 IN intelligence officer)

Intelligence within tactical mission execution exists simply to support the commander with relevant, predictive, and tailored assessments.[10] An assessment is not a certainty; instead, it is a delicate balance between logical problem solving and the use of an informed intuition. When time is of the essence, this balance relies to a greater degree on an officer's informed intuition. To integrate these intelligence assessments within a mission command system, a close working relationship between the commander and the intelligence officer is crucial. The S-2 must understand the commander's decision-making process and gain trust.

Intelligence sections exist to organize the ever-growing amount of information flowing into a TOC and then condense that information into intelligence for an assessment to the commander. This is not a mechanical procedure that can follow a rote formula. The S-2 must balance time committed to logical problem solving (informing battlefield visualization) with assessments made through informed intuition (providing predictive analysis).[11] Below is a tactical situation that demonstrates the need for an effective balancing of both.

A reconnaissance attack identifies a dismounted infantry company defending a hill, clearly isolated and unsupportable from their main battle line. The S-2 makes a rapid assessment of where the enemy may maneuver that company. Logical problem-solving dictates parameters of time available for movement, distance to the next defendable piece of terrain, etc., but the S-2 must make a rapid assessment that enables the commander to take action to exploit a tactical advantage. Instead of laying out all possibilities in a logical problem-solving process, an experienced S-2 uses informed intuition to provide a rapid assessment to the commander of where that combat power is going to shift. There is no certainty in war, and there is no time to incorporate every possible data point into the assessment that can lead to analytical paralysis, forfeiting an intelligence officer's chance to effect time-sensitive decision-making.

The intelligence section is the tool within the battalion to execute deliberate thinking about the enemy, but "the fruits of that type of analysis can set the stage for rapid cognition."[12] The S-2 must balance reviewing a mountain of analytical data points provided by the section with the need for a rapid assessment. This must be done by intuitively deducing from that mountain those data points that are most useful in producing a relevant, predictive, and tailored assessment for the commander's immediate use. This is possible through clearly defined processes and procedures for organizing an intelligence section, which aids both in the tempo of these assessments and their accuracy (see figure 3, page 49). Without taking the time to define and refine processes and procedures, intelligence teams will not be able to develop fully the balancing of logical problem solving and informed intuition within the heat of battle.

Just as a maneuver element will reflexively execute a battle drill when making unexpected contact, an intelligence section must have clearly defined battle drills to execute intelligence preparation of the battlefield (IPB), MDMP, and battle tracking (see figure 3, page 49). An intelligence section must have a tailored task organization and troops-to-task to support IPB, MDMP, and battle tracking, independent of the personalities involved. In order to develop these systems, the intelligence officer must evaluate in detail the tasks to be completed and manage talent accordingly; a holistic excel document can serve as a base knowledge management tool for these systems. With personnel aligned against each task, the section can develop, refine, and rehearse battle drills and SOPs.

The next objective is to achieve mastery. Repetition is not enough to achieve mastery.[13] For true mastery, the section must plan, prepare, and execute its own staff exercises to rehearse and ingrain the task organization, battle drills, and SOPs.

These staff exercises do not need to be elaborate, or significantly time-consuming. Instead, they should be tailored to build muscle memory during moments of significant fluidity (e.g., TOC movements, battle tracking during main attacks, and rapid IPB execution after identification of significant changes in the operating environment). With these systems and practices in place, privates in the Warrior Battalion for less than

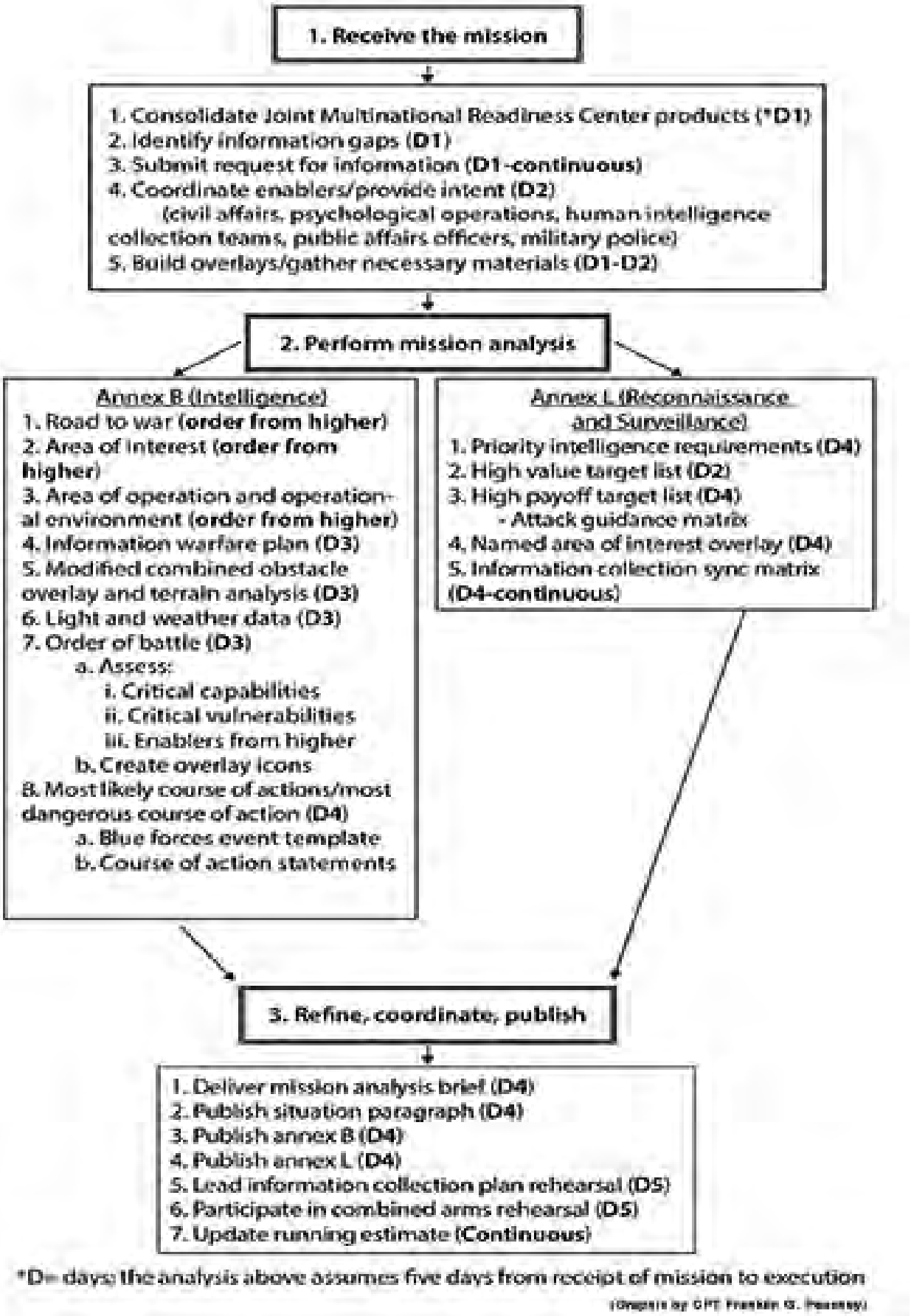


Figure 3. Battle Drill 1: Intelligence Preparation of the Battlefield

a year have the confidence in themselves and their team to take the initiative and make intuitive leaps in an analysis that they would not have previously. This preparation enables an S-2 to focus the analytical skills of the section, which in turn feeds directly into the informed assessments developed during the planning process.

As the intelligence section begins planning, it incorporates the logical and intuitive capacity of the entire staff. IPB is not completed in isolation. The executive officer sponsors it, and the S-2 facilitates it. The S-2 uses the analysis provided by the section and the staff to develop the enemy's courses of action. An S-2 must continuously seek additional input from the staff and commanders during COA development but remain cognizant of the source in the development of their assessment. When the S-2 briefs mission analysis to the battalion commander, it is on behalf of the staff and their collective analysis.

ing MDMP in earnest, the S-2's role becomes two-fold. First, initial movement of collection assets begins while the intelligence section continually revises its assessments as the data begin to flow. Secondly, the S-2 plays an active role in friendly COA development and war-gaming. When the staff begins war-gaming, the intelligence officer comes to the table with a fundamental understanding of the enemy's composition, and has coordinated for collection assets to begin to refine the details of enemy disposition.

During war-gaming, the intelligence section must be confident in their assessments to give the battalion staff an accurate perspective of the threat. The war-gaming session should be frustrating, even contentious. The S-2 is the spoiler to all the hard work and best-laid plans the staff develops. The same is true once the commander selects a friendly COA and the battalion moves to the combined-arms rehearsal. The S-2 must act as the spoiler and incorporate the

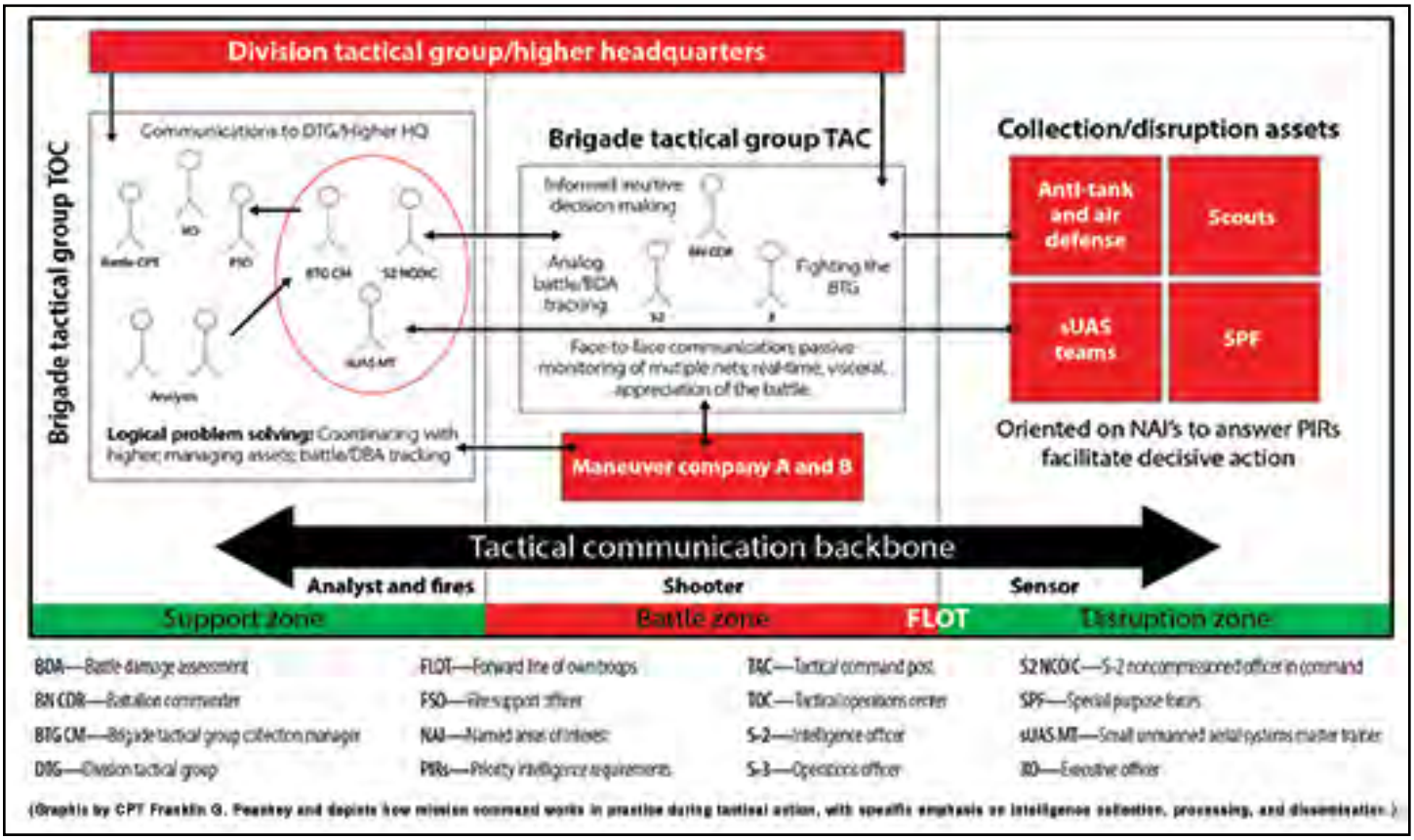


Figure 4. 1st Battalion, 4th Infantry Regiment Intelligence Mission Command Document Template

Concurrent with the development of COAs, the S-2 works closely with the collection manager and operations personnel to establish priority intelligence requirements (PIRs) and align collection assets. Once the S-3 approves the PIRs and the staff begins execut-

enemy's combined-arms approach simultaneously within multiple domains to give the battalion an accurate look at the risk to be mitigated in their plan. This pressure encourages maneuver commanders to react deliberately to likely enemy actions, developing

shared understanding across the battalion as they do so. Overall, the intelligence officer must synchronize the section's assessments across the staff and be confident in their presentation during key MDMP events.

Once this planning phase ends, the importance of an ingrained mission command system within the battalion and the intelligence section grows exponentially. As reconnaissance elements gain and maintain contact with the enemy, analysts are sorting and consolidating the reporting, then feeding it to the collection manager, the small-unmanned-aerial-system master trainer, and the intelligence NCO in charge of the TOC intelligence cell. With this initial analysis, the intelligence cell updates the common operating picture and the battle damage assessment, answers PIRs, coordinates relevant targeting information with the fires cell, pushes actionable intelligence to the TAC via the operations and intelligence net, and continuously refines the employment of collection assets (see figure 4, page 50). A synchronized section using an ingrained mission command system can better multitask and more efficiently conduct analysis and intelligence dissemination.

Beyond these battle-tracking tasks, the intelligence cell uses two specific synchronization sessions a day to maintain a shared understanding across the force. First, the intelligence cell conducts an intelligence synchronization with the reconnaissance company. This includes reviewing the common operating picture, adjusting PIRs, validating named areas of interest, and refining the collection plan for the following twenty-four hours. From this synchronization, the S-2 refines the enemy COA and provides an updated assessment during the second daily synchronization session, which consists of both an operations and an intelligence update brief to all commanders.

By collocating with the commander during the fight, the S-2 can have face-to-face communication and can gain a real-time appreciation for the fluidity of the battle (see figure 4, page 50). The S-2 must balance a dependency on information from the intelligence cell with his or her own analog tracking systems. The two vital pieces of information that the commander needs about the enemy are always enemy disposition and composition (battle damage assessment and relative combat power analysis). A simple means of tracking through an analog system is by having a pushpin board continuously synchronized with information from the intelligence cell.

There must be a balanced use of analog systems with technological enablers. Whether due to sophisticated electronic warfare jamming or to the threat posed to survivability that a large digital presence will have, all elements must be prepared to execute mission command and combat operations in a digitally denied environment. It is crucial not only to understand the threat but also to continuously train to operate in a nonpermissive environment. Ultimately, it is the S-2's duty to provide relevant, predictive, and tailored assessments to the commander no matter the technical or tactical constraints.

Some concluding recommendations for intelligence officers include the following:

- Train and use the intelligence section for logical problem solving; keep informed and be available to make the intuitive leaps in the analysis when they are necessary.
- Be informed and available to provide relevant, predictive, and tailored assessments to the battalion commander at all times.
- Owning IPB as a staff process is critical to the successful execution of MDMP. Bring your NCOs, other members of the staff, and the commanders to discuss enemy COAs.

Mission Command Warfighting Function

(Written by CPT Jennifer Sims, 1-4 IN signals officer)

Communications technology (CT) permeates human existence at an ever-increasing rate, with a piece of digital CT for every aspect of life.[14] The U.S. military is not immune to this, as digital CT covers every echelon and function, despite the Army not taking a significant philosophical look at technology.[15] While CT's ability to overcome human communication gaps is obvious, there is an improper association that more technology is good. In land conflict, one must consider the impacts of CT on mission command. While CT overcomes shortfalls in human capability, CT is not synonymous with mission command, and its current pervasive application degrades the human aspects of executing mission command and leads to an undesirable reliance on CT for this execution. The mission

command war-fighting function uses personnel, networks, information systems, processes, and equipment to facilitate how commanders and units fight rather than dictating that commanders and units use prescribed technology.

Mission command is a human endeavor, while CT is merely a tool that can overcome human limitations. CT allows the human voice to carry over unlimited distances, it allows for virtually limitless storage of information and data, it creates a means for multiple people to share input on data collection and processing to create information, and it provides the means to share that limitless storage of collaborative products over an unlimited distance. This grants a substantial capability to commanders at all levels when executing mission command, but leads units to focus on CT when establishing mission command systems. Most people immediately think of specific CTs when someone mentions mission command. CT, however, only makes up two components of a mission command system, networks and information systems, and not personnel, SOPs, or facilities and equipment.[16] This narrow focus creates a situation where commanders attempt to fill gaps in the other components of mission command with CT.

Land conflict is a complex venture. The number of variables that can affect any operation is immense, if not infinite. From factors ranging across a spectrum such as weather or enemy actions, most plans will face unexpected elements during their execution that require deviations. A holistic mission command system allows units to adjust to these variables without further direction from their command. A system that relies upon CT will require command intervention and undermines the inherent value of Auftragstaktik.

CT provides an illusion of situational understanding when every unit at every level is capable of seeing every other unit's exact position. CT facilitates ad-hoc querying of an icon for what that unit may be doing but does not synchronize the unit. CT cannot make a commander's intent clear or help units adjust quickly when they miss the intent. CT cannot tell a unit what to do when they are unsure. CT cannot mitigate risk or explain what disciplined initiative may be in the face of that risk. CT does not adequately make up the intangibles within the art of command if a unit ignores the human dimensions. CT merely enables people, placed in the proper locations with the proper tools, to execute well-defined and practiced SOPs. When a unit does not give proper deference to the human aspects of mission command, a commander, or a member of their staff, must use CT to resolve unexpected events instead of the unit merely responding.

Mission command in 1-4 IN is people executing their assigned duties in accordance with rehearsed SOPs. CT allows people to reach out further than they may have otherwise been able to, but it does not place individuals where they need to be or execute SOPs autonomously. Only a well-practiced SOP ensures data and information collection and dissemination occurs properly and reaches the requisite people. With the SOPs for the execution of mission command, a commander and the S-6 can employ CT with an accuracy that is more precise than spreading CT to every spot it can be.

When CT is ubiquitous, it is significantly easier to rely on it rather than develop and practice SOPs. One can visualize reliance on CT and the human dimension of mission command as having a linear relationship, where the less a unit focuses on the human dimension, the more reliant they are on CT, and vice versa. Decreasing reliance on CT is desirable, as it carries enemy and friendly vulnerabilities to reliability. Everyone has experienced one of these vulnerabilities and knows the frustration when a relied-upon system fails, leaving one unable to communicate.

Enemy electronic warfare and cyber capabilities have the ability to deny, disrupt, and degrade analog and digital communications, but enemy vulnerabilities also extend beyond the electronic warfare and cyber domains. Digital CT in command posts requires significant equipment, including a satellite dish placed outside of tree coverage and logistical efforts that create increased vehicle traffic, all of which give a large visual signature for direct or indirect targeting. Vehicles with digital CT require a satellite connection, meaning tree cover or steep terrain inhibit systems from functioning properly, and a recent publication theorized the potential compromise of computer systems onboard combat platforms making the whole platform combat ineffective.[17]

Friendly vulnerabilities can be both external and internal, some of which are interference, network congestion, misconfiguration, or malfunction. Units that

are highly reliant on CT are likely to have many CT devices in use, increasing the specter of interference between systems as well as causing congestion from multiple people attempting to communicate via the same means at the same time. Internally, a human will still have to configure CT systems, both physically and technically, creating the potential for human error to lead to a misconfiguration. While training and system testing can reduce this risk, some functions are only testable at the point they are necessary, such as a radio system reaching a given point, or a battle tracking system receiving and sending multiple streams of data from and to multiple locations. The ability to fix the misconfiguration and restore service can vary greatly between people and systems, but the vulnerability to imperfect reliability remains.

These vulnerabilities make overreliance on CT dangerous. While some reliance is unavoidable, reducing reliance on CT to the lowest possible levels lowers the threat. A unit reduces reliance by focusing on the human dimension and taking a surgical approach to the application of CT. 1-4 IN relies on SOPs for conducting mission command and takes a precise approach for selectively integrating CTs to connect people and not for explicating their responsibilities or placing them in the proper locations. Lower echelons have well-defined boundaries, phase lines, code words, and mission sets, so knowing where other units does not require looking at a screen, only normal situational awareness. As a result, the Joint Capability Requirement screens remain black.[18] Rather than Command Post of the Future, the battalion uses an analog map. The unit ensures a robust very-high frequency (VHF) radio network rather than ultra-high frequency radio channels because the tactical command post is almost always in a position to communicate with the entire formation. Finally, a rigidly enforced communications contingency plan sets an expectation for when communications become degraded; 1-4 IN focuses on the human dimensions of mission command, using CT precisely and reducing risk from its vulnerabilities.

Some concluding recommendations for signal officers include the following:

- CT plans have a primary, alternate, contingency, and emergency (PACE) methods for a reason. If your higher headquarters dictates CT that does not make sense for your operations, provide them feedback and use the auxiliary means as appropriate. Operations dictate communications, not the other way around.
- Establish the communications plan based on a deep understanding of current operations. Changes in the maneuver plan will necessitate changes in the communications plan.
- Ensure the formation understands the impacts from using or not using each piece of CT. Remember that these impacts are not restricted to the communications realm.

Conclusion

The Warrior Battalion practices its trade over and over again, without the distractions inhibiting other battalions and brigades. We also do not have a higher headquarters with an information demand mandating usage of specific mission command systems that are not conducive to maneuver. Luxuries aside, the Army can benefit from the JMRC's perspective within the continued dialogue about mission command; so, as combined-arms maneuver competence evolves, it is not being inhibited. The alternative is to place the desire for combined-arms maneuver at the altar of communications technology rather than the demands of the situation.

A generation of leaders are comfortable with CT based on their experiences in the contingency operations in Iraq and Afghanistan, where those systems have evolved. However, the necessities of combined-arms maneuver are different just as the assumptions across the range of military operations for leveraging mission command and utilizing CT vary. The authors of this article have vast experience in Iraq and Afghanistan in a variety of positions. Those experiences formed, in part, the optic for how we've viewed mission command not only for this paper but also for fighting this battalion. This battalion's experience has been that effective mission command emerges when commanders ensure their organization and systems are clear and codified in SOPs; plan thoroughly, and often, so the entire team understands each other and trust emerges; and execute based on the command's needs, not on constraints imposed by technology. It is our sincere hope this article helped further the dialogue and perhaps provided a useful insight into mission command.

Notes

1. Army Doctrine Reference Publication (ADRP) 6-0, *Mission Command* (Washington, DC: U.S. Government Publishing Office [GPO], 17 May 2012).

2. John T. Nelsen II, *Auftragstaktik: A Case for Decentralized Battle* (Fort Belvoir, VA: Defense Technical Information Center, September 1987), 21.

3. 1-4 Infantry Regiment (IN) receives an order from the Operations Group, Joint Multinational Readiness Center for each phase or battle period during a rotation. While there are directed actions, or injects, to achieve training objectives, and the unit must update its higher headquarters and backbriefing the Operations Group, the Warrior Battalion experiences "free play"—the ability to plan and fight as freely as the opposing rotational unit.

4. Field Manual 6-0, *Commander and Staff Organization and Operations* (Washington, DC: GPO, May 2014), 9-3.

5. Peter Senge, *The Fifth Discipline: The Art & Practice of Learning Organization* (New York: Random House, 1990), 217. "When a team becomes more aligned, a commonality of direction emerges, and individuals' energies harmonize. There is less wasted energy. In fact, a resonance or synergy develops…There is a commonality of purpose, a shared vision, and understanding of how to complement one another's efforts."

6. Joint Capability Requirement is the incremental upgrade of Force XXI Battle Command Brigade and Below, and Blue Force Tracker.

7. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1987), 261. "No single communications or data processing technology, no single system of organization, no single procedure or method, is in itself sufficient to guarantee successful or even adequate conduct of command in war."

8. Senge, *The Fifth Discipline*, 220–21. "The discipline of team learning requires mastering the practices of dialogue and discussion…the discipline of team learning requires practice."

9. Daniel Goleman, Focus (New York: HarperCollins, 2013), 28. "If we haven't practiced enough, all of these (activities) will take deliberate focus. But we have mastered the requisite skills to a level that meets the demand, they will take no extra cognitive effort—freeing our attention for the extras seen only among those at the top levels."

10. Army Doctrine Reference Publication (ADRP) 2-0, *Intelligence* (Washington, DC: U.S. GPO, 31 August 2012), chap. 2-2.

11. Malcom Gladwell, *Blink: The Power of Thinking without Thinking* (New York: Little, Brown, 2005), 141. "Truly successful decision-making relies on a balance between deliberate and instinctive thinking."

12. Ibid., 141.

13. Malcom Gladwell, *Outliers: The Story of Success* (New York: Little, Brown, 2008). Gladwell describes how "researchers have settled on what they believe is the magic number for true expertise: ten thousand hours." Whether it is actually closer to eight thousand or to twelve thousand, one thing is clear: if someone is going to be an expert in their field, they must strive for maximum repetition.

14. Drew Silver, "Chart of the Week," Pew Research Center, last modified 14 March 2014, accessed 7 November 2017, http://www. pewresearch.org/fact-tank/2014/03/14/chart-of-the-week-the-ever-accelerating-rate-of-technology-adoption/; Daniel Burrus, "The Internet of Things Is Far Bigger than Anyone Realizes," Wired (website), November 2014, accessed 7 November 2017, https://www.wired. com/insights/2014/11/the-internet-of-things-bigger/.

15. "Project Manager Mission Command," PEO-C3T (Program Executive Office Command Control Communications-Tactical) (web- site), accessed 17 November 2017, http://peoc3t.army.mil/mc/.

16. ADRP 6-0, *Mission Command* (Washington, DC: U.S. GPO, 17 May 2012), 3-8–3-11.

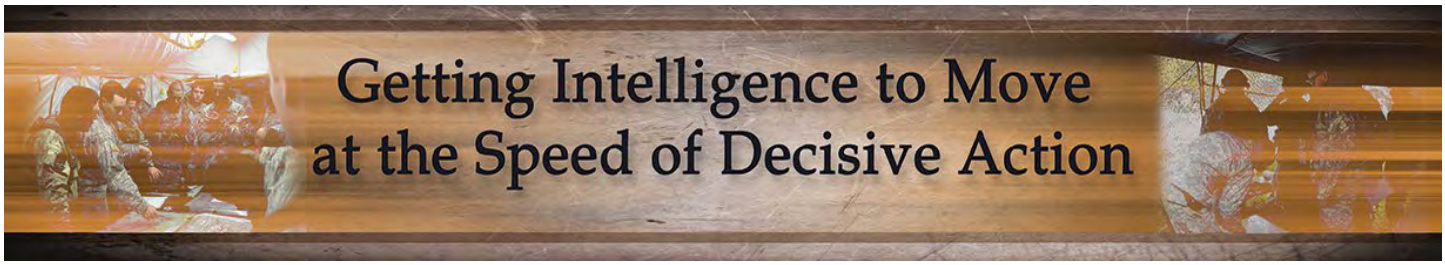
17. Asymmetric Warfare Group, *The Defense of Battle Position Duffer: Cyber Enabled Maneuver in Multi-Domain Battle* (Fort Meade, MD: Asymmetric Warfare Group, 2016), 5–6.

18. Two key issues keep 1-4 IN from greater use of Joint Capability Requirement systems, the speed of position-location updates and the requirement to connect to a satellite. In high-intensity conflict, units are moving faster and events are taking place quicker than the rate of updates, meaning commanders using the systems are receiving inaccurate information and thus making potentially incorrect decisions. Additionally, units must operate in tree cover and steep, undulating terrain, both of which can degrade the connection to the satellite. This effect increases the further north operations take place.

LTC Matthew Archambault, U.S. Army, is a senior observer-controller/trainer at the Joint Readiness Training Center. He holds a BS from the United States Military Academy and an MS from the School for Advanced Military Studies. His battalion command was in Germany, and he previously served at Joint Base Lewis-McCord with deployments to Afghanistan.

CPT Franklin G. Peachey, U.S. Army, is the intelligence planner for the Joint Multinational Readiness Center at Hohenfels, Germany. He holds a BS in secondary education from Millersville University and an MA in diplomacy from Norwich University. He previously served as a battalion intelligence officer, a scout platoon leader during a deployment in Afghanistan, and a company commander at the National Security Agency.

CPT Jennifer Sims, U.S. Army, is a signal planner for the Joint Multinational Readiness Center in Hohenfels, Germany. She holds a BS from Florida Atlantic University and an MA in international relations from Webster University. Her assignments include tours in Hawaii and Afghanistan, and most recently she was the signal officer for the Opposing Forces Battalion at the Joint Multinational Readiness Center.



Getting Intelligence to Move at the Speed of Decisive Action

by Captain Alex Morrow and Captain Michael Dompierre

To find, know, and never lose the enemy
—Military Intelligence Creed

Introduction

At the outset of the U.S. Army's return to decisive action and unified land operations, CSM Lance P. Lehr, who was at the time Command Sergeant Major of the National Training Center (NTC), said that a decade of combat in Iraq and Afghanistan had left us "very good at [counterinsurgency] COIN operations…going into a mature theater where we have all of our enablers and all of our sustainment [in place]."[1] As a consequence, he admitted that "we got a little rusty on the combined-arms maneuver—going out and fighting the near-peer competitor with tanks and Bradleys and artillery."[2]

Countless leaders at every echelon echoed CSM Lehr's assessment in the years since, and it is just as applicable to our intelligence enablers and assets as it is to our maneuver forces. On the analytical side, MAJ David Johnston, who served as the brigade combat team (BCT) S-2 for 3rd Armored Brigade Combat Team (ABCT), 3rd Infantry Division, noted after the first NTC decisive action rotation, "It quickly became apparent that our skill and methodology for accurately templating a near-peer conventional force had deteriorated."[3] Similarly, on the enabler side, when BG Jeffrey Broadwater served as the commander of 2nd ABCT, 1st Infantry Division, he identified a shortfall in effective dissemination of intelligence. He said, "The details, or in this case lack thereof, of how information moves from sensor to shooter became critical in the fast paced environment of offensive operations."[4]

The Army's intelligence community has been aware of these problems for years now, but progress toward solving them has come slowly, challenging the entrenched and hard-earned experience of Iraq and Afghanistan. The primary mission of military intelligence (MI) in the U.S. Army is to provide timely, relevant, accurate, and synchronized intelligence to tactical, operational, and strategic-level commanders. To accomplish this mission in a decisive action environment requires teams of intelligence Soldiers and leaders who are prepared to cope with a complex and fast-paced battlefield.

Challenges and Pitfalls

To understand the challenges and pitfalls of conducting effective intelligence during decisive action, it is important to first discuss the key roles of the intelligence warfighting function in this operating environment. For example, compared to COIN operations, military source operations and pattern/network analyses are far less critical during large-scale combat operations due to the highly kinetic, rapid operational tempo. Instead, intelligence leaders must shift their focus from these comfort zones toward more relevant conventional tasks of—

- Understanding and tracking enemy maneuver.
- Providing rapid and detailed terrain analysis and analysis of threats to maneuver elements.
- Processing frequently overwhelming and contradictory reporting from a confusing battlefield.
- Filtering the available information to answer the commander's priority intelligence requirements (PIRs).

These are essential responsibilities for Army intelligence professionals; these skills have suffered significant atrophy over the last decade of COIN and forward operating base-centric warfare.

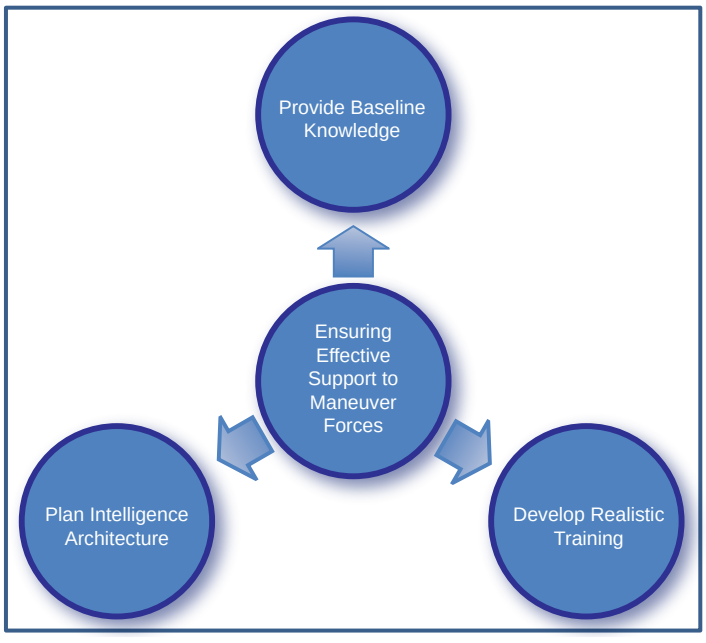
Several pitfalls now plague the intelligence elements within BCTs. Analysts, especially junior Soldiers, lack necessary knowledge to be effective in the more demanding operating environments Army forces face today. This may be due to an absence of seriously demanding home-station intelligence training prior to brigade-level collective exercises. Leaders are too comfortable with the COIN environment and exaggerate the focus on the consolidation area portion of the mission. We are creatures of habit, and the years spent combating improvised explosive devices and criminal networks have left their mark. Intelligence cells are limited in the amount and caliber of immersive, scenario-based training they are able to conduct because of the

difficulty in developing effective training scenarios. Simulated exercises are an effective solution but are prohibitively difficult to arrange at echelons lower than brigade. This leaves battalion S-2 sections, along with the brigade S-2, spending much of the training cycle focused on individual Soldier, classroom-based training or on garrison tasks with little relevance to the analytical mission.

Intelligence support teams, while technically proficient in employing their systems, lack the experience navigating their command and support relationships to effectively support and inform both their battalion and brigade-level customers. Similar to the S-2 sections, these assets spend much of the training cycle on individual training, and when integrated into maneuver training, their responsibilities to answer to the brigade are rarely exercised because scenarios focus on the lower echelons. This leaves both the collection asset and the supported battalion with the impression that they work only with each other, making the general support-reinforcing relationship difficult during larger collective exercises. This last pitfall can ultimately result in a breakdown of information flow between sensors and the brigade intelligence cell. BG Broadwater's observation about the importance of knowing "how information moves from sensor to shooter"[5] highlights the importance of training this relationship, which will surely be a focus at NTC while he is the commanding general.

Effective Support

With these problems in mind, the question is how do we as intelligence professionals ensure we are as prepared as possible to effectively support our maneuver forces during large-scale combat operations?



Provide Baseline Knowledge. First and foremost, we must ensure that every analyst has enough baseline knowledge to be effective in the stressful and fast-paced environment of large-scale combat operations. This includes basic analytical tasks; knowledge of enemy weapon systems, capabilities, and tactics; and ideally a working knowledge of the specific culture and worldview of potential adversaries. *The Applied Critical Thinking Handbook* (formerly the *Red Team Handbook*), version 7.0, as published by the University of Foreign Military and Cultural Studies, discusses "cognitive autopilot"[6] and how many staff members are "blind to the ability to see the world through the eyes of another national...group."[7] Decisive action critical thinking, especially for regionally aligned forces, demands a solid understanding of enemy thinking and motives. This requires significant study, discussion, and testing, for which we must make time around the many administrative demands placed on S-2 sections.

Develop Realistic Training. Next, we must develop and execute realistic and stressful training for our analysts, validating them in the same ways in which equivalent maneuver forces are tested. This means moving beyond classroom-based training and putting in the effort to develop robust intelligence scenarios. Looking beyond the S-2 sections, inclusion of the maneuver elements in training is essential. It is critical that maneuver leaders understand the capabilities of their intelligence enabler assets and understand how to employ them. The 1st Brigade, 4th Infantry Division, places significant emphasis on developing these supporting relationships, from enabler leadership professional development to ensuring enabler integration in every training event from platoon situational training exercises onward. The best way to ensure enabler integration will go smoothly is to practice it in a field environment, but junior intelligence leaders must ensure that an emphasis is placed on training their Soldiers during these events, rather than simply having them be present for maneuver training. Providing effective scripting and scenarios also demonstrates to the supported maneuver elements the kinds of situations in which these assets are effective; it also helps them develop tactics, techniques, and procedures (TTPs).

Plan the Intelligence Architecture. Finally, planning, briefing, and rehearsing of the intelligence architecture as early as possible in the training cycle are a necessity. This requires more than a tactical operations center exercise for validation. Reports from maneuver units and collection assets (who hopefully have a strong understanding of the PIR) are a key factor to this process. Perhaps most importantly, every element on the battlefield (not just intelligence assets) must clearly understand the PIR and what, how, and when

to report. Flexing these communications during training is the only way to ensure the leadership will have a clear picture of the battlefield.

Professionalizing Army Intelligence

Ultimately, tackling the challenges of decisive action is just part of a broader challenge of professionalizing Army intelligence. The *Oxford English Dictionary* describes a profession as "a paid occupation, especially one that involves prolonged training and a formal qualification."[8] Senior leaders in the MI Corps must ask whether we are truly holding our intelligence professionals to a rigorous standard of formal qualification. While the U.S. Army Intelligence Center of Excellence's development of the MI Training Strategy to certify the MI Corps is a promising start to the standardization of analytical training, the MI Corps needs to re-visit the certification of analysts, which should use standardized skillsets on a recurring basis. Just as cryptologic linguists (military occupational specialty [MOS] 35Ps) must attend annual language training to remain certified in their MOS and the MI systems maintainers/integrators (MOS 35Ts) must take technical exams to demonstrate to the Army that they are still able to do their jobs, there should be no exception for the rest of the intelligence disciplines.

A more formalized, rigorous program of home-station training and certification for intelligence sections is critical to being effective during large-scale combat operations. A program for training all-source intelligence analysts should have several objectives:

- All-source intelligence analysts (MOS 35Fs) and all-source intelligence officers (area of concentration 35Ds) need to complete a course in fundamentals of Army intelligence analysis. This course should feature orientation on intelligence tradecraft fundamentals, report writing, and research databases for intelligence preparation of the battle (IPB) product preparation under time-constrained conditions in complex operating environments.
- Production of the Annex B (Intelligence) and Annex L (Information Collection) to plans and orders within the military decision-making process must be addressed. A primary focus needs to be implementing "staff integrated IPB" in which the S-2 turns to other staff sections for their relevant expertise in assessing enemy maneuver, fires, sustainment, etc.
- Rehearsals must be dedicated to TTPs and best practices for maintaining the intelligence common operational picture within a tactical operations center. This gives junior analysts and young MI officers a taste of just how fast-paced large-scale combat operations are and how quickly the battalion or BCT commander needs assessments, which will influence their decision making.

Keeping up with the Pace of Large-Scale Combat Operations

If you have ever spent time in a battalion or brigade tactical command post, you know inundation of piecemeal (and often conflicting) reporting from subordinate maneuver elements is normal. The pace is marginally slower at the tactical operations center, but the scope of the information to process is larger. Making the previously mentioned adjustments to how we train our analysts and collectors will ensure we have an intelligence team that is comfortable with uncertainty and confident in its skillsets, which is critical to adapting to and keeping up with the pace of large-scale combat operations. Our intelligence professionals are responsible for ensuring we understand the enemy, both before an engagement and on the battlefield. Having the knowledge to keep up with the confusion of a fast-paced, kinetic decisive action fight will allow our maneuver leaders to better understand, and ultimately defeat, the enemy. Proficiency with digital systems, while critical, is only one piece of being an effective analyst.

Mississippi National Guard photo by SSG Shane Hamann, 102nd Public Affairs Detachment

SPC Clayton P. McInnis, a human intelligence collector with 1st Battalion, 155th Infantry Regiment of the Mississippi Army National Guard, reviews reports in the unit's tactical operations center, at the National Training Center, Fort Irwin, CA.

More importantly, analysts who can recognize enemy formations and schemes of maneuver based on patchwork reporting enable their unit to see through the fog of war and determine the enemy's course of action. Similarly, while technical and tactical proficiency is vital for an intelligence collector, regardless of specific discipline, being able to provide clear, concise reporting to both the immediate maneuver leader and the intelligence cells at higher echelons ensures the relevant information makes it from the sensor to the shooter. It also ensures the commander has the best possible picture of the enemy. Successful intelligence in large-scale combat operations demands that we train our core competencies and intelligence architecture in a time-constrained environment.

Endnotes

1. David Crozier, "Decisive Action: How to Fight and Sustain in the Army's Futures Battles," *NCO Journal* (28 May 2013), http://ncojournal.dodlive.mil/2013/05/28/decisive-action-how-to-fight-and-sustain-in-the-armys-future-battles/.

2. Ibid.

3. National Training Center, *Training for Decisive Action: Stories of Mission Command, Collected Insights from Commanders and Leaders on their Experience at the National Training Center* (Fort Leavenworth, KS: Combat Studies Institute Press, U.S. Army Combined Arms Center, 2014), 55, http://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/TrainingForDecisiveAction.pdf.

4. Ibid, 8.

5. Ibid.

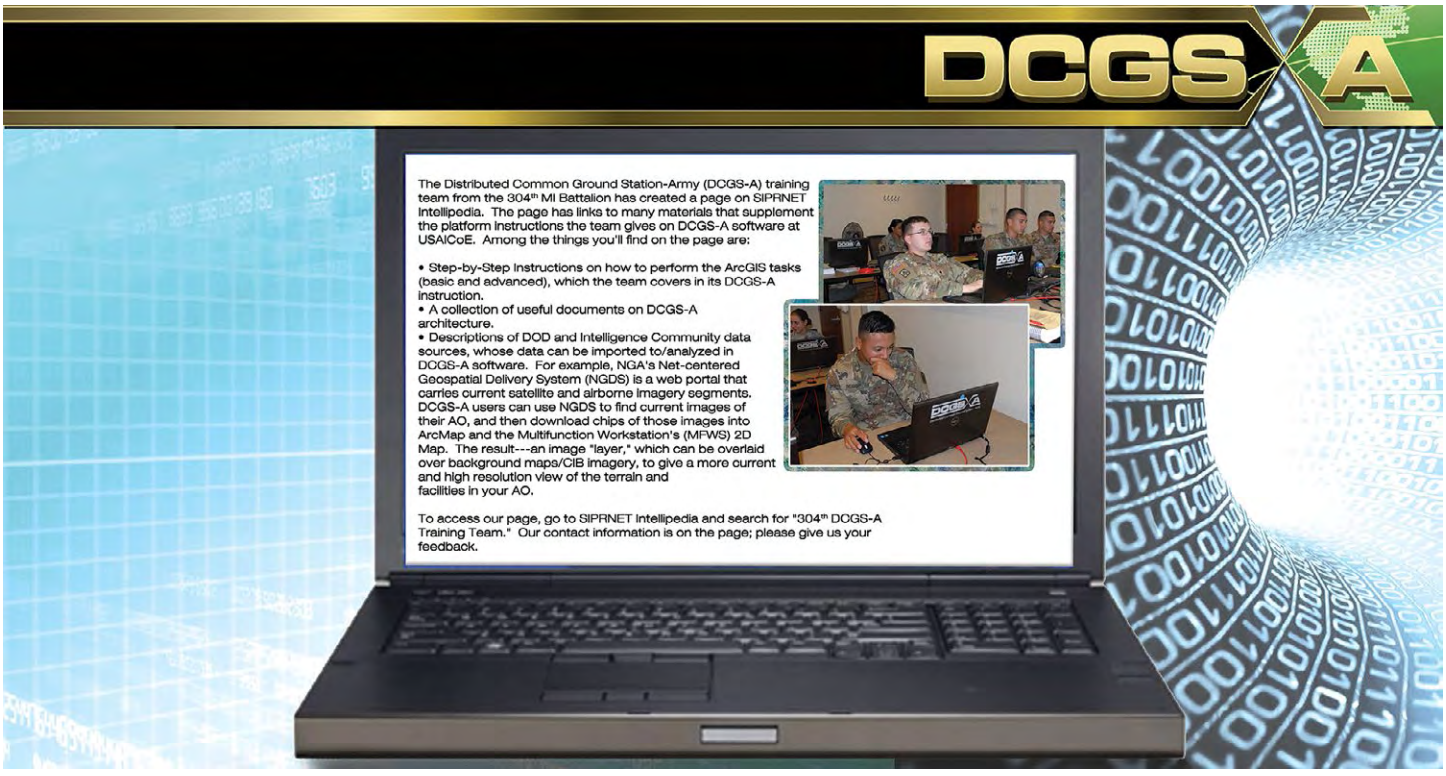
6. University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook* (formerly the *Red Team Handbook*), version 7.0, January 2015, 47-48, https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Applied_Critical_Thinking_Handbook_v7.0.pdf.

7. Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 4, quoted in University of Foreign Military and Cultural Studies, *The Applied Critical Thinking Handbook*), 24.

8. *Oxford English Dictionary*, s.v. "profession," accessed 28 February 2018, https://en.oxforddictionaries.com/definition/profession.

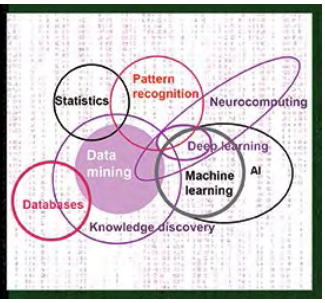
CPT Alex Morrow is currently the S-2 Collection Manager, 1st Brigade Combat Team, 10th Mountain Division at Fort Drum, NY. His previous assignments placed him in a maneuver battalion S-2 section and the Military Intelligence (MI) Company of the 1st Stryker Brigade Combat Team, 4th Infantry Division. CPT Morrow is a graduate of the MI Captains Career Course.

CPT Michael Dompierre is currently the S-2 for the 5th Battalion, 5th Air Defense Artillery Regiment at Fort Sill, OK. In his previous assignments, he spent time as a junior leader in maneuver battalion S-2 sections and the MI Company of the 1st Stryker Brigade Combat Team, 4th Infantry Division. CPT Dompierre is a graduate of the MI Captains Career Course.



Data Analytics to Win in a Complex World

by Chief Warrant Officer 3 Garrett Hopp, Chief Warrant Officer 3 Glenn Gleason, Chief Warrant Officer 3 Nick Rife, and Chief Warrant Officer 2 Ashley Muller



Introduction

U.S. Army intelligence analysts currently dedicate the majority of their time and resources to data management rather than to intelligence analysis. As conflicts have become more complex and the amount of intelligence data has increased, the Army needs to keep pace with these changes. There is an equal, if not greater, need to automate the common intelligence picture contribution for collection, targeting, and decision making. In a future conflict, advanced technology will create an evolving battlefield with engagements conducted simultaneously across multiple domains. To achieve a tempo and depth in this type of fight, it is necessary to maximize operations and intelligence data integration. This will drive predictive insight. The pace of battle requires straightforward processes and simple-to-use technologies that enable a shared understanding of the environment for operations, intelligence, and decision makers. Army systems use cumbersome data processes with outdated technological solutions that decrease the value of data for the consumer. Ultimately, this limits the Army's capabilities and reduces the effectiveness of joint and combined operations. This article explores the role of embedded analytics in future conflicts. It also proposes concepts for a combined computing operating environment that is modular, flexible, and adaptable.

Intelligence Support to Situational Understanding

With smaller command posts, the Army can no longer rely on droves of intelligence Soldiers analyzing volumes of reports. Several factors currently serve to lengthen the timeline for decision making: disparate nodes, low bandwidth, poorly designed communications frameworks, and a broad misunderstanding of how to interact with data at each echelon. The battlefield of the future must operate on one common data tier for all warfighting functions. Embedded analytics software must then enhance this data tier to support algorithmic-driven decisions. Correlation, normalization, and association of enemy data should occur on the same interface as friendly data in order to optimize decision superiority. Land component intelligence analysts should use embedded analytics to quickly and accurately assess the adversary's multi-domain deception operation, instantly share it with other services in a common intelligence picture, and allow the joint force commander to exercise decision superiority.

In a commercial sense, "companies realize that making analytics programmatic by automating operational decisions can be beneficial to both the top and bottom line."[1] Bringing analytics software to the forward tactical edge could mitigate poor decisions and increase favored outcomes in engagements with limited reliance on external proficiencies, systems, and processes. Embedded analytics will—

- Evaluate all information against enemy courses of action, decision points, force ratios, and terrain effects.
- Make recommendations to the analyst on changes to courses of action, emerging warning concerns, and named areas of interest.
- Make recommendations for reports to read, data to query, and associations to validate based on what the analyst is seeking across the multi-domain extended battlefield.

In the future, these analytics are essentially a channel to effective intelligence support to decision making. Recently, this concept was applied in a theater exercise encompassing threats across all domains. Embedded analytics in a land component intelligence cell instantly correlated new data detailing the disposition of the adversary's army special forces in a named area of interest, enabling land component intelligence analysts to compare it against the adversary's operations in the air, sea, space, and cyberspace domains.

Intelligence Support to Information Collection

In future zones of conflict, sensors will saturate the operational environment in all domains: air, land, sea, space, and cyberspace. To achieve and exploit positions of relative advantage, exploitation of sensor data must be efficient and disseminated rapidly. The exploitation process is tedious and often results in missed information and dated analysis. Like maneuver, command post computing must maintain speed and agility, and the supporting sensor analytics must be autonomous. Analytic software embedded in the computing environment will decrease the amount of labor

required for tasking, collecting, processing, exploiting, and disseminating. This increases efficiency and significantly reduces the need for human data processing. Analysts will be able to tip and cue at the click of a mouse because they interact with the information collection environment in near real time. Embedded analytics will provide intelligence, surveillance, and reconnaissance (ISR) platform recommendations based on factors such as permissive flight paths, weather variations, and projected collection yields, thereby increasing the speed and efficiency of collection.

In a research report titled *Operationalizing and Embedding Analytics for Action*, Fern Halper, Ph.D., characterizes this as "small tactical decisions that can be made repeatedly and can add up to high revenue."[2] When applied to collection, the term "small tactical decisions" translates to multiple autonomous sensor cues, while the "high revenue" could be an understanding of local enemy capability. Units will employ embedded analytics to exploit the surveilled environment and automatically synthesize the results into structured database objects. These objects create a usable data set for analysts and decision makers alike. Leveraging embedded analytics for ISR will conserve thousands of Soldier-hours and provide concise collection and timely results for support to targeting and decision making.

Intelligence Support to Targeting

Current systems use more human effort than machine in their support to targeting. At the tactical and operational levels, targeting practices often devolve into manual exchanges of sticky notes or chat programs like mIRC, TransVerse, and Psi. Both methods are inefficient and prone to significant human error. Using these methods in multi-domain operations would be disastrous, leading to desynched operations and a joint force unable to create simultaneous effects in multiple domains. Embedded software analytics in support of targeting will shorten the sensor-to-shooter link and will enhance the effects in an environment using a series of cues and triggers. Targeting cells will define target selection standards and set rules for automated fire mission nominations based on the unit's authorities and standards. Intelligence handover lines and fire control measures tailor information according to echelon and mission requirements. Anticipated and unanticipated target notifications appear on the same collaborative interface to the targeting and intelligence officers.

This concept was recently applied in a theater exercise encompassing threats across all domains. Embedded analytics in a land component intelligence cell instantly correlated new data concerning Marine elements aboard a naval vessel en route to a target area of interest, triggering an alert that sent the data to the joint force targeting cell. Joint force targeteers dynamically delivered multi-domain effects to the target, which neutralized the target before it reached its destination. Embedded analytics will analyze which targets were serviced, what allowed them to be serviced, and what ISR assets were involved in the kill chain.

As battle damage assessments and mission fire reports are updated, predictive analytics will correlate all gathered ISR and targeting information. The analytical software will then provide estimates on the enemy's remaining combat effectiveness, regeneration time, and confirmation on the effectiveness of target areas of interest. Expanding to all domains, embedded analytics allows all services to see, coordinate, and collaborate, regardless of the hardware used by different services. The continual analysis and re-analysis of data from all domains will enhance the speed and lethality of coordinated multi-domain fires.

Photo Credit: U.S. Air Force

The Intelligence, Surveillance, and Reconnaissance Division at the Combined Air Operations Center at al Udeid Air Base, Qatar, provides a common threat and targeting picture that is key to planning and executing theaterwide aerospace operations.

Conclusion

Economist John Maynard Keynes once wrote, "The difficulty lies, not in the new ideas, but in escaping from the old ones."[3] Still relevant today, his words could not translate more accurately to the challenges

the Army must address as it seeks a transformative shift for future conflicts. Operationalizing embedded data analytics will redefine the depth and tempo in combined arms maneuver for multi-domain conflicts of the future.

Endnotes

1. Fern Halper, *Operationalizing and Embedding Analytics for Action* (Chatsworth, CA: TDWI, 2015), 4, https://www.sas.com/content/dam/SAS/en_us/doc/whitepaper2/tdwi-operationalizing-embedding-analytics-for-action-108112.pdf.

2. Ibid., 6.

3. John Maynard Keynes, *The General Theory of Employment, Interest and Money* (London: Macmillan and Co, Limited, 1936), preface, https://cas2.umkc.edu/economics/people/facultypages/kregel/courses/econ645/winter2011/generaltheory.pdf.

CW3 Garrett Hopp serves as the Iraq team chief for the Combined Joint Task Force–Operation Inherent Resolve (CJTF-OIR) CJ2. He was instrumental in employing analytics with III Corps during two warfighter exercise events. He was also a principal curriculum writer for the Digital Intelligence Systems Master Gunner Course.

CW3 Glenn Gleason serves as the U.S. Army Intelligence and Security Command Foundry All Source Training and Integration Center officer in charge (OIC) and the Digital Intelligence Systems Master Gunner Course OIC at Fort Bragg, NC. He is responsible for producing all-source/Distributed Common Ground System-Army training in support of Foundry 3.0, and oversees the content, delivery, and administration of the Digital Intelligence Systems Master Gunner Course.

CW3 Nick Rife serves as the senior All-Source Intelligence Technician for 2nd Security Forces Assistance Regiment, Fort Bragg, NC. He has previously managed the Digital Intelligence Systems Master Gunner Course where he benefited from curriculum implementation that examines commercial technology strategies analogous to military operations. CW3 Rife intends to implement like strategies within his own organization and work to proliferate positive lessons learned to the Digital Intelligence Systems Master Gunner community of interest.

CW2 Ashley Muller serves as the Senior All-Source Intelligence Technician for Asymmetric Warfare Group. She previously assisted in addressing theater architecture shortfalls within the CJTF-OIR footprint as well as employing analytics in past warfighter exercise events with III Corps. CW2 Muller is a Digital Intelligence Systems Master Gunner Course 17-02 graduate and contributed greatly to augmenting the courseware.

The Intelligence Warfighting Function: Rethinking Force Generation

by Chief Warrant Officer 3 William J. Fann

Introduction

Is the U.S. Army's human-centric approach to operations an inhibiting factor in today's information technology driven world? Although *Shaping the Army Network: 2025-2040* states that the "Army of 2025 and beyond will largely be located within the continental United States (CONUS), with a smaller deployed footprint" and that the "military must also determine how to harness the power of emerging technologies, such as supercomputing and data analytics," tactical units have taken few strides to bridge the gap between data and knowledge.[1] Special emphasis is being placed on command post transitions and distributed mission command at combat training centers primarily based on Chief of Staff of the Army GEN Mark Milley's supposition that during future conflicts, "If you stay in one place for longer than two or three hours, you will be dead" and the force is "on the cusp of fundamental change" as it relates to being required to adapt based on competitor's capabilities.[2]

During command post transitions, commanders and staffs tend to think and prioritize in terms of personnel, systems or sensors/platforms, information, and data, sequentially in that order, inferring "people" are the most essential portion of mission command. Although one would be hard-pressed to dispute people are not the essential element of mission command, thinking "people-first" neglects the importance of data and information where knowledge is derived to support decision making. This article does not dispute the importance of people in mission command, but rather it proposes leaders should enable people (staffs) to plan a digital architecture by clearly identifying requirements when conceptually planning distributed mission command. Taking on a data-first approach, particularly during force generation, facilitates detailed planning and will help to ensure mission command nodes are adequately resourced and manned to support decision making in distributed mission command settings.

Conventional Thinking

Commanders and staffs usually think about personnel and systems during planning with limited consideration of the information and data needed to support decision making. This applies specifically during force generation planning at tactical echelons. This human-centric train of thought may derive from an overall shared understanding in the military that a staff's effort leads directly to warfighter success on the ground. ADRP 6-0, *Mission Command*, even states a "commander's mission command system begins with people. Commanders base their mission command system on human characteristics more than on equipment and procedures"[3] While it is difficult to contradict the importance of "people" in mission command, the conventional idea of focusing on people first during force generation of staff sections neglects the importance of getting information and knowledge down to subordinate staffs and the warfighter. The following vignette relays a common scenario observed at the Joint Readiness Training Center, which highlights the impact of human-first thinking, specifically for the intelligence warfighting function, during staff force generation.

During a 2017 training rotation at the Joint Readiness Training Center, a brigade combat team (BCT) deployed a tactical command post (CP) from the main CP to support mission command forward and provide a continuity in operations during command post transition. The BCT S-2 wanted to keep a light footprint forward to support decision making at the main CP, leaving the majority of intelligence personnel in the brigade intelligence support element (BISE) so that they could provide intelligence reach support. The tactical CP included the BCT S-2, intelligence planner, collection manager, and two all-source analysts. Equipment included one Portable-Multi-function Workstation (P–MFWS), a component of the Distributed Common Ground System-Army, to stay in the tactical CP and one P–MFWS to accompany the BCT S-2 in the mobile CP. Equipment undedicated to the S-2 but integral to the S-2's primary, alternate, contingency, and emergency plan included the Joint Capabilities Release kit and BCT commander's Point of Presence.[4] The tactical CP S-2's communication with battalions and main CP was limited by the BCT's sporadic and slow access to their SECRET Internet Protocol Router Network. The tactical CP depended heavily on digital systems for its enemy common operational picture, order of battle, information collection matrix, and significant activity tracker, but it only maintained limited analog trackers and overlays of the same products. The tactical CP and main CP were simultaneously functional for approximately 48 hours. The main CP

provided support to the tactical CP by continuing to produce their system status updates and intelligence summaries. The tactical CP provided the BCT commander and S-2 with the current enemy situation, conducted mission analysis for offensive operations within the area of operation, updated the BCT priority intelligence requirements, and tracked the BCT collection assets. It took over 93 hours for the main CP to fully assume the mission from the tactical CP after they displaced from their intermediate staging base to a new location in the BCT's area of responsibility. This extensive amount of time was due in part to insufficient drivers' equipment and certifications within the unit's movement plan as well as poor command, control, tracking, and security of their serials during ground movement.

Unpacking the Vignette

Issues with logical requirements that include actual production inputs/outputs (e.g., intelligence summaries, synchronization matrices, and estimates) and technical requirements (e.g., account access, communications security considerations, and bandwidth/latency considerations) severely limited the rotational BCT's intelligence warfighting function. The P–MFWS in the tactical CP was configured to connect to the BISE's TROJAN network at the main CP, not the BCT commander's Point of Presence. No one at the tactical CP had administrative rights to reconfigure the P–MFWS, thereby rendering it useless for the 93 hours during which the tactical CP controlled the fight. The BCT maintained its common operational picture on the battle captain's Command Post of the Future. The S-2 did not have a dedicated system to update the enemy common operational picture and had to share the battle captain's Command Post of the Future to maintain a distributable product. The S-2 did not bring a mission data loader to the tactical CP. The loader provides the capability of moving digital products between upper tactical internet systems and the Joint Capabilities Release for ease of dissemination to subordinate units. The BCT commander and S-2 did not identify roles and responsibilities at each node before the tactical CP deployment forward. Probably the most important logical requirement neglected was the information collection plan. The collection manager at the tactical CP was responsible for ensuring the information collection plan was projected out 72 hours. To do this, the collection manager needed access to the division portal; however, without a dedicated system, the information collection plan fell behind in production and in support to the BCT. The BCT and its subordinate elements' movement into the area of operations was uninformed by echelons above brigade collection assets. Figure 1 is a visual representation of the BCT's intelligence system capabilities in time and space.

Rethinking Force Generation

The vignette represents a common theme observed at the Joint Readiness Training Center by rotational units exercising mission command across distributed nodes. When units think about people before data and information requirements during force generation, they forgo the necessary detailed planning. Thinking "data-first" allows for more thought on technical and logical requirements and how to adequately resource mission command nodes. For example, a BCT collection manager at a remote mission command node needs to have the capability to gather collection requests from subordinate elements primarily on a lower tactical internet system. The collection manager will need to communicate with the military intelligence company (the BISE via the P–MFWS) for the updated digital enemy common operational picture and organic collection teams (unmanned aerial systems platoon, human intelligence collection teams, signals intelligence collection teams, and cryptologic support team). The collection manager will also need to communicate with the division G-2 collection manager, usually via upper tactical internet systems, to access

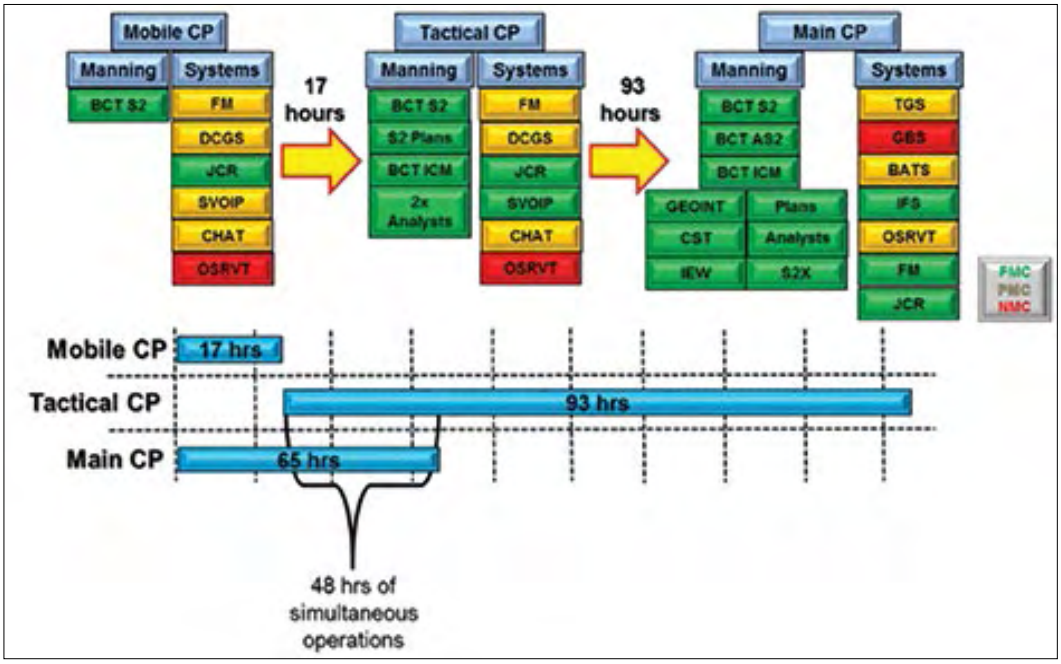


Figure 1. BCT's Command Post Transition

the division portal to submit echelons above brigade collection requests. A dedicated P–MFWS, configured for the appropriate network to allow access to the BCT upper tactical internet network and access to the BISE's Intelligence Fusion Server data (e.g., Tactical Entity Database), gives the collection manager the ability to develop, update, and disseminate named areas of interest as a part of the information collection plan.

Granted, this is not a detailed or all-inclusive list of requirements, but it shows the level of complexity for just one cell (collection management) in a distributed mission command setting. Thinking about data and information requirements before systems and personnel enables commanders and staffs to develop more detailed, well thought-out running estimates during mission analysis. Necessary details include how data and information will get from sensors to warfighters, from sensors to analysts, and from analysts to warfighters. It also encompasses how information and analytical products are passed to higher and lower echelons in accordance with the primary, alternate, contingency, and emergency plan. Thinking about systems to process the data and information before personnel helps commanders and staffs to identify not only the potential resources needed but also the right people and training to operate the systems. This detailed way of thinking requires staff sections to communicate with other warfighting functions, across higher and lower echelons. Staffs and subject matter experts are also forced to contemplate logical requirements and technical requirements before receipt of mission. Figure 2 helps to illustrate a data-first approach.

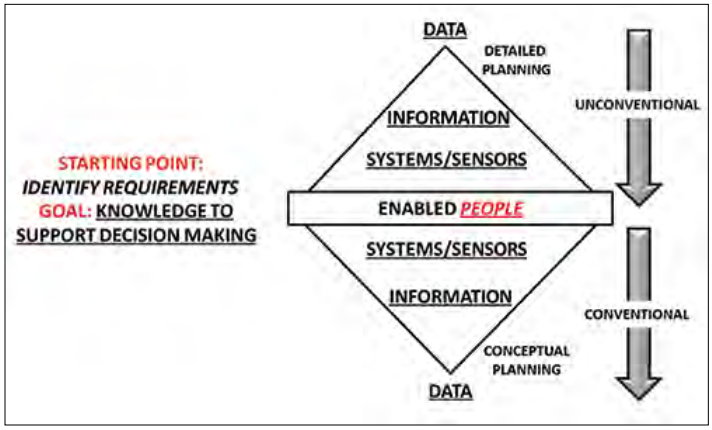


Figure 2. Data-First Approach

Final Thoughts

While this article focuses on the impacts to the intelligence warfighting function as an example, other warfighting functions may benefit from looking at how they approach force generation planning at the tactical level. The Army's human-centric thinking drives us to think about people first during force generation, which mission command doctrine supports. Thinking data-first during force generation will allow for more detailed planning earlier to support developing and maintaining staff running estimates. This is particularly true for intelligence and mission command and will help to ensure mission command nodes are adequately resourced to support decision making in distributed mission command settings. As the Army continues to focus on having a lighter footprint forward and distributed mission command with more intuitive, scalable, and adaptable systems to support the warfighter, digital architectural issues will have a lessened impact on operations. However, until those innovative systems become a reality, commanders and staffs should think of efficient and effective ways to improve support to decision making.

Endnotes

1. U.S. Army, Office of the Chief Information Officer/G-6, *Shaping the Army Network: 2025-2040* (Washington, DC, March 2016), 3, https://www.army.mil/e2/c/downloads/429258.pdf.

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

3. Department of the Army, Army Doctrine Reference Publication 6-0, *Mission Command* (Washington, DC: U.S. Government Publishing Office [GPO], 17 May 2012), 1-5. Change 1 was published on 10 September 2012. Change 2 was published on 28 March 2014.

4. A commander's Point of Presence "hosts mission command applications and services to facilitate situational understanding and enable mission command on-the-move. Commanders can use the Point of Presence to monitor activities in their operational area via Command Post of the Future or chat applications while traveling or during command post displacement." Army Techniques Publication 6-02.60, *Techniques for Warfighter Information Network – Tactical* (Washington, DC: U.S. GPO, 3 February 2016), 2-11.

CW3 William J. Fann is the all-source intelligence technician (350F) observer, coach, trainer and digital intelligence systems master gunner at the Joint Readiness Training Center. He holds a master's degree in strategic security studies from the National Defense University, College of International Security Affairs.

Human Intelligence and Counterintelligence in the Brigade Combat Team

by Chief Warrant Officer 3 Adam Hanson, First Sergeant Gary Vilano, and Sergeant First Class Brendon Wiese

A brigade combat team (BCT) is the Army's primary combined arms, close-combat force and is the principal ground maneuver unit of divisions. Its flexibility allows it to function across the range of military operations. The infantry BCT, Stryker BCT, and armored BCTs have human intelligence (HUMINT) capabilities that are organic and counterintelligence (CI) capabilities that may be downward reinforced to their formations. The BCT's HUMINT and augmented CI capabilities are an important part of the BCT S-2's information collection activities that support offensive, defensive, and stability operations. Providing the proper support requires constant oversight, taxing the BCT S-2 and staff. To manage these capabilities, the BCT S-2 has a HUMINT officer to fill the role of the S-2X working in conjunction with the military intelligence (MI) company commander. The HUMINT and CI structure may vary across the BCTs but usually consists of an S-2X, an operational management team, HUMINT collection teams, and a small CI footprint.

Organic and Supporting Collection Capabilities

The ideal HUMINT and CI structure for the BCT consists of the following:

- HUMINT operations cell.
- Operations support cell.
- CI coordinating authority.
- HUMINT analysis cell.
- CI analysis cell.
- Supporting HUMINT collection teams and CI teams.

However, not all elements of this robust structure are present within the BCT. The commander's requirements and priorities can drive CI and additional HUMINT augmentation from the expeditionary-MI brigade. At a minimum, the following elements should be a part of a BCT HUMINT and CI structure:

S-2X. The S-2X serves as the primary HUMINT and CI advisor to the BCT commander and S-2. The S-2X provides mission focus, technical support, technical control, and oversight to all the BCT's HUMINT and CI activities, ensuring they are in compliance with the business rules of the defense HUMINT executor and CI enterprise policies and regulations. They work closely with the BCT S-2, MI company commander, and subordinate S-2s to enable operations. The S-2X should have a HUMINT operations cell and a CI coordinating authority capability supplementing the S-2X's efforts in oversight and operational support.

Operational Management Team. The operational management team manages and maintains the HUMINT collection team's activities. It is also responsible for the repository of the brigade's HUMINT-centric databases, manages HUMINT collection requirements, sets quality and control measures for publishing reports, and provides feedback and guidance to its HUMINT collection teams. The operational management team cross-cues and disseminates information to other operational management teams' and HUMINT collection teams' collection entities throughout the BCT's operational footprint. It is important to have experienced HUMINT personnel at this level to provide the best possible oversight. The operational management team chief works closely with supported battalion S-2s to assist the HUMINT collection teams in answering collection tasks and maintaining situational awareness.

Human Intelligence Collection Teams. HUMINT collection teams vary in size and mission and provide support to the battalions and companies. Depending upon the skillsets required for the mission, HUMINT collection activities include interrogation, debriefings, and military source operations.

Counterintelligence. A small CI footprint in the BCT can be leveraged to support limited CI activities. If additional support is obtained from the expeditionary-MI brigade, the support is robust, and no CI coordinating authority currently exists at the BCT, then the S-2X may consider standing up a CI coordinating authority and a CI analysis cell to oversee and provide analytical support to the CI teams. This CI capability may be limited to supporting Threat Awareness and Reporting Program activities and force protection and conducting military CI collection.

Successful Operations Start in Garrison

The BCTs have many weapon systems in their arsenals that require soldier familiarization and gunnery. Like these weapon systems, HUMINT and CI skills must be exercised through continuous onsite and offsite intelligence training. The MI company commander must identify at what level to employ their teams depending on requirements of the S-2 and METT-TC (mission, enemy, terrain and weather, troops and support available–time available and civil considerations). The MI company commander is responsible for training HUMINT and CI personnel, while the S-2X

integrates this capability throughout the BCT. They should both be aware of training opportunities for their Soldiers that are available through the intelligence community and Active Duty, National Guard, and Army Reserve MI units. As the BCT continues to train, the MI company commander and S-2X should pay close attention to courses that improve their unit's mission capabilities.

Recommendations, Lessons Learned, and Best Practices

Listed below are recommendations, lessons learned, and best practices. They are in no way the be-all and end-all of how to best support the BCT's mission; however, within the BCT, they will increase the effectiveness of an S-2X, an S-2X staff, a HUMINT collector, and/or a CI special agent.

The S-2X works for the BCT S-2. The BCT S-2 is the primary intelligence conduit to the BCT commander. The S-2X manages an intelligence discipline that is a prime contributor to the all-source intelligence picture. The S-2X must ensure the BCT S-2 is aware of significant HUMINT and CI activities affecting operations and the safety and welfare of personnel. Before briefing the BCT commander and command sergeant major on sensitive investigations and operations, the S-2X should provide the BCT S-2 with the necessary information and obtain their advocacy to ensure the BCT commander makes informed decisions.

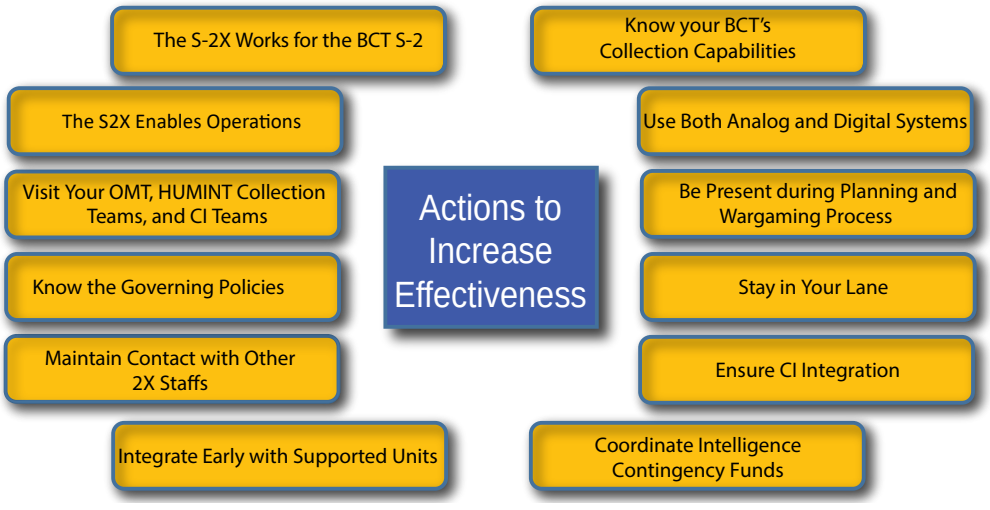
The S-2X enables operations. The S-2X has many competing requirements that are often difficult to balance. It is common for S-2Xs to address commanders' directives and staff requirements and to provide operational oversight responsibilities all at once. Regardless of those requirements, their primary focus is to provide the purpose and key tasks of the operation and to achieve the desired end state. Warrant officers and noncommissioned officers (NCOs) can assist in this process; however, the S-2X has oversight of all the BCT's HUMINT and CI operations and supports them as needed. The S-2X's mission effectiveness is based on their presence within the staff and how they interact with the BCT's decision makers. The S-2X must understand the operational environment and elements making up the force to accomplish the mission from the BCT to the combatant commander. The S-2X must understand the HUMINT collection requirements for their area of operations and implement the HUMINT portion of the collection plan to maximize the BCT's mission success.

Visit your operational management team, HUMINT collection teams, and CI teams. The S-2X staff should take every opportunity to personally visit their operational management team, HUMINT collection teams, and CI teams. Additionally, leaders further validate the use of their collection elements through observation and reinforcing guidelines and policies, ensuring their collectors and special agents are properly executing operations. In some cases, face-to-face visits may not be feasible, so radio, phone, or video teleconference must be the mode of contact. The S-2X should avoid solely relying on email and chat programs to assess their subordinate's missions, health, and welfare.

Know and understand the policies governing your activities. Policies, regulations, and orders enable your operations. These documents provide guidance that supports current and future operations; identify these areas early enough in the planning process to enable operations. If the S-2X and supporting staff fail to plan accordingly, their contribution to the BCTs' mission will be severely degraded.

Maintain close contact with higher, adjacent, and subordinate 2Xs and their staffs. Regardless if one is in garrison or a deployed environment, the S-2X staff needs to engage their higher, adjacent, and subordinate 2Xs through video teleconferences or personal visits. Division and higher 2X staffs are more knowledgeable and experienced in HUMINT and CI activities and can provide excellent on-the-job training and guidance to ensure continuity between deployments for redeployed personnel. Sister BCTs can assist in developing and identifying best practices. This interaction provides a better understanding of how the 2X leadership and staff operate, and one may discover additional capabilities that the BCT can use.

Integrate early with supported units. Ensure HUMINT and CI personnel support units during their training exercises—from battalion field training to combat training center



rotations. The teams should first educate supported unit staffs about how HUMINT and CI capabilities can support and satisfy their intelligence requirements. This will enable the supported units to work out personnel, equipment, and support issues before deployment. The trust built over a series of exercises will go a long way in a deployed environment.

Know your BCT's intelligence collection capabilities and requirements. Not all BCTs are created equal. HUMINT and CI personnel must understand their BCT's collection requirements, force structure, equipment, and intelligence collection capabilities in order to enhance the effectiveness of their operations.

Use analog and digital systems. Ensure HUMINT and CI personnel use authorized hardware and software to disseminate information. Prior to train-up for deployment, identify hardware, software, and defense HUMINT and CI enterprise databases used in theater to reduce the learning curve associated with the train-up on these programs. Be prepared to go analog in order to support complex operations that are fluid and where connectivity is intermittent.

HUMINT and CI leadership needs to be present during the planning and wargaming process. Presence at wargaming and planning events will establish familiarity and trust with your BCT staff officers and NCOs. The initial introduction to the BCT S-3 should not be at the combat training center rotation.

Stay in your lane. CI personnel should not be running HUMINT operations, nor should HUMINT personnel run CI operations; however, they can mutually support one another. The Army has dedicated a significant amount of personnel, time, and funding to train HUMINT and CI officers, warrant officers, and enlisted Soldiers, and they should exercise those skills. The S-2X and MI company commander must understand those specific capabilities that could be lost if not assigned accordingly.

Ensure counterintelligence integration. CI should have representation in the 2X staff. The CI officer, warrant officer, or NCO should be familiar with key leaders and the BCT's battle rhythm. Many times, CI opportunities arise out of liaison with key leaders, intelligence briefings, and S-3 operations.

Coordinate intelligence contingency funds. HUMINT and CI leadership should conduct the required coordination for intelligence contingency funds as early as pre-deployment and during the planning and wargaming process. Custodians must obtain intelligence contingency funds and learn the limitations and incentives of their use because they will be the subject matter experts. All HUMINT collectors and CI personnel, including leadership, should share the same understanding of the legal and proper use of these funds. AR 381-141, *Intelligence Contingence Funds,* governs the use of intelligence contingency funds.

Final Words

The BCT's HUMINT and CI capabilities are an integral part of the BCT's mission. HUMINT and CI reporting is often the driving force behind brigade, battalion, company, and platoon operations. To be a part of that driving force, the S-2X and its personnel must take the time to understand the policies, systems, and capabilities that enable it. It is our hope that this overview, these recommendations, lessons learned, and best practices, together with one's unique skills and leadership style, provide baseline areas of emphasis for successfully leading, managing, and enabling HUMINT and CI capabilities in your BCT.

CW3 Adam Hanson currently serves as the deputy C-2X for 2nd Infantry Division–Republic of Korea and U.S. Combined Division. He has over 25 years of experience in counterintelligence (CI) and human intelligence (HUMINT). He has served in a variety of 2X-related assignments ranging from a combatant command J2-X operations officer to a HUMINT collector in an infantry brigade. He has spent numerous years training Active Duty, National Guard, Army Reserve, sister-service, and civilian intelligence professionals as a National Intelligence University-Southeast Campus adjunct faculty member, senior instructor/writer, Active Component/Reserve Component trainer, and Advanced Individual Training (AIT) drill sergeant. He holds a master of business administration in global management from the University of Phoenix, Arizona, and a bachelor of arts in political science from Ottawa University, Kansas.

1SG Gary Vilano currently serves as the First Sergeant of Charlie Company 309th Military Intelligence Battalion. He has served in a variety of 2X and special staff functions within the HUMINT and special operations community. These functions include HUMINT team leader, operational management team (S-2X) noncommissioned officer (NCO) in charge (NCOIC), HUMINT operations cell chief (J2X), Combined Special Operations Task Force–Afghanistan, chief HUMINT NCO for 4th Battalion/3rd Special Forces Group (A), and HUMINT J3X/ J35 planner. He has dedicated a number of years developing the next generation of warfighters and intelligence professionals as a New Systems Training and Integration Division NCOIC, senior NCO Academy instructor, and a senior instructor/writer at the HUMINT Collector AIT Course.

SFC Brendon Wiese currently serves as the situational training exercise committee NCOIC for the 309th Military Intelligence Battalion and has over 17 years of HUMINT, CI, and infantry experience. Throughout his career, he has been an intelligence provider and end-user, serving as a forward-deployed brigade S-2 NCOIC, brigade combat team HUMINT and CI platoon sergeant, operational management team NCOIC, and sniper team leader. He has also trained HUMINT collectors as a senior instructor/writer.

Developing Analytical Capabilities in Changing Environments

by Captain Christie P. Cunningham

In the past century, the nature of warfare has seen several changes. Relative isolation in World War I shifted to full-society involvement in World War II. Cold War offset strategies gave way to a unipolar system of American superiority. American innovation led to the creation of the internet and integrated technologies—a boon for the military and now a central part of life for ordinary citizens. However, the dispersion of technology is increasing the significance of peer and near-peer competitors and non-state actors on the international stage. Incidents in the media—Islamic State in Iraq and Syria global activities, Chinese intellectual property theft, Russian information campaigns, criminal activity, and North Korean actions—highlight formerly impossible technology-enabled concerns and an increasing conventional and hybrid threat. In light of these challenges, we must review our analytic capabilities and methods and evolve our force to contend with the speed of change.

The Analyst's Weapon System

As intelligence professionals, we are charged with understanding the environment and its effects. Analysts at all echelons—from the newest analyst serving in a battalion S-2 section to a strategic intelligence officer—are critical in helping leaders understand the environment and make decisions. Starting at the institutional level, analysts learn the basics of defining the environment, describing environmental effects on friendly and adversary forces, and forecasting adversary behavior. Analysts truly "cut their analytical teeth" later when they work on real-world intelligence problems and are entrenched in the environment they are analyzing. When we seek to improve analytical effectiveness, we must consider the analysts' holistic "weapon system." Some argue that analysts merely need more "on keyboard" training. In truth, an analyst's weapon system is more nuanced, comprised of physical and cognitive components:

- Equipment: analytical hardware, software, and tool proficiency.
- Knowledge: environmental "immersion," critical thinking, and a constant pursuit of understanding.

These components integrate with one another and are jointly affected by changes in the environment.

Evolving Environments: The Driver for Training and Capability Refinement

The way we adapted to this evolution within environments shaped analysts' capabilities. From World War II through the Cold War, resource-intensive, lengthy development processes and analytical efforts matched powerful nation-state threats. After the Cold War and absent an international balance-of-power, adversaries became harder to define. State actors were still a threat, but non-state actors rose in significance. Analysts had to pivot to understand the human element of the environment because newer adversaries had varied histories, goals, and no obvious doctrines.

Many individuals refined their analytical capabilities on the job. Some read older texts on terrorism and guerrilla warfare, and others attended rapidly developed courses. Younger analysts benefitted from adapted capstone exercises and doctrine. Special operations communities framed the human aspect of the environment as a domain and made it a key part of their analysis and operations.[1] The Department of Defense (DoD) and the Army established the Joint Improvised Explosive Device Defeat Organization and the Army Asymmetric Warfare Group to better understand, analyze, and adapt to threats. Collaboration led to newly developed joint equipment and technical intelligence tools.[2]

Though adaptation was acknowledged on broad scales, many analysts found it difficult to do so cognitively and technically. Few were fully trained on these dynamic problem sets. Many struggled to incorporate unfamiliar topics into analyses, and proficiency levels varied based on units' ability to balance specialized training with other pre-deployment requirements. During my last deployment,

I saw this firsthand. Analysts impressed me with their efforts to understand culture, tribal-based politics, asymmetric tactics, and tools they received in theater. However, steep learning curves and information overload oftentimes resulted in significant activity reporting versus intelligence. Many struggled to incorporate before-unseen data, such as biometric and explosive components, into their analysis and collection requirements. On-the-job exchanges with subject matter experts helped but only to a degree.

Interestingly, many concepts that analysts found challenging to evaluate were already familiar topics in their daily lives. They understood that politics, economics, and social beliefs affected their own communities, and that law enforcement used technical means to uncover leads. The challenge was to align this "immersed" mindset early enough to convey that apart from resourcing, the core tenets of intelligence did not change with one's location.

Human Instinct and Incentives: The Key to Adapting to the Contemporary Environment

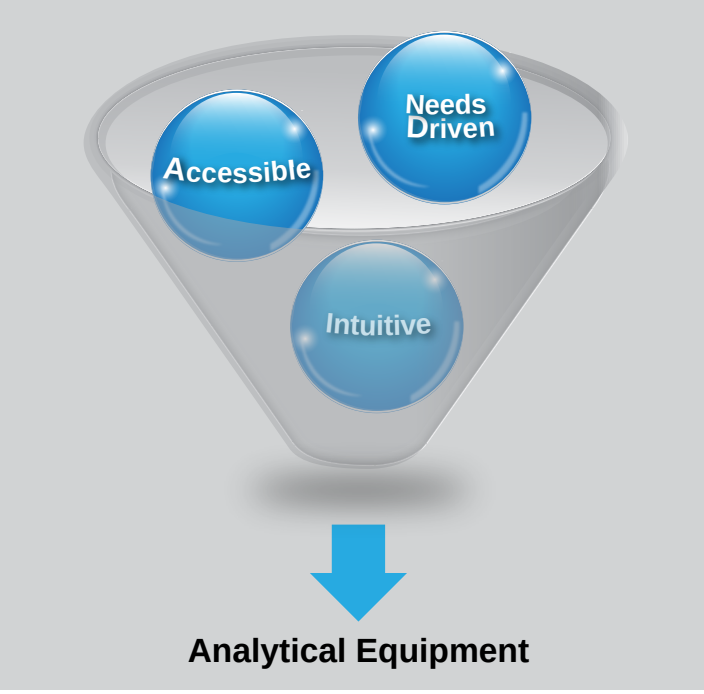
The technology-centric cyberspace domain is a natural progression of the evolving environments. It enables state- and non-state actors to project power remotely, increasing relative strength with moderate investments. It has also elevated the significance of criminal actors and other organizations that formerly were only tangentially considered. As individuals, we are immersed in this environment daily. We are well-versed in new technology and understand how it can be weaponized. Private sector security compromises, the Office of Personnel Management breach, and concerns over "fake news" are a part of life. Though this immersion should make it easier to incorporate these considerations into analysis, the learning curve is still steep. Why is this so? It comes down to having to analytically adapt to multiple paradigm shifts—not only the advent of the cyberspace domain but also the growth of regular, irregular, and hybrid threats—and needing more fundamental changes in the support structures to enable this transformation.

The DoD and the Army are embracing tenets of the technology environment like rapid transformation, agility, and adaptation. Prototypes and existing capabilities are helping shorten development timelines and needs-based features into acquisitions.[3] From a knowledge perspective, manuals and publications have been updated to reflect aspects of the contemporary environment. Analysts are being assigned to cyber units for "hands-on" learning; courses exist for others to attend. Leaders have participated in classes, workshops, and field demonstrations to understand how technology, the threats, and multi-domain considerations influence combined arms maneuver.

However, in addition to these models, we can better adapt using insights from nongovernmental sectors. In the business world, "just-in-time"[4] operations management revolutionized the industry by maximizing each aspect of operational sub-processes. In the technology sector, the Agile Methodology[5] exploited end-user insight to design software, breaking free of lengthy linear approaches and process bottlenecks. Both methods point to the oft-overlooked centrality of the human aspect of systems. Our approach to analytical modernization should fully explore how we can apply these concepts to all-source intelligence in a changing environment.

Make Analytical Equipment Needs-Driven, Intuitive, and Accessible. Let us first look at the most tangible part of the analyst's weapon system: analytical equipment and tools. Contemporary tools must help analysts examine conventional and hybrid peer and near-peer threats, keep pace with the refresh cycle of the technology environment, and be practical in myriad operational environments; in short—requirements, needs, and real-world considerations. Analysts require data aggregation and sharing. They also need systems that account for varying skill levels, high stress, information overload, connectivity problems, and adversary attacks. Grounding system development in users' habits and patterns can help to improve the initial efforts to address these concerns.

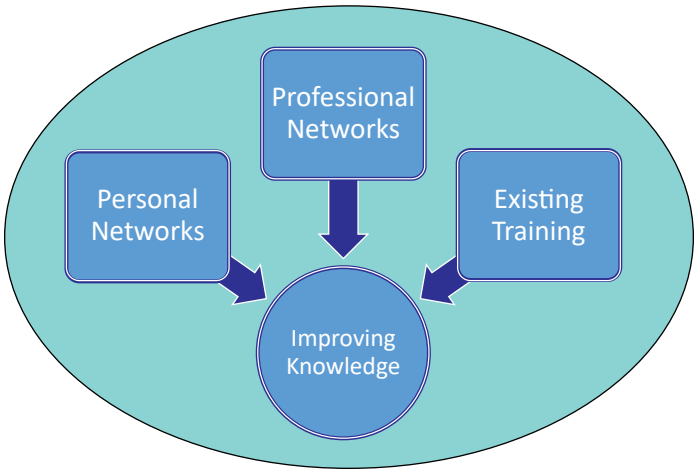
- **Human Factors and Needs.** It is no secret that external human factors influence analytical processes. Despite system capabilities, mission needs will always drive analysts to use the most practicable means to provide value



to their commander's decision-making process. As an example, some rotational units at the Joint Readiness Training Center established the Distributed Common Ground System-Army on tactical networks but reverted to manual methods (such as PowerPoint) for analysis, production, and dissemination.[6] System design must consider human factors like commanders' needs and analytical "fall-back" practices. If we can find ways for systems to address issues like these—synchronizing digital and analog products, or tracking dispersed system updates to cue alternate information request methods—we could preserve responsiveness to commanders while maintaining system accuracy and use.

- **Intuitive Interfaces and Learning Systems.** Contemporary budgetary and training constraints, coupled with rapid system changes, can contribute to "fall-back" practices and limit analytical capability and capacity. Like the private sector, the Army can overcome these challenges with intuitive, organically improved software. Intuitive interfaces would improve user proficiency through experiential discovery. Machine-enabled assistance, such as suggestions, requests for report feedback, and user data analytics, could help improve the usability and quality of systems. By engaging with stakeholders and specialists—junior analysts, supervisors, task-organized non-intelligence Soldiers, collectors seeking feedback, software developers, and behavioral psychologists—we could better align digital systems with natural analytical habits. These systems would help analysts of all proficiency levels, and those tasked to support intelligence efforts, contribute their fullest abilities to a unit's mission.
- **Accessibility and Habits.** Even if tools meet user needs and are intuitive, accessibility is key to refine skills and reinforce good habits. Current cloud-based systems are a good first step, but we should continue to explore ways to innovate. Government devices with mobile analytical software, commercially available solutions that mirror system interfaces, and unclassified news aggregator apps that allow individuals to mark, associate, and analyze reports could help analysts train on the go. While these ideas would come with risks that require evaluation, incorporating these processes into normal routines could help strengthen analytical practices.

Make Knowledge Accessible and Reinforcing. In line with making analytical tools intuitive, accessible, and grounded in human habits, the same ideas should be applied to improving an analyst's knowledge. Many Soldiers have become comfortable operating in a counterinsurgency environment. Some few remember how to analyze conventional



threats. However, many find the changing multi-domain environment confusing as advances in technology affect our assumptions about key aspects of the environment and our adversaries. Terrain and borders now span many layers and are semipermanent. Threat actors may be hard to define, and can be partners under certain circumstances. Tactical actions can create strategic effects but also cause unintended blowback. Like all Soldiers, analysts across the Army balance many competing requirements—daily tasks; 6-week, quarterly, and annual training requirements; family matters; and career progression. Responsibilities that do not reinforce warfighting analytical skills or knowledge can quickly consume an analyst's time. By better understanding analysts' competing priorities, we can augment existing training, operations, and incentives to improve knowledge and critical thinking.

- **Incentivize Analysts' Networks.** In complex networks, many influencers shape an individual's perceptions, goals, values, and priorities. As such, engaging analysts' personal and professional networks could strengthen constant learning. Personal networks encourage and support analysts to master new skills, progress in their careers, and develop themselves holistically. Professional networks do much of the same. "Soldier/Noncommissioned Officer of the Year" and "Best Warrior" competitions groom Soldiers to improve, while bringing pride to individuals and units. Specialized career fields and organizations leverage this competitive mindset to improve technical skills—Explosive Ordnance Disposal has an annual Team of the Year competition, the Defense Advanced Research Projects Agency hosts cyberspace hacking tournaments, and other units include critical thinking aspects to competitions. Standalone analytical challenges, or the addition of analytical aspects to existing competitions, would incentivize Soldier networks

to encourage analytical proficiency. To units, the events would create near-term goals to reinforce intelligence tasks, encourage analysts to improve analytical skills and knowledge, and give leaders better insight about their analytical force. By incorporating individual incentives into these events, such as evaluation, promotion, or permanent-change-of-station (PCS) considerations, broader portions of an analyst's network would be encouraged to reinforce analytical proficiency.

- **Create an Operational Context for Career Progression.** Apart from unit communications, Soldiers generally prioritize branch correspondence because critical information about promotion boards, PCS options, and newsletters about career progression are important to them. As such, leveraging branch communications to highlight operational context—from deployments or combat training center rotations—would frame broader continuous knowledge improvement as a key part of career advancement. A colleague recently took this "tap into branch" approach in starting an analyst-to-analyst collaborative effort with hundreds of other captains from across the branch. Though unconventional, the exchange opened up lines of communication, shared observations, and spread valuable knowledge about Army enablers and resources.
- **Tap into Existing Training.** Lastly, efforts to improve knowledge should be incorporated into as many existing training opportunities as possible. Recently, Secretary of Defense James Mattis called for a reevaluation of mandatory training requirements to ensure they support core operational warfighting tasks.[7] After this review, some online training will likely remain but should be refined to give Soldiers an understanding of the topic's mission impact. For example, cyber awareness training has improved cyberspace hygiene but does not address threat employment of cyberspace weapons. Issues such as the Office of Personnel Management breach and cyberspace-enabled espionage clearly affect the warfighter and DoD. Incorporating unclassified news reports and assessments into existing training would constantly remind analysts of the need to include all aspects of their immersed environment into analyses.

Conclusion

In summary, the Army—like organizations in the private sector—is in the business of achieving goals. To best do this, we develop plans to achieve proficiency, train, assess individual and collective training, and retrain. We seek to modernize our equipment and processes to address changes in the environment that do not work well with old models. What we must apply more effort to, however, is how our human resources change with that environment. By adapting our equipment and goals to the human aspect of our weapon system, we can better innovate and uncover ways to improve.

Endnotes

1. GEN Stanley McChrystal, Tantum Collins, David Silverman, and Chris Fussellet, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin Random House, 2015).

2. Thomas B. Smith and Marc Tranchemontagne, "Understanding the Enemy: The Enduring Value of Technical and Forensic Exploitation," *Joint Force Quarterly* 75 (September 30, 2014), http://ndupress.ndu.edu/Media/News/Article/577571/understanding-the-enemy-the-enduring-value-of-technical-and-forensic-exploitati/.

3. Aaron Mehta, "Strategic Capabilities Office Preparing for New Programs, Next Administration," *Defense News*, September 9, 2016, https://www.defensenews.com/pentagon/2016/09/09/strategic-capabilities-office-preparing-for-new-programs-next-administration/.

4. "Just-in-time manufacturing," Wikimedia Foundation, last modified 16 June 2018, 13:30, https://en.wikipedia.org/wiki/Just-in-time_manufacturing.

5. "Agile Methodology: Understanding Agile Methodology," Agile Methodology, September 15, 2010, http://agilemethology.org/.

6. Nathan Adams, "Observations from a Year as the Brigade S-2 Observer-Coach-Trainer at the Joint Readiness Training Center," *Military Intelligence Professional Bulletin* 43, no. 2 (April–June 2017): 12.

7. Tara Copp, "Mattis: Get unnecessary training off warfighters' backs," *Military Times*, July 25, 2017, http://www.militarytimes.com/news/your-military/2017/07/25/mattis-get-unnecessary-training-off-warfighters-backs/.

CPT Christie P. Cunningham is currently an Army Congressional Fellow. She is a career intelligence officer with private sector experience. Her recent assignments have included Commander for Headquarters and Headquarters Company, 781st Military Intelligence Battalion (Cyber); Deputy Analysis and Control Element Chief, Army Cyber Command; assistant brigade S-2, 95th Civil Affairs Brigade; and battalion S-2, 192nd Ordnance Battalion (Explosive Ordnance Disposal).

Collecting in Vichy: Intelligence Operations in the French Resistance

by Captain Charles F. Nadd

How it Began

As Nazi Germany invaded France in the late spring of 1940, the French citizenry saw a rapid, unprecedented erosion of their national institutions: their border defenses and the Maginot Line were defeated, their military was in retreat, and their government was forced into exile. The 35-day Battle of France that ended with Nazi Germany's arrival in a largely undefended Paris on June 14, 1940, left the newly occupied nation humiliated and her people eager for an opportunity to reverse their fortunes. It was in this framework that citizens quickly banded together to form a movement that became known as the French Resistance. These networks, centered on a "military structure," did not have the resources to execute overt action against the German occupiers but were able to prove very capable in "gathering intelligence for Free France or the Intelligence Service."[1]

Among the most robust and active components of the French Resistance from 1940 to 1944 was the *Bureau central de renseignements et d'action* (BCRA), a descendant of the *Deuxième Bureau de l'État-major général.* The intelligence collection apparatus grew and changed from its inception through the end of the war but remained a constant source of accurate, actionable intelligence for both those fighting in the Resistance and with the Allies. The BCRA's ability to collect, securely hold, and quickly disseminate reliable intelligence in Vichy France, despite competition between rivaling networks, played a pivotal role in preparing the Allied powers for Operation Overlord and the eventual defeat of Nazi Germany in Western Europe.

A Government-in-Exile

While a French government-in-exile quickly formed in Great Britain, many highly skilled military and intelligence personnel remained in occupied France, setting the groundwork for an unprecedented collection operation. This expertise delivered a unique resource for exiled leadership and Allied planners on the opposite side of the English Channel between 1940 and 1944. Specifically, "French resistance operations…before 1944 focused on surveillance; intelligence collection against German order of battle; repatriation of downed pilots; stockpiling of weapons for D-Day; and sabotage."[2] Those in Great Britain were able to better plan and execute bombing attacks, strategic logistical operations, and the eventual Normandy invasion thanks to the skilled cadre on the ground throughout France.

In fact, there was such extensive experience within the occupied territories that multiple intelligence networks emerged: a number of "Resistance groups within France each had an intelligence network."[3] Subordinate resistance groups like the "Cohors Asturies, Centurie, Turma-Vengeance, and Fana…gathered and distributed information about the German Army and war production, as well as assisting in the rescue of Allied aircrews escaping through France."[4] This reality created a steady flow of actionable intelligence from different regions of France. Exiled headquarters in Great Britain were able to understand the movements and machinations of the German war machine, helping them to better identify resource allocation and determine their enemy's likely future courses of action.

Operation Overlord

While the diversity of information was critical in helping planners understand the German situation, it is equally true that the various networks that made up the Resistance served as the primary source of intelligence in the weeks and months leading to Operation Overlord. André Dewavrin, codenamed "Colonel Passy" and the father of the French Resistance's intelligence operation, explained that his forces "were furnishing the Allied general staff with 80 percent of its intelligence on France."[5] They accomplished this with covert cross-Channel air taxi deliveries and seaborne agent transports.[6]

Certainly, such a haphazardly organized collection operation was not without its flaws. Born of an age-old disdain and contemporary distrust for the British, French intelligence agencies created "a separate French code" to

Photo Credit: U.S. Army Signal Corps photographer, from the collections of the Imperial War Museums.

Watched by two small boys, a member of the French Forces of the Interior poses with his Bren gun at Châteaudun.

overcome suspected eavesdropping.[7] Due to frustrating practices like these, the role that Resistance French intelligence truly played during the Second World War remains contested. Some historians go so far as to claim "that the French played a significant role in their own liberation through intelligence collection, sabotage, and guerrilla actions against the German occupiers became a 'necessary myth' in postwar France," serving as "a psychological crutch that helped France limp beyond the humiliation of 1940."[8] The legacy of the collection capabilities, both in terms of breadth and depth, of the French Resistance was significant enough for Dewavrin's (Passy's) 1998 *New York Times* obituary to assert that, "by D-Day, June 6, 1944, Mr. Dewavrin's network had mounted extensive sabotage operations and provided Eisenhower, the Allied commander, with so much information that he said the Resistance was worth six allied divisions."[9]

In addition to being able to collect large amounts of actionable intelligence, securely holding information and materiel was a responsibility of critical importance for the fledgling French Resistance network. Of particular import was the conscious accumulation of resources to aid in future operations. Specifically, "in the surviving French Army, officers hid weapons and ammunition and organized intelligence networks, preparing for future battle against Germany."[10] While "other military leaders fled to Britain with Brigadier General Charles de Gaulle (q.v.) to form the Free French movement based in London," those same leaders left a cadre of capable, reliable officers to build cache sites, develop methods to collect and hold valuable intelligence, and help integrate the efforts of citizens within the French Resistance with the government-in-exile.[11]

Role of the *Bureau Central de Renseignements et d'Action*

As critical as the abilities to collect and hold intelligence were during the period from 1940 to 1944 in Nazi-controlled France, these efforts would have been rendered meaningless without an effective way of disseminating their output. To this end, the venerable "Colonel Passy" personally "ran the BCRA in an office in Duke Street, London."[12] The intelligence officers knew exactly to whom they reported and how they could deliver information to him. This singular node of information was particularly useful in disseminating a wide range of intelligence from a wide range of informants and sources across the Channel. Colonel Passy had effectively become a clearinghouse for actionable intelligence and, "by 1944 the BCRA was producing an information sheet twice a day for the Allied intelligence community."[13]

This unique advantage did not come without its challenges. Because of regional interests and the competitive nature of the relationship between different intelligence networks within the French Resistance, "the BCRA effectively became a tributary, sometimes even a hostage, to local Resistance groups in intelligence collection and action missions."[14] While this may have destroyed the BCRA's ability to provide accurate, timely information, the underlying reality remained that "the intelligence networks in France had loyalties to different leaders but they were united in wanting to work for the defeat of Nazi Germany and the liberation of France."[15] This unifying factor allowed Colonel Passy to become one of the most prolific military intelligence officers of all time, despite working in exile. Indeed, by 1944 the effort was so unified that the competing intelligence networks "all used the same air taxi service," and those air taxis all delivered to Passy.[16] One officer had positioned himself to be the central node for intelligence dissemination from the French mainland. This simplified the process of intelligence dissemination, which provided an invaluable service to both Free French headquarters and the Allied forces.

A Philosophy of Liberation and the Intelligence Network

Another aspect of the French Resistance that proved to be critically important, especially in southern France where people could meet more freely than in the occupied zone,

was its deeply intellectual nature. French Resistance networks became keenly aware of the significance of information operations and spreading the ideas that defined the Free French movement. Indeed, "most resistance encompassed some form of written resistance: the disseminating of information and ideas, the dispelling of propaganda or devising ruses against the occupiers."[17] This focus on spreading the philosophy of liberation grew concurrently with the focus on spreading the intelligence that would make that possible with the exiled government. This bimodal approach to insurgent warfare was unmatched on any contemporary battlefield.

In the weeks leading to the June 6, 1944, Allied amphibious landing on the beaches of Normandy, General Dwight D. Eisenhower wrote to his wife Mamie that, "I seem to live on a network of high tension wires," due largely to "intelligence information acquired…that indicated the Germans were reinforcing the area where the American paratroopers were going to drop."[18] This demonstrates how critical information about German operations was to those in the highest levels of Allied leadership. Historians explain today that "intelligence offered one way in which the internal Resistance in France could influence the external Resistance in London."[19] As the government-in-exile and its international partners prepared for the re-invasion of France, the intelligence that was collected, secured, and disseminated served a critical, practical purpose: it was used to build strategy.

Though the vast network of diverse collection operations within the French Resistance eventually helped set the stage for a successful liberation of France, the internal discord that existed within the movement was nearly crippling. As late as mere weeks before the 6th of June landings in Normandy, "the Mediterranean theater was fast becoming a secondary front in every struggle but that of the civil war which raged within the French intelligence services."[20] A desire to be recognized and exert influence on policies being formulated in Great Britain drove an incredible competitive spirit between these organizations. Ultimately, Colonel Passy was able to help the Allies overcome these challenges.

Conclusion

Against this tenuous backdrop, the ability of the intelligence networks in the French Resistance and the leadership of the government-in-exile in Great Britain to unite to achieve effective intelligence collection, security, and dissemination was nothing short of extraordinary. These intelligence efforts set the stage for the successful Allied invasion and, eventually, the fall of the Vichy France regime. They exposed the Germans' greatest weaknesses and supported Allied fighters as they arrived to exploit them.

Endnotes

1. Antoine Prost, *La Résistance, une histoire sociale* (Paris: Les Éditions de l'atelier, 1997), 43.

2. Rodney P. Carlisle, *Encyclopedia of Intelligence and Counterintelligence* (Armonk, NY: M. E. Sharpe, Inc., 2005), 164.

3. David T. Zabecki, *World War II in Europe: An Encyclopedia* (New York: Routledge, 1998), 150.

4. Ibid.

5. Douglas Porch, *The French Secret Services: A History of French Intelligence from the Drefus Affair to the Gulf War* (New York: Farrar, Straus and Giroux, 2003), 228.

6. Craig R. Whitney, "Andre de Wavrin, 87, 'Col. Passy' of Resistance Fame, Dies," *The New York Times*, December 22, 1998.

7. Ibid.

8. Thomas C. Bruneau, *Reforming Intelligence Obstacles to Democratic Control and Effectiveness* (Austin: University of Texas Press, 2007), 136-137.

9. Whitney, "Andre de Wavrin."

10. Zabecki, *World War II in Europe,* 150.

11. Ibid.

12. Terry Crowdy and Steve Noon, *French Resistance Fighter: France's Secret Army* (Oxford, UK: Osprey Pub., 2007), 12.

13. Ibid.

14. Porch, *The French Secret Services*, 229-230.

15. K.G. Robertson, *War Resistance and Intelligence* (Traverse City, MI: Cooper, 2000), 184.

16. Ibid.

17. Zabecki, *World War II in Europe*, 151.

18. Stephen E. Ambrose, *Eisenhower: Soldier, General of the Army, President-elect*, 1890-1952 (New York: Simon & Schuster, 1985), 367-368.

19. Porch, *The French Secret Services,* 230.

20. Ibid., 223.

CPT Charles F. Nadd served in Operation Enduring Freedom as a Battle Captain and Black Hawk pilot. He graduated from the Military Intelligence Captains Career Course as an honor graduate in 2015 and was then assigned to Fort Bliss, TX, where he served as a Company Commander and RC-12X pilot. CPT Nadd was most recently forward deployed as the Guardrail Detachment Commander in Afghanistan. He has a bachelor's degree in political science and U.S. history from the U.S. Military Academy.

Army Aviation Association of America Soldier of the Year

by Ms. Jocelyn Broussard, U.S. Army Intelligence and Security Command Deputy Public Affairs Officer

The Army Aviation Association of America (AAAA) presented a U.S. Army Intelligence and Security Command (INSCOM) Soldier with its Soldier of the Year Award during the association's 2018 Army Aviation Mission Solutions Summit in Nashville, Tennessee, on 26 April 2018. Vice Chief of Staff of the Army GEN James C. McConville presented the award to SPC Madeleine R. Rampona, A Company, 224th Military Intelligence (MI) Battalion, 116th MI Brigade, INSCOM, Hunter Army Airfield, Georgia. MG William K. Gayler, Commander, U.S. Army Aviation Center of Excellence, participated in the presentation.

SPC Rampona accepted the Soldier of the Year Award and humbly thanked her coworkers and leadership. "I feel honored to have won the award," said SPC Rampona. "I want to thank some of my NCOs, the warrant officers, and commissioned officers. Everything I know, I learned from them."

SPC Rampona was selected for the award for her numerous achievements, including quickly mastering all required training of an aerial sensor operator, which enabled her to effortlessly assume duties as a flight instructor. She achieved the status of a fully qualified aerial sensor operator and flight instructor for the Army's newest aerial intelligence, surveillance, and reconnaissance platform—the Enhanced Medium Altitude Reconnaissance Surveillance System (EMARSS) aircraft.

According to SPC Rampona's supervisor, her accomplishments are exemplary considering her short time of service in the Army. "Specialist Rampona has demonstrated a competence and professionalism beyond her three years of service," said SGT Kevin Costa. "In that short period of time she has quickly outpaced others in her profession and become the most qualified aerial sensor operator in our unit."

SGT Costa added that SPC Rampona's contribution to the development of the EMARRS nonrated crewmember training program at the 224th MI Battalion was instrumental in preparing multiple groups of fellow Soldiers for worldwide deployment.

SPC Rampona leveraged her unparalleled knowledge of MI and aircraft full motion video systems to provide outstanding support during her deployment to U.S. Southern Command and stateside training events. "Rampona's initiative and self-development is what set her apart from her peers," said CPT Jordan M. Schumacher, Commander, A Company, 224th MI Battalion. "The EMARSS program of record is one of the newest in the Army, and she saw the opportunity to make a positive impact and ran with it. Her attention to detail resulted in the development of [aerial sensor operator] ASO checklists and troubleshooting guides that has reached three different [combatant commands] COCOMs, well beyond her scope of influence."

SPC Rampona's battalion and brigade commanders are also very proud of her accomplishment. "The Soldiers, Families, Civilians, and defense partners of the 224th MI Battalion could not be more proud to have Specialist Rampona amongst our ranks. Her selection as the AAAA Soldier of the Year highlights one of the most underrated enlisted crewmembers in Army Aviation, the aerial sensor operator," said LTC Nathan Lewis, 224th MI Battalion, commander. "When Soldiers are in harm's way in combat and need a guardian angel above them, Rampona and her ASOs can provide that voice and eye from above to direct them to safety. Her selection for this award demonstrates the fusion and synchronicity of Army Aviation and military intelligence towards safeguarding our forces and seeking out to destroy the enemy."

The 116th MI Brigade's recent successes in support of worldwide operations are entirely dependent on the training, proficiency, and professionalism of Soldiers like SPC Rampona, according to its commander. "Intelligence Soldiers and nonrated crew members like Specialist Rampona are the center of gravity of the 116th Military Intelligence Brigade (Aerial Intelligence) and our intelligence, surveillance, and reconnaissance manned capabilities," said COL Daniel Mettling, Commander, 116th MI Brigade (Aerial Intelligence).

COL Mettling added that SPC Rampona's recognition as the AAAA Soldier of the Year is a testament to the credibility and trust his brigade's Soldiers have built with the maneuver forces' brothers and sisters in harm's way across the globe. "As the Commander, I could not be prouder of any individual in our formation to achieve such recognition and accolades; and am certain the entire brigade is equally proud of her distinguished accomplishment," said COL Mettling.

SPC Rampona has led the way for aerial sensor operators onboard Army aircraft, completing more than 90 missions in her short career. She is currently serving on her first combat deployment in support of Operation Inherent Resolve and plans to return to her home station to continue training more aerial sensor operators to provide the voice and eyes from above.

Biography of Specialist Madeleine R. Rampona

U.S. Army photo

SPC Madeleine Rampona was born in Fort Bragg, North Carolina, and graduated in 2015 from First Colonial High School, Virginia Beach, Virginia. She enlisted in the U.S. Army and began basic combat training in November 2015 at Fort Leonard Wood, Missouri. After basic training, she attended a 24-week Advanced Individual Training at Fort Huachuca, Arizona, where she received a certification of completion for the military occupational specialty 35G, geospatial imagery analyst.

Following her training, SPC Rampona went to her first duty assignment at Hunter Army Airfield, Georgia, with Alpha Company, 224th Military Intelligence Battalion, 116th Military Intelligence Brigade. During the assignment, she accomplished more than 90 missions as an aerial sensor operator on the MC-12 S/M aircraft and trained five people as a flight instructor. She is currently serving on a deployment to an undisclosed area in support of Operation Inherent Resolve.

SPC Rampona's military education includes the Special Electronic Aircraft Course, Special Survival Skills Course (SV-38), and hypobaric chamber training. Her awards and decorations include the Army Achievement Medal, National Defense Service Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, and Army Service Ribbon.

SPC Rampona was awarded the Army Aviation Association of America Soldier of the Year Award at the 2018 Army Aviation Mission Solutions Summit in Nashville, Tennessee, on 26 April 2018.

U.S. Army photo

SPC Madeleine R. Rampona and LTC Nathan Lewis, Commander, 224th Military Intelligence Battalion, pose with the Army Aviation Association of America Soldier of the Year trophy.

Introduction

This past fall, representatives of the Training and Doctrine Command Culture Center were privileged to travel with the Regional Leadership Development Program-Pacific (RLDP–P) in support of its cultural immersion phase, visiting several nations in the Indo-Pacific region.[1] The trip provided ample food for thought, including thoughts about the United States' image as it is presented through various forms of media. In the 21st century, many people see the United States' power as plateauing, or even declining, and China's power as rising. Our image is more important now than ever before, and America may need to maximize international awareness of all the good it has to offer. The conscientious use of cultural awareness can help make this happen.

How is the United States Perceived?

The United States is still "on top" in many ways, but some places in the world are catching up to, if not surpassing, the United States in various aspects. This is especially true when it comes to economic growth rate and affordable consumer technology. Research generally shows that China is gaining on the United States in terms of how countries perceive a foreign power. For example, the Brookings Institution conducted a study that indicates the majority of nations in the Indo-Pacific region see China as Asia's most influential power.[2] Many countries, especially in Europe, also see China as the world's leading economic power.[3] While one may debate the validity of these perceptions, the existence of the perceptions creates a reality in terms of other countries' opinions about the United States as a world power. The perceptions influence the choices those countries make when forming alliances, both today and in the future.

Our public image as viewed by another culture's consciousness plays a significant part in our geopolitical and strategic presence. With the many economic and political options, one can argue that a country's image is more important than ever before. In the West, highly biased or unvetted news, internet sources, and social media often convey that public image. This view of the United States, and the influence of our own mass media on those views, is becoming the standard on which people around the world base their opinions, especially millennials and post-millennials.

Observations from the trip to the Indo-Pacific region consistently confirmed our own media's effect on the world's opinion of the United States. Today, we have more *ways* to get information, which we often confuse with having *better* or *more* information. An increasingly biased, narrowly sourced, rumor-based, and less validated media shapes much of the world's public consciousness. In many cases, our movies, social media, and overtly or clandestinely agenda-driven internet sources also inform the professional foreign media.

Regardless of one's views about our media, the bottom line is that it generally portrays an overwhelmingly negative assessment of America—civil strife, conflict, racial and cultural divisiveness, violence and murder seen in the form of a

gun culture, and almost cartoonish "good guys vs. bad guys" sociopolitical atmosphere. To those people who have little or no direct contact with Americans, what is portrayed in our sensationalized media, in all of its forms, "is" America. Polls, such as one that global market research company Ipsos conducted, show public opinion of the United States drops precipitously following a barrage of negative press, such as after President Trump's election, rather than after a policy change that has time to affect the world, providing quantifiable evidence of this phenomenon.[4] This can also be seen by perusing YouTube videos or social media posts that essentially parrot the most antagonistic take on whatever is currently trending, but in exponentially multiplying numbers, with decreasingly truthful and increasingly outrage-inducing content—essentially the telephone game gone horribly awry.

Far-Reaching Effects

It is important for all Soldiers to know that for many people in other countries, our media image is the only available filter through which the locals judge us. Time and again during the RLDP–P trip, people of various ages and nationalities asked about the only America they know—the one shaped by our media, rather than information they gained through education, experience, or an awareness of American policies relevant to their own country. And their curiosity was genuine. The most openly opinionated were some Australians and New Zealanders traveling through the region. They aggressively approached Americans with near-inquisitorial agendas regarding their internet, press, movie, and TV-informed version of media hot-button issues that were inaccurate, sensationalized, and one-sided.

While propaganda, information, and other forms of media have always been a factor in our military thinking, the

Photo by CPT Joshua Taft

Students from the RLDP–P visit tour the Korea Expressway Corporation Headquarters on Sept. 28, 2017.

Information Age has grown media into an 800-pound gorilla. In a world where both media companies and user-driven social media can instigate massive political pressure, protests, and uprisings, we have greater democracy—with all the good and bad that can come from the opinions, actions, and will of the public (however well- or ill-informed they may be). In many countries, the mass will of the populace, enabled by the various forms of media and the internet, is more easily susceptible to the rampant effects of social proof than ever before. This can be a wonderfully constructive phenomenon—or a destructive one. This rapidly mobilizing effect can take different forms, from causes such as the #MeToo movement to the Arab Spring, and can supercharge the ramifications of individual tactical-level events on an international scale. An example is the response to human rights violations against detainees in the Abu Ghraib prison in Iraq, both in the United States and abroad. In extreme cases, it is readily apparent that to a much greater, widespread, and sophisticated degree, entities such as terrorist organizations can access and manipulate what we see into "weaponized" media. This had been historically limited to nation-states and large political or economic entities—actors who often had aims that were clearly identified or at least were open to some modicum of reason, restraint, or negotiation.

But in the 21st century, the potential to manipulate the media is open to almost anyone, regardless of what they have, or don't have, to lose. It is obviously not lost on several extremist organizations that much of America and Europe, with their generally wealthier populations, are further removed from survival-level existence than other people in the world. Because of this, Westerners are particularly susceptible to the influence of media, which is often their main contact with issues and consequences of day-to-day struggles or fears. Public perception considerations in many situations are no longer just considerations for strategic decisions, but potentially central factors in determining courses of action.

The 1Malaysia Program

For most of the 20th and 21st centuries, much of America's "message" has centered upon the opportunity, personal freedom, and material advantages that our lifestyle and values create. However, not only does much of American media output contradict this message, it may actually be an argument against the message of democracy, multiculturalism, and personal freedoms themselves. When one thinks of the collectivist, order-seeking culture that some nations around the world have, what is our media culture presenting as the benefits of an individualist, diverse, open democracy? The world hears about our violence, discord,

racial strife, a grim middle-class job outlook, greed, amorphous forces bent on ill doings, and social and political vitriol. Is this the American-style alternative to the order, stability, and peace (even if it is an enforced peace) that collectivist, more government-centered authority systems, such as China or Russia, are offering? Yet many Americans are surprised when people from different cultures and vastly different educational levels tell us that they either don't want what they see as U.S.-style democracy, or at least not too much of it.

One of the places where this occurred was Kuala Lumpur, the capital of Malaysia. Malaysia is a country with both a multicultural and collectivist society where the people value harmony and the stability it brings over the potential chaos and conflict that individualism can bring. There are many different ethnic and religious groups in Malaysia, along with the various issues that so often accompany such a situation. One of the methods the government is employing to overcome some of these issues is the 1Malaysia program, which seeks to have people socially embrace and publicly emphasize the unity of Malaysia's diverse population, even though there is comparatively little one-on-one social interaction between individuals belonging to different ethnic and religious groups. The general "line" given during the RLDP–P trip was that "everybody gets along." A skeptical American's first reaction to the 1Malaysia program, which emphasizes a single country over the undercurrent of some serious societal divisions, might be one of wry cynicism—"As if saying people are 'one' really makes it so!"

The Small, Everyday Things Matter

While everyday social niceties may not address underlying societal problems, they might make for smoother everyday interactions and less open conflict. Consider the acerbic, polarized, and fractious elements of our individualistic culture where loudly proclaiming confrontational views, without any interest in hearing alternate opinions, is acceptable and even celebrated by those who share the same viewpoint. Employing a little more etiquette toward public discourse might help create an atmosphere of dialogue and solution-seeking debate rather than the polarizing character of public discussion glorified by much of our media and tacitly, if not actively, supported by members of academia. This, of course, would not play well in our sensationalized social and mass media atmosphere where high ratings, pushing an agenda, or "going viral" is so often the objective for Americans, and in so many other countries the atmosphere people wish to avoid.

So, what can we do to counteract this? It is already a given that as Soldiers and representatives of the United States, we should be culturally aware. But are we regularly doing the simple albeit easily overlooked things? We should not just read a few books on cross-cultural competency and specific cultures. We should consistently turn this into training and guidance for all echelons, not for just the designated key leader engagement participants, civil affairs Soldiers, or advisors. Are we systematically and deliberately emphasizing the small, everyday things that can contribute to perceptions of America through foreigners' personal experience? The cynical or hostile media cannot corrupt or reshape Soldiers' direct experiences in the same way it can with national-level policies or high-echelon operations.

We are generally a friendly and talkative people. Simply educating all Soldiers about topics and behaviors that are acceptable and not acceptable in whatever country they're in can make a huge difference in how other people feel about Americans. This impression will spread through word of mouth and will show up on social media, replicating itself and creating or reinforcing a positive impression of Americans. Deliberately facilitating positive interactions between U.S. personnel and the local population at every echelon can be a way to multiply this effect.

A case in point, during a deployment to Iraq an hour-long session of playing dominoes favorably changed the dynamic between U.S. Soldiers and Iraqi Army and Border Enforcement soldiers. This occurred when senior leaders were holding a meeting on a very small U.S. base. The Iraqis had some of their security personnel shown to a tent to wait. Up until that time, some U.S. Soldiers had experienced being received with wariness, skepticism, and even borderline hostility during incidental "joe to joe" encounters while visiting Iraqi border posts. With some of these same personnel now on the U.S. base, a few U.S. Soldiers (and two interpreters) went to the tent where the security personnel waited, bringing some cots for the Iraqis to sit on, and dominoes, a popular Iraqi pastime. The U.S. Soldiers began by conversing only about dominoes, using the Iraqis' communication styles, but with a slightly more open and friendly body posture

U.S. Army photo by PFC J. Princeville Lawrence

SSG Larry Saunders waits for CPT Timothy Vandewalle to lay his dominoes during a game on Camp Savage, Iraq, Oct. 31, 2009.

and facial expression. They also progressively increased the use of physical and verbal humor and culturally common conversation topics to build a rapport with the Iraqis. In less than 25 minutes, the tent filled with laughter and conversation. On his own initiative, one Iraqi soldier said that simply sitting there, talking and playing dominoes with the U.S. Soldiers, had completely changed his opinion of Americans. He said he previously thought of Americans as intruders who did not care about what happened to Iraqis, but now he saw that Americans were "just people," and largely just like them. By the time the meeting was over, names, humorous stories, and even thoughts on the value of family had been exchanged and some friendships had begun. For the rest of that tour, trips to border stations, even if none of the personnel there had participated in the domino games, were much more relaxed and often imbued with a sense of friendship.

A Simple Photo Op Can Help

During the RLDP–P trip, after a reception led by senior, male Malaysian leaders, a young female U.S. captain asked some young female Malaysian soldiers if they would take a few pictures together with her. This simple interaction instantly created camaraderie—as Soldiers, women Soldiers, and world citizens—as well as a favorable impression of the United States. Pride and appreciation of the U.S. officer's gesture were plainly evident in the beaming smiles of these Malaysian soldiers, and a personal, emotionally cemented impression of the United States as an inclusive and welcoming culture was established that might strongly counterbalance social media posts or news stories decrying U.S. ethnocentrism or sexism.

While these kinds of encounters do not guarantee that everybody is going to join hands with us and sing Kumbaya, they usually require minimal effort, have the potential to pay big dividends, and already naturally take place wherever our Soldiers are. A coordinated effort to make these types of interactions happen could collectively make a positive difference in accomplishing our missions, especially when there are so many cultures for which establishing personal relationships is a critical aspect of getting things done. Even something as innocuous as making sure that all units working in view of locals are as diverse as possible can show that American-style individualism and diversity not only works, but does so in a cooperative, harmonious way.

China's Presence

Certainly, the fact that we are still the most immigrated-to country on Earth speaks to the international image of the United States. But political and strategic planning is taking place in a world where American ideals are not always aspired to in the same way as they were by some cultures in the latter half of the 20th century. The "selling" of what American-style liberties can do for countries is done in an age when our government talks of countries gaining freedom, peace, and prosperity by associating with the United States, but a torrent of information, opinions, and images that people receive from media here at home and abroad increasingly seems to cast doubt on this idea. This would be a concern even if we were assured of the political, military, and economic hegemony that the United States has enjoyed for several generations, let alone in an era where long-term trends point toward an increasingly multi-polar parity.

Take China, which is seen by many as the preeminent "country on the rise," yet on the RLDP–P trip, people from various countries, ethnicities, and social and ethnic strata consistently voiced displeasure with a Chinese presence that is often seen as one-sided, impersonal, and pecuniary. While the importance of material interests can never be overstated, neither can the importance of establishing relationships in Asia—between not only governments or organizations, but also between people. Growing Chinese power is increasingly capable of making things difficult for those who resist China's aims, so the United States needs to demonstrate the advantages of having relationships with our country more than ever if it wishes to pursue its interests.

The Example of Timor-Leste

The final place visited on the RLDP–P trip was Timor-Leste. It is a new country, having gained independence in 2002 after a long period of what many have called genocide, and having survived bouts of violence and an attempted revolution since then. Though small, Timor-Leste could be an opportunity to reinforce, publicly and loudly, the image of the United States as a role-model country and a friend—even if the direct material returns to us are few. Despite the difference in size, resources, and cultures between our two countries, surely a small, fledgling nation of 1.27 million people can strike a chord of solidarity in the American psyche. Timor-Leste has fought much larger forces than itself to assert its own fierce sense of independence and is by almost all international accounts one of the leading proponents of democracy in the region.

Robustly developing our existing ties with Timor-Leste, from a political to a culturally informed interpersonal level, could establish a relationship with the Timorese that stands on our direct actions, without the communicative "noise" of a thousand blogs, videos, broadcasts, and Facebook posts. The upside is that the United States can demonstrate it does not fit the narrative of only exploiting countries while

U.S. Air Force photo by TSgt Benjamin W. Stratton

Kathleen Fitzpatrick, U.S. Ambassador to the Democratic Republic of Timor-Leste, **addresses attendees of the Pacific Angel 2018 closing ceremonies at the Negri** Saran Kote Secondary School in Suai, Cova Lima Municipality, Southwest Timor-Leste, June 18, 2018.

paying lip service to freedom and liberty, but it can be a friend of any country that stands for democracy. Though Timor-Leste's small size might help minimize the down-side of such a venture, some will point out the myriad of financial, political, and military quagmires that could result from this. But what better way to directly advertise both the U.S. ideals and our commitment to them? This is some-thing we can champion better than others could regardless of the future economic or political situation. It's a chance to see if emphasizing an organized, deliberate, face-to-face, relationships-first approach can be a useful strategy for the United States in a century where the United States may not always be the clear-cut, best choice based on economics, politics, or even security.

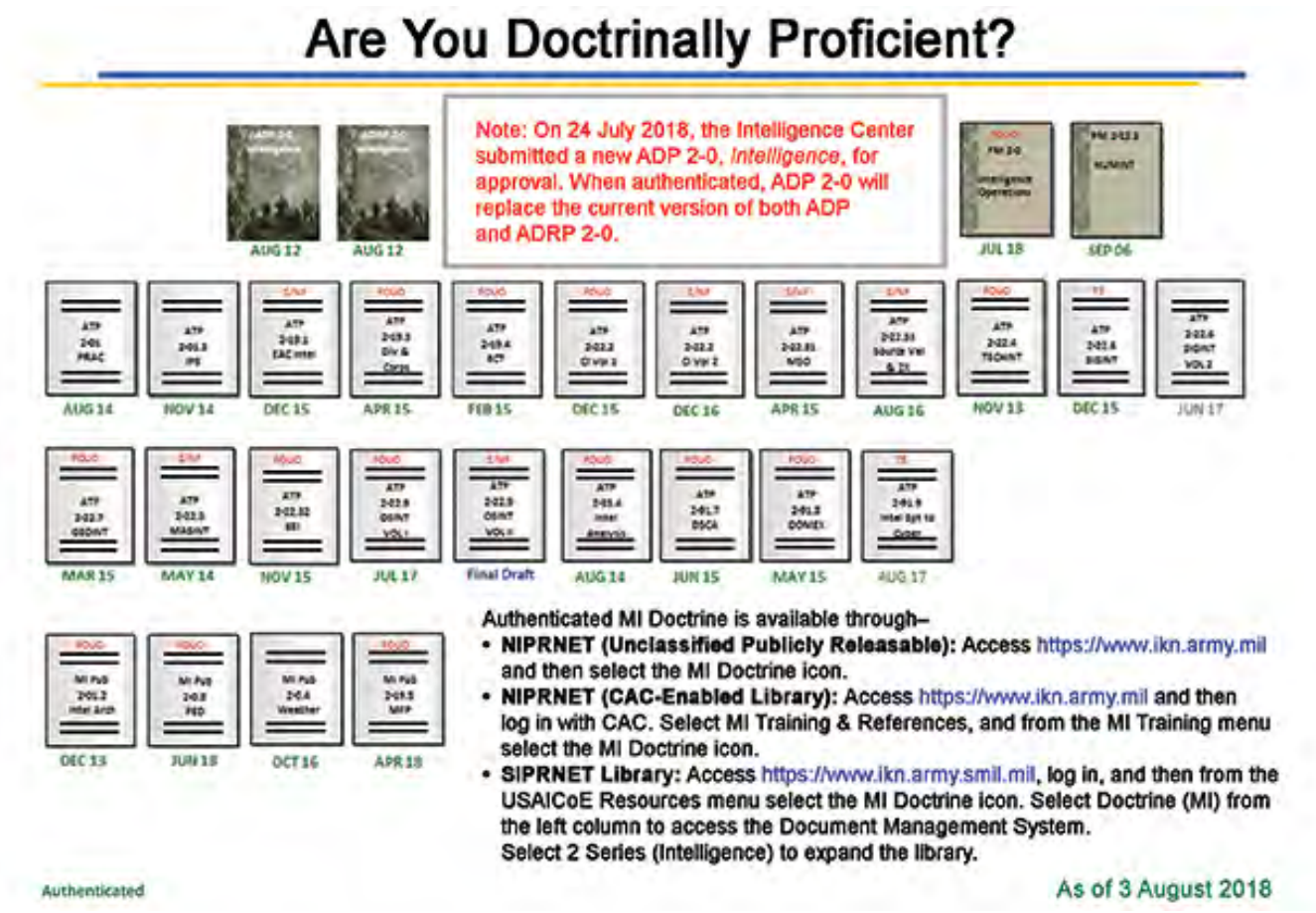
Endnotes

1. Joshua Taft, "USARPAC hosts Regional Leader Development Program," *Hawaii Army Weekly,* February 22, 2018, http://www.hawaiiarmyweekly.com/2018/02/22/usarpac-hosts-regional-leader-development-program/.

2. Richard Bush and Maeve Whelan-Wuest, "Order from Chaos: How Asians view America (and China)," *Brookings*, January 18, 2017, https://www.brookings.edu/blog/order-from-chaos/2017/01/18/how-asians-view-america-and-china/.

3. Abby Budiman and Dorothy Manevich, "Few see EU as world's top economic power despite its relative weight," *Pew Research Center*, August 9, 2017, http://www.pewresearch.org/fact-tank/2017/08/09/few-see-eu-as-worlds-top-economic-power-despite-its-relative-might/.

4. Jeff Cox, "Other nations view China more favorably than the U.S. survey shows," *CNBC*, 28 September 2017, https://www.cnbc.com/2017/09/28/other-nations-view-china-more-favorably-than-the-us-survey-shows.html.



Captain Bryan J. Nesbitt
2018 Recipient
Lieutenant General Sidney T. Weinstein Award
For Excellence in Military Intelligence

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

CPT Bryan J. Nesbitt was born and raised in Pittsburgh, Pennsylvania. He received a bachelor of arts in psychology with a minor in business administration from Wheeling Jesuit University in 2009. Following graduation, he entered Officer Candidate School, where he commissioned as a second lieutenant in the Military Intelligence (MI) Branch.

CPT Nesbitt started his career as a battalion assistant S-2 for the 40th Engineer Battalion, 170th Infantry Brigade Combat Team (IBCT). He deployed in support of Operation Enduring Freedom as a multi-sensor ground platoon leader for 502nd MI Company, 170th IBCT, in Regional Command-North, Afghanistan. Following his redeployment to Baumholder, Germany, the 170th IBCT inactivated, and in 2012, CPT Nesbitt reported to the 297th Ml Battalion, 513th Ml Brigade, located at Fort Gordon, Georgia. While serving as the Executive Officer for B Company, 297th Ml Battalion, he completed a 6-month deployment to Jordan in support of Operation Enduring Freedom.

Following his time in the 297th, CPT Nesbitt graduated from the MI Captain's Career Course at Fort Huachuca, Arizona. He then reported to the 201st Expeditionary MI Brigade at Joint Base Lewis-McChord, Washington (JBLM), where he served as the brigade assistant S-3 for 12 months. From April 2016 to November 2017, he served as the B Company Commander, 109th Expeditionary MI Battalion.

Upon assuming command of B Company, CPT Nesbitt established U.S. Army Forces Command's first home-station processing, exploitation, and dissemination (PED) mission. He oversaw the installation and operationalization of the network architecture and exploitation platforms required to support Operation Inherent Resolve from the JBLM Intelligence Operations Facility. This new capability for Army intelligence served as a proof of concept that drove a reorganization within expeditionary-military intelligence brigades Armywide. CPT Nesbitt then demonstrated the flexibility of his company by deploying an expeditionary PED element to the Republic of the Philippines in support of Operation Pacific Eagle. In addition to these critical real-world missions, CPT Nesbitt led his company to successfully execute nine major exercises.

In November 2017, he transitioned to the 1-2 Stryker Brigade Combat Team, 5-20 Infantry, to serve as a battalion S-2.

CPT Nesbitt's awards and decorations include the Meritorious Service Medal, Army Commendation Medal, Army Achievement Medal, Meritorious Unit Citation, National Defense Service Medal, Afghanistan Campaign Medal, Global War on Terrorism Expeditionary Meal, Global War on Terrorism Service Medal, Army Service Ribbon, Overseas Service Medal, and NATO Medal. His unit also received the BG Roy M. Strom Award for the best MI Company in the U.S. Army Forces Command for 2017.

Chief Warrant Officer 2 Jason LaPonsey
2018 Recipient
Chief Warrant Officer 5 Rex Williams Award
For Excellence in Military Intelligence

The MI Corps established the Chief Warrant Officer 5 Rex A. Williams Award in 2016 to recognize the outstanding achievements of a company grade warrant officer (WO1-CW2) within the MI community. This award is named in honor of an icon in MI, who spent his 31-year military career improving training, mentoring countless Soldiers, and helping define the foundations of intelligence analysis. CW5 Williams also served as the first Chief Warrant Officer of the MI Corps. He continued to serve the MI Corps as a Department of Army Civilian until his retirement from Federal service in 2017.

CW2 Jason LaPonsey enlisted in the U.S. Army as a non-communications interceptor analyst in 1996. He was appointed a warrant officer in November 2011 and awarded military occupational specialty 352N (signals intelligence [SIGINT] analysis technician) in May 2012.

CW2 LaPonsey currently serves as the SIGINT officer in charge (OIC) for the 25th Infantry Division. His other assignments include Resolute Support/U.S. Forces-Afghanistan SIGINT OIC in support of Operations Freedom's Sentinel and Resolute Support; 25th Infantry Division SIGINT Operations OIC; and Brigade SIGINT OIC, 2nd Stryker Brigade Combat Team, 25th Infantry Division. His other deployments include Camp Doha, Kuwait, with U.S. Army Central Command; multiple deployments to the Philippines in support of Operation Enduring Freedom-Philippines; and Camp Speicher, Iraq, in support of Operation Iraqi Freedom.

During his most recent deployment to Afghanistan, while serving as the SIGINT OIC at Headquarters, Resolute Support Mission, U.S. Forces-Afghanistan, CW2 LaPonsey synchronized SIGINT requirements and operations supporting special operations, conventional, coalition, and Afghan forces across the Combined Joint Operating Area-Afghanistan. He redesigned and rebuilt theater-wide tactical ground-based SIGINT capability at 11 enduring bases and spearheaded the integration of SIGINT capabilities into the enhanced targeting campaign, increasing threat reporting by 30 percent. These efforts provided greater fidelity on insurgent networks and resulted in the precision targeting of 27 Taliban-controlled narcotics facilities and the removal of more than $100 million of operational funding from Taliban control. During critical manning shortfalls, CW2 LaPonsey also served as SIGINT OIC for the Special Operations Joint Task Force-Afghanistan.

CW2 LaPonsey has a bachelor's degree in intelligence studies from American Military University. His awards include the Defense Meritorious Service Medal, Meritorious Service Medal, Army Commendation Medal, Joint Service Achievement Medal, Army Achievement Medal, Navy Achievement Medal, Joint Meritorious Unit Award, Army Good Conduct Medal, National Defense Service Medal with Star, Armed Forces Expeditionary Medal, Afghanistan Service Medal, Iraq Service Medal, Global War on Terrorism Expeditionary Medal, Global War on Terrorism Service Medal, NATO Medal, Military Outstanding Volunteer Service Medal, Gold German Armed Forces Proficiency Badge, Master Parachutist Badge, Air Assault Badge, Air Crewmember Badge, and Canadian and German Jump Wings. He is also a recipient of the Knowlton Award and a Sergeant Audie Murphy Club inductee.

Sergeant Calvin R. Christian
2018 Recipient
Command Sergeant Major Doug Russell Award
For Excellence in Military Intelligence

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

SGT Calvin R. Christian was born in Manama, Bahrain, in 1982, and he graduated high school in Colonia, New Jersey, in 2000. In March 2014, he enlisted in the U.S. Army as an all-source intelligence analyst (35F) and graduated from Basic Combat Training at Fort Sill, Oklahoma.

After completing Advanced Individual Training at Fort Huachuca, Arizona, SGT Christian served as a long-range artillery analyst with the 8th Army Headquarters and Headquarters Battalion in Yongsan, Korea. After completing the Basic Airborne School at Fort Benning, Georgia, he was assigned to the famed 1st Battalion, 504th Parachute Infantry Regiment, 1st Brigade Combat Team, 82nd Airborne Division, where he served as an intelligence analyst in the battalion's intelligence section. During this assignment, he served at the Joint Multinational Readiness Center in Hohenfels, Germany, as the future operations analyst during Operation Swift Response. In October 2016, he earned the rank of sergeant and was reassigned to Delta Company (Military Intelligence Company), 127th Airborne Engineer Battalion, as an all-source intelligence sergeant and team leader.

Shortly after reassignment to Delta Company, SGT Christian participated in the brigade culminating training exercise in preparation for combat operations. He deployed to Kandahar Airfield, Afghanistan, with the Combined Task Force Devil Strike Brave Hearts in support of Operation Freedom's Sentinel 17-18 from July 2017 to March 2018. He served in the Kandahar Intelligence Fusion Center as the lead analyst for the vehicle-borne improvised explosive device (VBIED) targeting team. He led the effort to interdict VBIEDs as they entered the Kandahar ground defense area and to identify key Taliban VBIED staging and support zones, resulting in the destruction of nearly 30 VBIEDs and VBIED facilities.

SGT Christian earned his bachelor's degree in finance in March 2017 from Maryland University College. Additionally, he graduated the United States Army Advanced Airborne School Jumpmaster Course in April 2017, distinguishing himself as an airborne leader. He is pursuing his master's degree in national security studies at American Military University.

SGT Christian's awards include the Army Commendation Medal, Army Achievement Medal, Good Conduct Medal, National Defense Service Medal, Global War on Terrorism Service Medal, Afghanistan Campaign Medal, Korean Defense Service Medal, Noncommissioned Officer Professional Development Ribbon, Army Service Ribbon, Overseas Service Ribbon, and NATO Medal. SGT Christian has also been awarded the Parachutist Badge and the Combat Action Badge, and his company received the MG Oliver W. Dillard Award as the best brigade combat team military intelligence company in the U.S. Army Forces Command for 2017.

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

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

PIN: 203757-000