

M Professional Bulletin

April-June 2021
PB 34-21-2

INTELLIGENCE WITHIN THE INFORMATION DIMENSION



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

Commanding General

MG Anthony R. Hale

Chief of Staff

COL Norman S. Lawrence

Commandant, Intelligence School

COL Christina A. Bembenek

Chief Warrant Officer, MI Corps

CW5 Aaron H. Anderson

Command Sergeant Major, MI Corps

CSM Warren K. Robinson

STAFF:

Editor

Tracey A. Remus

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

Associate Editor

Maria T. Eichmann

Design and Layout

Emma R. Morris

Jonathan S. Dinger

Cover Design

Emma R. Morris

Military Staff

CPT Michael J. Lapadot

CW4 Michael Janney

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

By Order of the Secretary of the Army

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

Official:



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

2123814

From the Editor

Over the past decade, technology has driven significant change for the print media, including professional military journals such as MIPB. Industry leaders are exploring new distribution channels for their publications through a process of constant evaluation and evolution. To ensure MIPB remains relevant and easily accessible to the military intelligence community, we believe it is time for us to modernize our publication. Initial information on this effort is available on page 7 of this issue.

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



Tracey A. Remus

Editor

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



Features

- 8 The Threat of Social Media: Operations in the Information Environment**
by Mr. Joshua Jackson and Mr. Rick Rodriguez
- 12 Truly Understanding the Adversary: Describing the Threat in the Information Space**
by COL Christina A. Bembenek
- 15 Spinning Victory: The Russian Approach to Information Warfare**
by SFC Sergei Volodin
- 22 Preparing for the Future of Cyberspace and Electromagnetic Activities Support to Corps and Below**
by MAJ Wallie G. Lacks
- 27 The Pathway to Multi-Domain Intelligence Proficiency: The I2CEWS Approach**
by MAJ Owen Ryckman and 1LT Erica Forktus
- 29 A Mathematical Probability of Success for Soviets in Cold War Confrontation**
by Lester W. Grau, Ph.D., and Mr. Clint Reach
- 36 The Vitality of Synchronized Intelligence Operations for a Division Support Area Command Post**
by CPT Julee R. Thomas
- 40 The Intelligence Warfighting Function in the Division Cavalry Concept**
by CPT Jonathan Guelzo
- 46 Russia's Military Police and the Syrian Campaign**
by Mr. Charles K. Bartles
- 51 344th Military Intelligence Battalion's Tactical Signals Intelligence Training Exercise**
by Mr. Brandon Allen, Mr. Brian Lemaster, CW4 Christopher Banks, and SFC LeeAnn Seitz
- 57 Deceivingly Decisive: U.S. Army Military Deception and Counterintelligence**
by 1LT Will Rector
- 63 1st Special Forces Command Has a Military Intelligence Battalion**
by LTC Sapriya Childs

DEPARTMENTS

- | | | |
|---------------------------|--------------------------------|---------------------------------|
| 2 Always Out Front | 5 Technical Perspective | 77 Futures Forum |
| 4 CSM Forum | 65 Doctrine Corner | 81 Moments in MI History |
| | 73 Lessons Learned | |

Inside back cover: Contact and Article Submission Information



Always Out Front

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



In order to counter the United States overwhelming military power, our peer adversaries and other threats are employing information through various means below the threshold of armed conflict. In many cases, these means are relatively inexpensive and disproportionately effective. Our adversaries seek to control the information environment through the spread of disinformation and misinformation and combine those efforts with nonlethal actions. This coordinated convergence of information activities influences a population's emotions, thoughts, and actions. This could jeopardize our posture across multiple theaters or U.S. interests. The Department of Defense, U.S. Army, and U.S. Army Training and Doctrine Command recognize these challenges and are taking action now while planning and building capabilities for the future.

This quarter's *Military Intelligence Professional Bulletin* (MIPB) will offer insight into how our adversaries treat the information environment as a battlespace and how we are adapting our formations to compete in that battlespace. COL Christina Bembenek's article, "Truly Understanding the Adversary," provides a succinct overview of how our main state rivals, Russia and China, are testing their abilities to influence the cognitive information space. Because of this, it is more critical than ever that intelligence professionals understand our adversaries' intent, processes, and methods to integrate information with operations.

In their book *LikeWar*, P. W. Singer and Emerson T. Brooking state that Russia, formerly part of the Soviet Union, was the first to study the "weaponization" of information. Citing Ben Nimmo, a British analyst of Russian information warfare and strategy, the authors identify four principles of Russian disinformation: dismiss the critic, distort the facts, distract from the main issue, and dismay the audience. To these "4 Ds," they add a fifth—




divide the target population.¹ In his article, "Spinning Victory," SFC Sergei Volodin provides an in-depth look into these concepts. "The objective of Russian psycho-informational activities," he writes, "is to gain a commanding level of influence of all nation-state domestic and international decision making through a systematic degradation or destruction of a nation's cognitive sovereignty." Through SFC Volodin's thorough analysis, we are able to understand how the Russian Federation has recently been able to target and employ weaponized narratives into other countries' cognitive space.

As intelligence professionals, we must analyze and describe relevant aspects of the information dimension, and as an inherent part of the operational environment, we must also drive offensive and defensive actions in the information domain at the appropriate echelons. For the future force, we must deliberately assess how we are structured and educated to compete in the information environment. However, across our force, leaders on the "information front lines" are spearheading efforts to maintain the information advantage. Some of those leaders have shared their experiences and lessons in this quarter's MIPB. MAJ Owen Ryckman discusses how his Multi-Domain Task Force military intelligence company broadens analysts' exposure to the information environment. MAJ Wallie Lacks offers observations of the current force structure, describes the three key layers of cyberspace, and discusses how intelligence professionals can arrange data to identify, characterize, and track enemy activity within cyberspace.

The importance of information to strategic competition and military operations is not new. However, the means of employing information and the severity of potential consequences within the information domain have changed significantly in the last 10 years. The information

dimension is changing rapidly with an acceleration in competition. Army intelligence is at the forefront of confronting these challenges. The Department of the Army G-2, U.S. Army Intelligence and Security Command, and U.S. Army Intelligence Center of Excellence are aggressively participating in a myriad of initiatives, programs, and actions involving the information dimension, including the

development of ADP 3-13, *Information*. We all have a responsibility to contribute to the solutions as these efforts progress. – Desert 6 

Endnote

1. P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Houghton Mifflin Harcourt, 2018).

Always Out Front!

Emerging Army Doctrine on Information

Introduction

The Army doctrine community is busy assessing its doctrine across many areas. One area involves reexamining the information dimension from a fundamental standpoint and the use of information from competition to conflict. The primary publications that will address the various aspects of information are FM 3-0, *Operations*, and ADP 3-13, *Information*. ADP 3-13 will provide fundamental doctrine on the information dimension. This article is a quick look at the basic information constructs within ADP 3-13.

Information Means Different Things

The writer's draft of ADP 3-13 is currently in development and will provide a foundation for thinking about information and the information dimension, as well as a framework for how Army forces, as part of a joint force, gain and maintain an information advantage. ADP 3-13 will describe an information advantage and explain how information advantage activities contribute to achieving positions of relative advantage and decision dominance.

Information means different things depending on context. In one sense, information is an element of national power that the U.S. Government employs in combination with diplomatic, military, and economic power to advance national interests. In another sense, information is a method of war as in the Russian construct of information warfare. Depending on context, information is a joint function integrated with command and control, intelligence, fires, movement and maneuver, protection, and sustainment to assist commanders in directing campaigns, operations, and activities. For Army forces, information is a contested dimension where both sides seek an advantage. This information advantage occurs when a force holds the initiative in terms of understanding, decision making, and influence on relevant actor behavior.


Information Advantage Activities

Commanders gain and maintain a relative information advantage by conducting information advantage activities. **Information advantage activities are the employment of capabilities to enable decision making, protect friendly information, inform domestic audiences, influence international audiences, and conduct information warfare.**¹ Commanders conduct information advantage activities using all available military capabilities integrated across the warfighting functions and synchronized through the operations process.

Information advantage activities consist of the core combination of tasks and sub-tasks conducted in a joint and combined arms approach. The first two tasks—enable decision making and protect friendly information—focus on outcomes internal to Army forces. The other three tasks—inform domestic audiences, influence international audiences, and conduct information warfare—focus on outcomes external to Army forces. Commanders and staffs coordinate and synchronize these five core tasks throughout the operations process to attempt to create and exploit an information advantage.

Information advantage tasks help focus the employment of capabilities resident in the various warfighting functions. An information advantage task may involve the employment of capabilities from all, multiple, or a single warfighting function depending upon the intended effect. The more capabilities brought to bear in a combined arms approach simultaneously, the more powerful the effects during the operation.

Conclusion

The development of ADP 3-13 will drive changes to many other Army doctrinal publications. It is critical that the Army Military Intelligence Corps maintain awareness and stay knowledgeable of these changes in order to be successful during multi-domain operations. Obviously, the intelligence warfighting function plays an integral role in almost every aspect of the information dimension. In the next issue of the *Military Intelligence Professional Bulletin*, we will discuss initial thoughts on those roles and potential new requirements for the intelligence warfighting function within the information dimension. 

Endnote

1. This definition is from the current writer's draft of Army Doctrine Publication 3-13, *Information*.



CSM Forum

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



Movies and television shows have highlighted rifles, pistols, tanks, demolitions, and artillery as the key weapon systems on the battlefield to gain the advantage over the enemy. Although these are still very important, they have been joined by another “system”—*information*—in the form of cyber warfare, electromagnetic warfare, information operations, psychological operations, signals intelligence, network operations, spectrum management, and space operations. Information has become a critical component of modern warfare that affects the Army’s ability to obtain and maintain the *information advantage*.

The world has evolved both technologically and socially, and continues to do so at a very fast pace. As a result, information is being operationalized throughout society, including the military, with a goal to inform, misinform, and influence audiences through direct and indirect messaging. When we watch television shows, look at social media, or listen to the radio or a podcast, whether we like it or not, what we see or hear affects our thoughts and actions.

So what is information advantage and why is it important to the Army? Simply stated, “Gaining and maintaining the initiative during competition, crisis, and armed conflict largely depends on a commander’s ability to attain an information advantage.”¹ With this in mind, it may be beneficial to consider information from an offensive/defensive perspective. We all know about lethal effects on the battlefield, but nonlethal effects can be just as important if properly planned, coordinated, and executed, especially if synchronized with other operations. Intelligence supports planning by providing understanding of the threat’s information element—those aspects of the information environment that influence or are influenced by the threat.

Understanding the battlefield capabilities and forecasting operations for both friendly and enemy forces will be key to maintaining an information advantage. For example, we have an information advantage when commanders are able to rapidly communicate orders on the battlefield and Soldiers can share information using our battlefield systems



to synchronize efforts and provide up-to-date situational awareness. We can maintain this advantage if we know both our and the threat’s communication capabilities on the battlefield. This includes asking questions like, what are we communicating, is the information classified, and are there any communication barriers or limitations. We must also ask how friendly, enemy, and civilian assets on the battlefield communicate, and whether there are trends with regard to the type of communication and time. However, when we find ourselves in a denied, intermittent, or limited communications environment, where communications are disrupted throughout the battlespace, we may no longer have an information advantage.

Training our Soldiers to consider the information advantage in all operations is important. This might be as simple as changing passwords on our networks and systems or updating software patches. It could also mean trying to learn what information is passed in a battlespace and then relaying it to higher headquarters in a SPOT/SALUTE report. It may also be through operations security. We need to communicate to our Soldiers the reasons for protecting information from an enemy that exploits social media to influence military and civilian populations. They must also understand the need to be skeptical of the information they see on social media and other sources, because if not, that gives the enemy the advantage.

Information advantage brings a new aspect to the battlefield. We must include it in our training so that Soldiers understand what they can do to contribute to decision dominance over the adversary. ✨

Endnote

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

Always Out Front!

Technical Perspective

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



As we gaze into the future and examine what large-scale combat operations might look like in a multi-domain environment, one thing is clear—achieving overmatch and dominating in the information space will be critical. Within intelligence circles, we have used the term *information dominance* for many years, but more recently, the phrase *information advantage* has entered the Army lexicon. While discussing information advantage in September 2020, LTG Stephen Fogarty, Commanding General, U.S. Army Cyber Command, indicated the intent “is for future commanders to be able to see what’s happening ‘in real time—not just the physical effects [e.g., weapons fire], and the physical space within the spectrum [i.e., radio and radar signals], but then also that information space, where ideas are being bounced around like crazy.’”¹

Inside the information space, peer and near-peer competitors will continue to operate void of restrictive policies. In recent years, several nation-states have proven they are capable, and in some cases adept, at combining physical and information-based effects to achieve operational and strategic ends. “Russian analysts conducting an early after-action report (AAR) of the Russian deployment to Syria in January 2016 concluded that Russia must sharply increase its attention to the information space to enable successful kinetic operations, demonstrating an immediate recognition of this priority after only 3 months of operations.”² Our ability to counter and disaggregate these adversary capabilities will be critical in creating windows of opportunity and ensuring freedom of movement in a large-scale combat operations fight.

From an intelligence perspective, ongoing modernization efforts within the Military Intelligence Corps will continue to enhance our sensing and analytic capabilities, significantly contributing to the establishment of information advantage. The intent is that information advantage will ultimately lead to “decision dominance,” giving U.S. commanders greater flexibility to act in both competition and conflict. Decision dominance “is a desired state in which a commander can sense, understand, decide and act faster and more effectively than an adversary.”³ By establish-



ing decision dominance, we increase efficiency and situational understanding, shorten the “kill-web,” and allow the prosecution of more targets across multiple domains.

Achieving decision dominance will ultimately require changes in the realms of structure, training, and equipping across multiple formations. In one example of this, as part of the Multi-Domain Task Force, the Army “created a multi-disciplinary battalion for Intelligence, Information, Cyber, Electronic Warfare, & Space (I2CEWS) and merged headquarters staff sections for space, command & control, and information.”⁴ The intent of the I2CEWS battalion is to fuse multiple data feeds to create joint situational awareness in support of kinetic and non-kinetic operations, as well as create offensive and defensive cyberspace effects and employ electromagnetic warfare and space capabilities against adversary forces. Clearly, having dominance of the information space is vital to shaping and winning future conflicts. Having said that, without a doubt, these concepts will continue to evolve as thinking matures in relation to how the U.S. Army executes multi-domain operations.

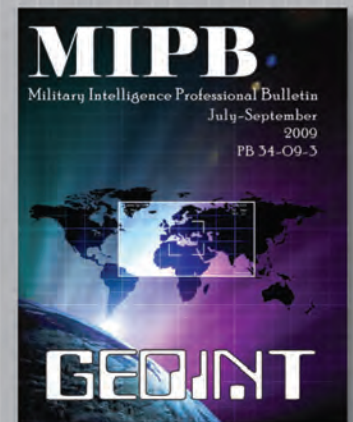
As always, I would like to thank you and your families for your daily sacrifice, selfless service, and contributions to the Army in defense of our Nation. I continue to wish you good health and safety as we continue to work through the impacts of this ongoing pandemic and engage in operations across the globe. ✨

Endnotes

1. Sydney J. Freedberg Jr., “Army Wrestles with Information Advantage,” *Breaking Defense*, September 29, 2020, <https://breakingdefense.com/2020/09/army-wrestles-with-information-advantage/>.
2. Mason Clark, *Russian Hybrid Warfare: Military Learning and the Future of War Series* (Washington, DC: Institute for the Study of War, September 2020), 21–22, <http://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf>.
3. Mark Pomerleau, “Out: ‘information warfare.’ In: ‘information advantage,’” *C4ISRNET*, September 29, 2020, <https://www.c4isrnet.com/information-warfare/2020/09/29/out-information-warfare-in-information-advantage/>.
4. Freedberg, “Information Advantage.”

Always Out Front! and Army Strong!

Are You Looking for Past Issues of MIPB?



They can all be found in MIPB's archive. Even as MIPB modernizes to take advantage of current technology, the archive will not go away. It can be accessed at <https://www.ikn.army.mil/apps/MIPBW/Home/Archive>.



Modernizing MIPB

Coming Soon

We are excited to modernize the *Military Intelligence Professional Bulletin* (MIPB)! Our goal is to improve the distribution of MIPB by leveraging current technology and delivering MIPB across the various mediums to Soldiers and intelligence professionals. We are currently assessing and planning the project and because we value our readership, your input will be part of the process. Some aspects of the modernization will be implemented in the first quarter of FY 2022.

Some of the key proposals include:

- Establishing a new website with new capabilities on LandWarNet.
- Posting the majority of MIPB articles online.
- Advertising MIPB across multiple social media outlets.
- Replacing long quarterly issues of MIPB with two or three special issues a year.
- Revising our dissemination model.

Future Article Focus Areas

- *Targeting and Intelligence*—suggested submission date 17 December 2021.
- *Army Intelligence and Modernization*—suggested submission date 18 March 2022.
- *Intelligence Training*—suggested submission date 18 August 2022.

You do not need to write articles on these specific topics. We consider and publish articles on a variety of subjects.

You may contact us by sending an email to:
usarmy.huachuca.icoe.mbx.mipb@mail.mil

Our article submission guidelines are located at: <https://www.ikn.army.mil/apps/MIPBW/Home/ArticleSubmission>

We will provide you with another update in the last quarterly issue of MIPB (July–September 2021), *Theater Intelligence Operations*, projected to publish in October 2021.



Federal civilian employees and Service members must be cautious of information-related activity on social media.

The Threat of Social Media: Operations in the Information Environment

by Mr. Joshua Jackson and Mr. Rick Rodriguez

Introduction

The U.S. Army's brigade combat team had not yet concluded its final rehearsal for an attack against enemy forces that were dug in just across the international boundary, when amateur bloggers released video footage of rocket strikes in a suburb near the unit's support area. Local news and social media posts quickly confirmed that the attack claimed 32 civilian lives and wounded more than 83 others, many of them women and children. No group claimed responsibility, but social media sites presented altered pictures and false narratives of U.S. Soldiers who were actually attempting to render aid, placing blame on U.S. forces. This rapid and unpredictable development quickly led to unrest and

insecurities in the brigade's rear area, which the unit had to stabilize before committing its combat forces to the attack—the attack was delayed.

While this incident is one of many replicated at Army combat training centers, it is a representation of the significant reality "information" has on military operations. In the real world, just last year, eastern adversaries disrupted United States training in Poland with alarming social media posts stating that a member of 1st Armored Division had allegedly killed a Polish soldier, had stolen a car, and was on the run. The posts even referenced the Soldier's unit, which was in the country at the time, and used his real photos.¹

Information Environment

For information operations to be effective, commanders' and their staffs' visualization of the area of operations must be expanded to include the information environment.² JP 3-13, *Information Operations*, defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."³ Numerous military information-related efforts/capabilities contribute to the information environment, including command, control, communications, computers, intelligence, surveillance, and reconnaissance systems; electromagnetic warfare; cyberspace operations; military deception; military information support operations; operations security; special technical operations; public affairs of- fice; and psychological operations, to name just a few.

The end state for most information engagements is to affect the decision making and behavior of adversaries and

designated others to gain an advantage across the range of military operations.⁴ Many of these engagements occur not directly with red (threat) on blue (friendly) but in the gray (civil) space, especially at the division and above echelons, which encompass social media platforms such as Facebook and Twitter. The collection, manipulation, and dissemination of publicly available information captured across social media and digital domains can accomplish adversarial objectives of influencing the operational environment; it can also diminish civilian and political support for current and future military operations. Future threats contend aggressively in the information environment throughout the entire competition continuum, seeking to deny support from civilian, political, and military audiences.⁵

Training for Information Engagements

To train for such engagements, the opposing forces (OPFOR) at all combat training centers have permissions to

The composite image consists of three main parts. The top left is a news article titled "A 24 Hour ceasefire between collapse after a spat" with a sub-headline "IN ANTICIPATION OF A BROKEN CEASEFIRE IN THE REPUBLIC OF TORBIA, IDPS COLLECT BELONGINGS". It features a photo of a pile of belongings and text about a temporary ceasefire in Torbia. The top right shows two Facebook posts from "Watcher_Unknown" dated July 17, 2020, reporting on deaths and US artillery rounds in the Kaaawa area. The bottom right is a poster titled "EXPLOSIVE WEAPONS The use of explosive weapons in populated areas - it is time to act" with a "KEY FACTS" section stating that between 2011 and 2015, nearly 108,325 persons were reported dead or injured globally due to the use of explosive weapons, and that 77% of those casualties were civilians.

A 24 Hour ceasefire between collapse after a spat

IN ANTICIPATION OF A BROKEN CEASEFIRE IN THE REPUBLIC OF TORBIA, IDPS COLLECT BELONGINGS

Many deaths reported. Destroyed homes and roads in the Kaaawa area. Take cover and stay safe!!! #FreeInformation

Many deaths reported. Destroyed homes and roads in the Kaaawa area. Take cover and stay safe!!! #FreeInformation

Reports are coming in from Kaaawa that state that US artillery rounds aimed at DPRT forces have missed and are hitting civilians!

EXPLOSIVE WEAPONS

The use of explosive weapons in populated areas - it is time to act

KEY FACTS²¹

Between 2011 and 2015, nearly 108,325 persons were reported dead or injured globally due to the use of explosive weapons.

- 77% of those casualties were civilians
- When explosive weapons were used in populated areas, more than 90% of the identified victims were children.

These images are fictitious training scenario examples developed for and contained within the Information Operations Network for training purposes only.

access, obtain, and use publicly available information about rotational units to help them plan and execute their OPFOR mission. With some caveats, OPFOR Soldiers may view publicly available information posted to the internet, including social networking sites, installation newspaper websites, blogs, and any form of social media not requiring a login or the creation of a username and password. This information may then be analyzed to collect order of battle and other critical unit metrics to determine and assess the rotational unit's level of training, morale, strength, and deployment timeline,⁶ while also providing the training unit commander with feedback about their operations security vulnerability within the information environment.

At a recent home-station training exercise, a brigade combat team conducted decisive action operations in a live, virtual, and constructive environment against a multitude of threats. One of the commander's training objectives was to dominate the information environment, at echelon. To replicate the competitive information environment on the internet, the unit used the Information Operations Network, which is a U.S. Army Training and Doctrine Command (TRADOC)—developed government off-the-shelf system for replicating immersive aspects of the worldwide web, especially social media. Information Operations Network content is housed on closed intranets and accessed via the web. Content is unique to each exercise or event and allows the training audience to search web material and social media content that matches the scenario and meets training needs.

During the brigade's exercise, scenario developers, OPFOR elements, and intelligence subject matter experts used the Information Operations Network to replicate the effects that would naturally occur in the operational environment. The Information Operations Network reinforced intelligence message traffic while correlating network linkages developed through human intelligence reporting and patterns of life observed on social media. The Information Operations Network was also used to identify friendly and adversary



A TRADOC G-2 Information Operations Network training scenario with the 25th Infantry Division.

locations, provide real-time indicators and warnings, and confirm target locations and battle damage assessments via social networking sites and microblogging services.

Additionally, the Information Operations Network allowed analysts (not just intelligence analysts) to monitor sentiments and actions of the local populace and potential OPFOR elements based on tweets and social media posts. Conversely, the OPFOR capitalized on information about the training unit to conduct hasty attacks and long-range fire missions. The OPFOR also developed a robust anti-U.S. campaign focused on disrupting military movements and operations by creating chaos while blaming attacks and events on the brigade. Deliberate deception stories inundated the internet, showing U.S. forces breaking the rules of engagement by shooting into buildings falsely identified as schools or community centers. As misinformation increased throughout the exercise without appropriate training-unit responses, their area of operation further destabilized, undermining their ability to maintain stability operations as the third pillar to decisive actions (simultaneous offense, defense, and stability operations).

At the combat training centers, exercise developers take the Information Operations Network to even more complex

levels by introducing specialized training units to the surface (or white) web and deep web. This includes replicating dark web/net domains, which consists of underground café chat rooms (for criminal and adversarial irregular forces networks), as well as a black-market interface, from which adversarial networks can buy, sell, and trade nefarious items based on the scenario.

During exercise execution, Operations Group planners develop daily scenario “normal” internet content (news stories, videos, and social media posts) and place heavy emphasis on dynamic scripting that is based on exercise-driven outcomes and robust adversarial social media attacks/rhetoric, all delivered through microblogging services, social networking sites, and adversarial news outlets.


To better prepare, some training-unit best practices include having designated personnel monitor the information environment continuously, proactively posting information ahead of an exercise to establish context of the operational environment, and anticipating and rapidly countering misinformation that may affect the unit’s mission. Additionally, Soldiers must take personal responsibility to keep their information safe and assist in detecting and countering misinformation. U.S. forces must be prepared to operate effectively in the complex, dynamic operational environment created by the ubiquitous nature of the information environment in which local incidents can have global effects.

Learn More about the TRADOC G-2 Operational Environment Center

The Operational Environment Center (OEC) supports the creation of a complex, tailorable operational environment for training, education, and leader development, using global data and innovative technologies to enable readiness. The OEC’s Support Division collaborates closely with the operational units, mission training complexes, Global Simulation Center, and combat training centers to help provide focused and scalable exercise design and expertise, share operational environment-derived lessons, and present OPFOR training and support to develop tough, realistic, and complex multi-echelon training.

In addition to the Information Operations Network and exercise design support, the OEC captures supported ex-

ercise data into comprehensive exercise support packages and posts them to the Exercise Support Application, a web-based repository where users can download exercise material for reuse or request additional OEC support. The TRADOC G-2 OEC Application and Service Hub, which houses the Information Operations Network, Exercise Support Application, and Operational Environment Data Integration Network, the authoritative source for all decisive action training environment operational environments, is located at <https://oedata.army.mil>.

To learn more about the TRADOC G-2 training tools and capabilities, contact the authors or the OEC at usarmy.jble.tradoc.list.tboc-operations@mail.mil or call (757) 878-9564/9503/9696. The TRADOC G-2 hosts in-person tools training sessions at Fort Eustis, Virginia, can travel to meet your organization’s needs, or can conduct virtual or telephonic training. Training includes more than the tools listed in this article. More information is available at <https://oe.tradoc.army.mil/operational-environment-center/>. “Victory Starts Here!” 

Endnotes

1. Gina Harkins, “Fake News Is Wreaking Havoc on the Battlefield. Here’s What the Military’s Doing About It,” *Military.com*, 16 August 2020, <https://www.military.com/daily-news/2020/08/16/fake-news-wreaking-havoc-battlefield-heres-what-militarys-doing-about-it.html>.
2. Robert Cordray III and Marc J. Romanych, “Mapping the Information Environment,” *Joint Information Operations Center* (Summer 2005): 7–10, <https://www.quantico.marines.mil/Portals/147/Docs/MCIOCIORecruiting/MappingtheInformationEnvironmentIOSPHERESummer2005.pdf>.
3. Office of the Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Information Operations* (Washington, DC: The Joint Staff, 27 November 2012, incorporating change 1, 20 November 2014), I-1.
4. Department of Defense, *Strategy for Operations in the Information Environment* (June 2016).
5. Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-3-8, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045* (Fort Eustis, VA: TRADOC, 6 December 2018).
6. U.S. Army Forces Command memorandum, 10 April 2018; and 7th Army Training Command memorandum, 25 June 2018.

Mr. Joshua Jackson is a U.S. Army Veteran who continues to serve the Army as a civil servant within the U.S. Army Training and Doctrine Command (TRADOC) G-2. In his current capacity, he supports the Army’s program for replicating the dynamic complexities of the operational environment within training, education, and leader development.

Mr. Rick Rodriguez is a training specialist assigned to the U.S. Army TRADOC G-2 Operational Environment Support Division. He is a retired U.S. Army intelligence officer with 22 years of service, multiple deployments, and experience in a variety of government contractor positions at the U.S. Army Intelligence Center of Excellence.

Truly Understanding the Adversary: Describing the Threat in the Information Space

Colonel Christina A. Bembenek

Analysis Denial Psyops
Cyberspace Jamming Data Spoofing
Social Media Disinformation Advantage
Competitive Degradation Disturbance Technology
Data Overloading Mining
Tactical Communication Misleading Noise
Propaganda Disinformation

Introduction

Imagine sending the 82nd Airborne Division on a no-notice deployment to Europe as Russian troops make an initial incursion into the Suwalki gap. The division lands in darkness at the staging airfield, but the host-nation government, a close ally, refuses to allow the Soldiers to disembark. Local media has reported credible information that American forces are preparing to arrest government leaders so that those forces can use the entire country as a staging area for a wider conflict. Social media, news stations, and radio broadcasts are all carrying the same narrative.

How could rational leaders in an allied nation believe the U.S. military was there to stage a coup? Unfortunately, this is not an imaginary scenario, and it has already happened in the United States—in 2015, Russian intelligence services engineered a conspiracy around the United States military exercise Jade Helm, which caused the governor of Texas to send the Texas State Guard to observe the exercise just in case the story was true.¹ According to Michael Hayden, retired Air Force general and former director of the Central Intelligence Agency and National Security Agency (NSA), Russia used Jade Helm, to test its ability to influence the cognitive information space by co-opting a narrative found in the fringes of American media and using bots, social media influencers, and fake personas to amplify the story.²

In order to prevail in conflict, the military must train to compete in the cognitive information space now, which requires a more nuanced understanding of how the two greatest challengers, Russia and China, operate in this space.

Manipulating the Information

Russia has provided both clear doctrine and several real-world test cases exemplifying its proficiency in informa-

tion operations. In his March 2017 speech at the Russian Academy of Military Sciences, Chief of the General Staff Valery Gerasimov outlined an operational concept that emphasized the “extensive employment of political, economic, diplomatic, information, and other nonmilitary measures” in confronting the threat from the United States and the North Atlantic Treaty Organization (NATO).³ Understanding the underpinnings of this operational concept and how it merges Russia’s military capabilities with gray zone operations, particularly in the information space, is critical for the United States to compete in this space.

President Vladimir Putin believes Russia is in an ongoing conflict with the West, and his ultimate goal is to restore Russia’s position as a great power and world civilization.⁴ This includes—

- ◆ Returning to a multipolar world.
- ◆ Ensuring Russian primacy in the post-Soviet spaces.
- ◆ Opposing NATO and all transatlantic institutions.
- ◆ Forming a closer partnership with China.⁵

As a former KGB officer, Putin views information as a key component of his strategy, and an element of risk management, to be employed in concert with military operations or when hard power applications are not suitable. According to Fiona Hill, former senior director for European and Russian affairs on the National Security Council, Putin focuses most of his efforts on manipulating information to shape a particular perception of himself and Russia. One of the reasons he granted asylum to Edward Snowden, the NSA contractor who provided reams of sensitive intelligence to WikiLeaks, was because it allowed him to present himself as a protector of free speech and information transparency.⁶

The Example of Crimea and Disinformation

Russia's 2014 annexation of Crimea, an autonomous republic within Ukraine, offers a rich example of its effective use of information operations in concert with military operations. Following the overthrow of the Ukrainian government amidst widespread protests, Russian operatives introduced further uncertainty and confusion into the local populace by flooding the media with false narratives and conspiracy theories about the interim Ukrainian government and its military forces. Putin capitalized on this environment of mistrust to move Russian troops into Crimea to "protect" its citizens. The Russian government crafted a narrative claiming Crimea was Russian territory in every respect—historically, linguistically, and culturally—and used media, theatrics, and military troops to bring the story to life. When the occupation was complete, Putin hosted a televised extravaganza in the Crimea that re-created the events leading up to the annexation and mixed in masonic symbols, swastikas, and dollar signs to denigrate the West while also featuring old Soviet symbols and patriotic songs to hearken back to the historic greatness of the Soviet Union. To the international community, Putin transmitted the message that Crimea is part of the *Russkiy mir* (Russian world) by assembling the Russian Duma in Yalta, the site of the 1945 great power conference that divided up Europe following World War II, and attesting that Russian society would consolidate and return to "hard work for Russia and in the name of Russia."⁷

Russia has been dominating the information space every day since Crimea and honing the tactics that it will undoubtedly use against the United States in any future conflict. According to a report by the Global Engagement Center, Russia has created an ecosystem of disinformation and propaganda that magnifies the effectiveness of its "information confrontation" strategy.⁸ The Russian government issues key themes that are echoed across state-funded media like RT and Sputnik, "verified" in Russian-aligned think tanks like Global Research, and amplified across social media by networks of bots and false personas. More perniciously, the Russians have become adept at co-opting and spreading misinformation and false narratives generated by domestic actors in a country, thus making it appear that the disinformation is genuine and coming from inside the state. As they exploit partisan divides, the Russians are not concerned with creating one consistent version of the "truth" but rather seek to amplify all sides of an issue and create what the RAND Corporation labeled a "firehose of falsehood" that spreads confusion, overwhelms the information space, and further divides society.⁹

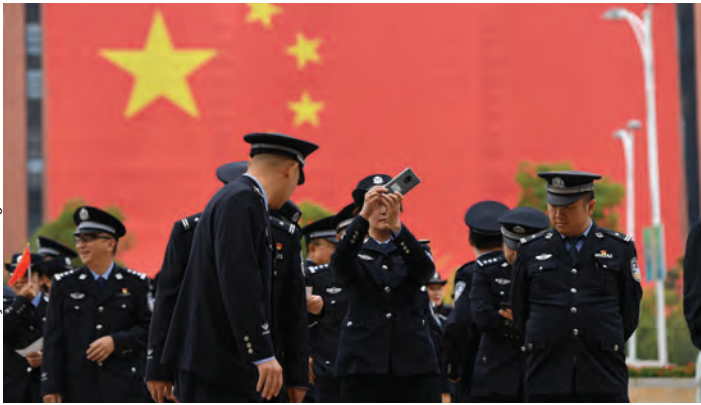
Information Confrontation

"Information Confrontation" is the term used in Russian strategic and military circles to describe their approach to the use of information in both peacetime and conflict. There is also a rich public record of the use of "Active Measures" to describe long-standing Russian political warfare methods that utilize disinformation and propaganda as a core tool.¹⁰

The Chinese Strategy

The Chinese are equally engaged in the information space, and though President Xi Jinping shares the same nationalist goal as President Putin—to return China to its rightful place at the center of the world—Xi has a different strategy. Rather than create confusion and disunity in the information space, the Confucius-based Chinese state seeks to build a unified, favorable opinion of China. Although China has not as explicitly paired information operations with military action, as Russia did in Crimea, information plays a key critical role in its military doctrine. The 2019 Chinese National Defense white paper states, "war is evolving in form towards informationized warfare, and intelligent warfare is on the horizon."¹¹ China's Ministry of National Defense aims to increase transparency with the Chinese population through monthly press conferences on military matters and its Information Office's Weibo and WeChat accounts, which have more than 6 million followers. The Defense Intelligence Agency labels "information warfare" as a core People's Liberation Army (PLA) strength, and PLA doctrine identifies "information dominance" as a prerequisite for victory in modern war.¹² Any future Chinese military operation will feature a robust information campaign conducted across multiple platforms.

Chinese influence in the cognitive information space is a sleeping giant. The Chinese Communist Party (CCP) runs a sophisticated propaganda model. It has created a diverse, sprawling information infrastructure to manipulate information and disseminate its preferred narratives both at home and abroad. China's Central Propaganda Department, established in 1924, penetrates every channel of mass communication in China, including the arts, social media, and print publications.¹³ Xinhua, one of the largest news agencies in the world, regularly pays to insert *China Daily* articles into international newspapers; Chinese language publications in diasporas also echo and amplify CCP narratives. The CCP operates on both domestic and international social media networks, posting messages tailored to an international audience on YouTube, Twitter, and Facebook and a domestic message on Weibo and WeChat. The CCP also



Chinese officials are taking to Twitter and other social media platforms to respond to criticism of China or the ruling Communist Party.

leverages in-person networks, including business and academic groups, to amplify its narratives that orchestrate local influence campaigns across the globe. China has also conducted covert influence operations online, targeting Western audiences with fake social media personas and using high-volume bot accounts to amplify controversial content.¹⁴ Considering that there are more than 1.3 billion Chinese native speakers compared to 379 million native English speakers,¹⁵ the potential for China to spread authentic-sounding messaging to Chinese speakers across the globe is enormous. With a ready network of Chinese-speaking humans, constructed personas, media outlets, and bots, China is a formidable competitor in the information space.

Conclusion

The *U.S. Army in Multi-Domain Operations 2028* describes Russia and China as information-based states and highlights their sophisticated information warfare capabilities, but it only scratches the surface of the complexity of their information ecosystem. Intelligence doctrine does not yet exist to support modern operations in the cognitive information space, but this is where the competition will take shape. In order to accurately describe the information ecosystem, as well as its effect on both domestic and international audiences, and to recommend operational counters, military intelligence agencies will need to expand their normal partnerships, work to expand their authorities, and get comfortable operating and communicating at the unclassified level. The Active Measures Working Group, an effective Cold War interagency team, offers one possible model for how military intelligence can contribute in both competition and conflict in the information space. Regardless of the strategy the military pursues, it is critical that we start competing

now because when competition turns to conflict, there is no time to build credibility, communications channels, or trusted partnerships. ✨

Endnotes

1. Molly McKew, "Current Information Operation Topics: US Intelligence Is Finally Figuring Out How To Communicate With The American Public On Threats In Our Information Domain, And We Should All Pay Attention," *Stand Up Republic* (blog), July 30, 2020, <https://standuprepublic.com/current-information-operation-topics-us-intelligence-is-finally-figuring-out-how-to-communicate-with-the-american-public-on-threats-in-our-information-domain-and-we-should-all-pay-attention/>.
2. Cassandra Pollock and Alex Samuels, "Hysteria over Jade Helm exercise in Texas was fueled by Russians, former CIA director says," *Texas Tribune*, May 3, 2018, <https://www.texastribune.org/2018/05/03/hysteria-over-jade-helm-exercise-texas-was-fueled-russians-former-cia-/>.
3. Harold Orenstein, trans., "Contemporary Warfare and Current Issues for the Defense of the Country," *Military Review* 97, no. 6 (November–December 2017): 23, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2017/>.
4. Fiona Hill and Clifford G. Gaddy, *Mr. Putin: Operative in the Kremlin* (Washington, DC: Brookings Institution, 2013), 324.
5. Eugene Rumer, "The Continuation of Politics," *The Primakov (Not Gerasimov) Doctrine in Action* (Washington, DC: Carnegie Endowment for International Peace, 2019), <https://www.jstor.org/stable/resrep20980.5>.
6. Hill and Gaddy, *Operative in the Kremlin*, 422.
7. *Ibid.*, 458.
8. Global Engagement Center, *Pillars of Russia's Disinformation and Propaganda Ecosystem* (U.S. State Department, August 2020).
9. Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," RAND Corporation, 2016, <https://doi.org/10.7249/PE198>.
10. Global Engagement Center, *Pillars of Russia's Disinformation*, 5.
11. The State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (Beijing: Foreign Languages Press, July 2019), 6, <http://www.xinhuanet.com/english/download/whitepaperonnationaldefenseinnewera.doc>.
12. Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (November 2018), 17.
13. Renée DiResta, Carly Miller, Vanessa Molter, John Pomfret, and Glenn Tiffert, *Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives* (Stanford Cyber Policy Center, July 21, 2020), 9.
14. *Ibid.*, 27.
15. James Lane, "The 10 Most Spoken Languages In The World," *Babbel*, September 6, 2019, <https://www.babbel.com/en/magazine/the-10-most-spoken-languages-in-the-world>.

COL Christina Bembeneck is the Commandant for the U.S. Army Intelligence School at Fort Huachuca, AZ. She previously has served as the 82nd Airborne Division G-2 and in multiple intelligence positions at the tactical, operational, and strategic levels. She recently completed an Army War College fellowship at Columbia University where her research focused on the impacts of disinformation on the military and society.

Spinning Victory: The Russian Approach to Information Warfare



by Sergeant First Class Sergei Volodin

Introduction

The modern interconnected information environment and the nuclear-restrained competition between global actors have changed the position of armed conflict within the realm of international relations. This evolution of war has given rise to new conflict formats, leading to the emergence of military-political objectives, in which a successful resolution of a conflict no longer solely depends on a decisive military victory but relies on perceived optics and the impact on the political narratives in regional and global arenas. As information is a primary tool of politics, its effect on conflict resolution has become increasingly more direct. This new dynamic was demonstrated in Afghanistan, Iraq, Ukraine, and Syria, where the underlying conflict actors cannot be decisively affected by military action but instead fight through the informational and political outcomes of regional conflicts.¹

According to general military thought in the Russian Federation, nations are never at peace, but rather transition between preparing for and waging war.² This approach

to international policy adds an adversarial character to the use of any instrument of national power. In effect, it weaponizes information, and through recent technological advancements, it gives an actor the ability to focus information effects to support tactical operations directly during armed conflict. Instead of full-scale military conflicts reminiscent of World Wars I and II, armed confrontation has become part of a larger campaign that integrates political, diplomatic, and economic campaigns, which allow governments to achieve their global political objectives.³ This focused and deliberate use of weaponized information results in the emergence of a “hidden war” that is continuously waged in the background of the global cognitive space.⁴ As a result, this perpetual informational conflict has created a new battleground of ideas and narratives in an ill-defined, largely uncharted global cognitive domain that has a reciprocal relationship with the other domains. This increasing political component of warfare also creates an increasing demand for decision makers and warfighters to accurately understand the operational environment, develop and

employ effective strategies, and accurately assess the impact of military activities in the information space.

Theoretical Approach

The weaponization of information and the military-political dynamic of warfare have become a universal issue for all global actors, prompting a race to understand emerging conflict dynamics and develop working models relevant to each actor's strengths.⁵ As a result of the global academic learning campaign, the Russian Federation has adopted new strategic and tactical conceptual frameworks for this type of warfare under various names, including "hybrid warfare," "network-focused warfare," and "swarm warfare," among others.⁶ Despite the different trajectories each theoretical approach takes, the common trend is the overwhelming use of information to effectively shape the operational environment in the pre-conflict and crisis stages of a conflict.

Information Warfare Systems and Activities. Embedded in the Russian theoretical understanding, information warfare encompasses all systems and activities that are involved with the information domain, including electronic warfare, psycho-informational activities, and cyber operations. Russian capabilities like cyber, electronic warfare, laser, and others have been combined into a techno-informational branch, while functions that use information to affect the cognitive state of the public are combined into the psycho-informational branch of Russian Information Warfare.⁷ Decisive information warfare effects can be achieved by both branches but are selected based on the needs of a commander or the state of the operational environment.

The objective of Russian psycho-informational activities is to gain a commanding level of influence of all nation-state domestic and international decision making through a systematic degradation or destruction of a nation's cognitive sovereignty—the ability to self-determine domestic and foreign socio-political directions.⁸ If this cognitive maneuver is successful, it not only transfers national decision-making control to the aggressor state, but it can also achieve an aggressor's global end state without a transition into an armed conflict.⁹

The nascent stage of a conflict can be understood as a clash of narratives;¹⁰ informational activities like propaganda and other messaging become part of a deliberate set of preparatory actions that shape the environment for a potential follow-on military operation. The success of psycho-informational campaigns will ultimately determine if military action is possible, but in both cases, cognitive and informational campaigns are used for physical, tactical, and operational advantages. On the tactical and operational levels, an actor's global narrative for a military confrontation

develops a tactical advantage for friendly forces and extends partial control over the decision making of the enemy.

Since a large percentage of the global population is dependent on the global information network for trade and entertainment, nation-states become vulnerable to psycho-informational and info-technical influence activities. Unless a nation completely severs its connection to the global network, it is impossible to completely prevent foreign campaigns against national cognitive sovereignty. In Russia's case, the dominant actors in Russia's cognitive space have declared the permeation of the Western message through social media networks and other media a threat. To regain control over their domestic cognitive space, the Russian Federation has implemented a series of measures that attempt to filter content and isolate its domestic political and social discourse.¹¹

Units of Action. According to Russian scholarly understanding, maneuver through information in the cognitive and information domains exists at all three levels of war but varies depending on the conflict format and the stage of a conflict. A key characteristic of the current cognitive units of action is that they are all bound in the physical domain but adopt a dual property, being able to act and be acted upon in the physical, informational, and cognitive domains. This means that the cognitive conflict is still understood through its relationship to the physical domain and not solely as operations in the cognitive and informational domains.

The classification of an informational [cognitive] "unit of action" separates into nine groups:

- ◆ Military organizations with psychological operations capabilities, known as PSYOPS.
- ◆ Official governmental organizations (like a ministry of foreign affairs).
- ◆ Intelligence agencies.
- ◆ Military-focused media activities that focus on the production of information materials.
- ◆ International nongovernmental organizations (NGOs), including government-owned NGOs.
- ◆ Think tanks.
- ◆ International religious organizations.
- ◆ Mass media.
- ◆ Private activists with capabilities to operate info-technical systems or produce psycho-informational materials.¹²

The private activist unit of action is unique on this list because its actions create plausible deniability for an aggressor state. Additionally, private activists must initially

be developed and maintained by a separate set of psycho-informational activities that align their objectives with that of the aggressor. This is achieved through information campaigns like philosophical movements, religious campaigns, etc., that reach a broad audience but are designed to resonate with marginalized groups and create private activists.

The general scheme of maneuver for Russian cognitive maneuver is to identify an entry point into the information space of a target nation and then find a way to insert weaponized narratives into the general discourse, developing tactical access for follow-on physical maneuver, and move those narratives into the cognitive center, creating political opportunities.¹³

Entry into a cognitive space is achieved by identifying elements in a country's informational network using compatible Russian narratives. For example, the Eurasian Youth Union, Russkiy Mir Foundation, and fourth political theory offer conservative, right-wing political ideals while socialism, communism, and the political movement Essence of Time are left-leaning. To the overall plan, ideology is irrelevant and is used only to create perceived compatibility of objectives between the aggressor state and a target group. After a narrative is inserted, it is pushed into general discourse through informational and physical measures, like rallies, internet trolls, or other amplification methods by an aggressor state's informational unit of action. Once a narrative moves closer to the center of discourse, it creates cognitive effects and windows of opportunity for other levers of influence, including an operational force.

An operational force's role during the pre-crisis and crisis phases is reframed to suit a military-political campaign in which information created from an operation is just as critical to overall success as a tactical victory. An operational unit has three main roles:

- ◆ Act as a security provider for the development of a new socio-political reality.
- ◆ Execute operations in a way that supports the established narrative of a conflict.
- ◆ Fabricate the "reality" of the narrative worldview.

A critical component of military-political warfare is having a pipeline of information from the engagement spaces into the global arena. Psycho-informational messages and activities are irrelevant unless they can be pushed into the global cognitive space to achieve necessary strategic effects. To this effect, mass media has been re-conceptualized as the "heavy artillery" of cognitive maneuver, able to amplify and convert physical action into political off-ramps.¹⁴

Emerging Conflict Methodologies. Hybrid, network-focused, and swarm conflicts are emerging Russian Federation methodologies that are a result of the military and the government adapting to the new technological and political realities of the modern operational environment.

Within the hybrid format, psycho-informational activities are used in tandem with other capabilities to create a socio-political movement through domestic political and social movements. If an attempt to steer a nation in the desired direction is not feasible through psycho-informational activities, a military confrontation in tandem with these activities may be required.¹⁵

The network-focused strategy is an adaptation of "network-centric warfare" developed in the United States. This approach uses technical and psycho-informational activities to control the behavior of all allies, enemies, and neutral participants in global positional warfare. This format uses technological and psycho-informational methods to gain informational superiority in pre-crisis and crisis periods and develop a common operational picture between all friendly participants of the nonmilitary and proxy elements while denying the enemy access to decision-making data.¹⁶

Swarm warfare shifts operations to a decentralized condition. Informational units of action build loose networks through joint ventures, remaining largely independent, but can quickly organize to achieve a directed effect. This approach eliminates a targetable center of gravity and creates a socio-political and military network that is co-created by all of its members and whose activity is synchronized by the overall objective.¹⁷

Practical Applications

The invasion of Crimea by the Russian Federation and its pre-conflict activities exemplifies the power of psycho-informational campaigns and their use in hybrid, network-focused, and swarm operations. Evidenced by the Russian Federation's campaign for the seizure of Crimea, shaping operations in the cognitive domain through information operations was a key factor in the success of the invasion. Though seemingly benign, during the emerging phase of the conflict, informational, cognitive, and physical tools were able to create a narrative of a marginalized Russian ethnic minority, create a *casus belli* for a Russian Federation intervention under the mantle of a peacekeeper, and simulate the self-determination of the Crimean Peninsula.

Before the first "little green man" stepped onto Ukrainian soil, the Crimean Peninsula was inundated with Russian Federation-backed cultural and humanitarian projects, based on representing the Russian ethnic population in

Crimea.¹⁸ During the initial stage of the crisis, groups like the Eurasia Movement, Essence of Time, and other Russian unification groups established entry points into the Ukrainian cognitive space concentrating on Crimea, Donetsk, Lugansk, Kharkiv, and Odessa regions.¹⁹ Elements of the Eurasia Movement and Essence of Time established local media and organizational proxies in the regions. These major groups and their affiliates acted independently from the main pro-Russian Unification movement, but all shared the same objective—to construct a situation in which the unification of Crimea and the Russian Federation would be feasible.

Konstantin Knyrik and other private activists were instrumental in developing the situation in Crimea and other regions that fabricated a *casus belli* for Russian Federation intervention. Knyrik was indoctrinated into political activism by Aleksandr Dugin, the current front-man of the Eurasia ideological movement and the creator of the fourth political theory. Knyrik's organization represented a fraction of the unification effort with entry points in the right of the political spectrum. Groups from the left conducted similar activities, but all shared a common narrative of reunification with the Russian Federation.

Knyrik became an active participant in the local politics and established a media-center called "South-Eastern Front." His chapter of the Eurasian Youth Union was specifically valued as having "nonstandard capabilities," being able to create diversionary ideological actions during peacetime. The Eurasian Youth Union and its surrogates like Russian Veche in Crimea conducted rallies and other events, during which they used criminalistic actions to create a narrative of a marginalized minority, which was later echoed through a Russian Federation-controlled media network and government-owned NGOs like the Russkiy Mir Foundation. According to Knyrik's estimates, by 2014, his movement consisted of approximately 5,000 activists out of about 2 million total inhabitants of the Crimean Peninsula.

As tensions increased during the Ukrainian crisis in 2014, Knyrik became one of the main organizers on the peninsula and established a tactical informational effort to delegitimize non-Russian narratives. To cognitively isolate the engagement space, Knyrik and a group of militants seized the main informational coordination center of Crimea—the Crimean Center for Investigative Reporting, the region's



Armed men without insignia (so-called "little green men") at Simferopol Airport, 28 February 2014.

Photo courtesy of Elizabeth Arrott, Voice of America

leading independent news source²⁰—functionally gaining control of the information space. Russian state-owned media outlets amplified and pushed messaging originating from Crimea into the global conversation space, loaded with political implications.²¹

Decisive control of the information space in Crimea allowed pro-Russian groups to influence the global conversation on the crisis in Crimea, creating uncertainty and a lack of definitive narrative evidence that would politically justify Western intervention or reaction. During the escalation phase of the conflict, Igor Girkin with other operatives, funded by a non-state Russian entity, arrived in Crimea and began to recruit individuals in the administrative and security apparatus in Crimea.²² Concurrently with the Crimean unrest, Aleksandr Dugin was influencing other pro-Russian activists in Ukraine, moving the narrative forward. Concurrent with the protest activity, other semi-synchronized activities were happening on the peninsula and other parts of Ukraine, being synchronized by the overall military-political objective: a case for Russian Federation intervention.²³

Once the fabricated socio-political crisis achieved a breaking point with the collapse of the Ukrainian government in Kyiv, the leader of the Russian Unity party formally requested Russian Federation intervention under the mantle of "peacekeeper."²⁴

When Russian Federation forces assaulted Crimea, their posture echoed a "homecoming" even though Ukrainian

forces were still on the peninsula and under the control of the Ukrainian General Staff. Even though there was a significant tactical risk to the force and the mission, keeping to the established narrative mitigated these risks because the populace accepted the positioning of “peacekeeping” forces. Russian troops adopted a non-hostile posture with the Crimean public and were very measured in their interaction with the Ukrainian military, constantly focusing on the optics of Russian actions. This Russian operational posture developed an environment in which the Crimean Defense Force was incapacitated because any logical military action against the Russians would be exploited in the informational and cognitive domains, allowing the Russian Federation to escalate military action.²⁵

Tactical risk mitigation by the Russian forces was further achieved through Crimean activists’ tactical psycho-informational supporting operations that were used to amplify and confirm the pro-Russian narrative. Through tactical information exploitation, these pro-Russian “swarms” were able to produce strategic effects for the Russian Federation by adding counter-narratives into the global discourse, creating uncertainty and inaction from Ukraine and the international community.

Conclusions and Recommendations

- ◆ Information warfare is part of a larger global strategy that is perpetual and deliberate and has real effects for maneuver and physical engagement. Propaganda is more than a charged narrative that resides in the cognitive and informational spheres. It has the potential to create impactful effects in the physical domains.
- ◆ New types of conflicts are fought in the open, in many cases telegraphing their objectives because disruptive actors depend on moving large numbers of people. This means that significant actors in the pre-conflict and early conflict stages are in public view and seek exposure and amplification.
- ◆ Any operational force will be exploited for information and cognitive gains whether that force chooses to participate in a narrative engagement or not. In many cases, the message will be framed because the tactical informational teams are not bound by any standard other than victory.

Commanders and staffs should develop a deliberate analytical approach to how they interact with propaganda and information warfare at the tactical and operational levels. Since information warfare uses information weapons like messaging and propaganda, these individual messages can be analyzed similarly to any other munition that has a sender, a receiver, and an effect—an information domain

crater analysis. Lasswell’s communication model (who said what, in what channel, to whom, and with what effect) offers a perfect framework for this type of analysis.²⁶ By identifying the factors behind a propaganda message, it may be possible to gauge the effects of this information munitions on the mission and the operational environment. Individual message analysis will lead to trends, which could provide an opportunity to develop a more accurate “What the Russians want is...” estimate for a decision maker and planners.

Operational units must understand their unique role in the narrative fight and be able to produce evidence of a conflicting narrative to a hostile actor’s propaganda campaign. This can be as simple as creating special teams in platoons and above to carry video-capture devices that record uncertain situations that can be used as counter-narratives if a unit is exploited. Enemy tactical information teams are currently more capable than ever at inserting narratives into the global and regional cognitive domains. The ability to produce, format, and post information from a cell phone places operational forces in a disadvantageous position because a skilled operative can exploit anything they do.

Russia views the West as a threat to its national security through the perceived manipulation of Russian domestic affairs. Propaganda, disinformation, and other methods of weaponized information are the methods the Russian Federation uses to assert its military-political advantage. The warfighter must develop a greater understanding of modern information warfare along with the political components and objectives influencing its activities. ✨

TERMS	DESCRIPTION
ESSENCE OF TIME	A movement founded and led by Sergei Kurginyan. A mixture of communism with Russian patriotic elements. ²⁷
EURASIA MOVEMENT	Founded by Aleksandr Dugin. A mix of Russian nationalism, orthodox faith, anti-modernism, and some Bolshevik ideas. ²⁸
EURASIAN YOUTH UNION	A Russian traditionalist anti-European political organization, the youth wing of the Eurasia Party, headed by Aleksandr Dugin. ²⁹
FOURTH POLITICAL THEORY	A book by Aleksandr Dugin. Integrates and supersedes liberal democracy, Marxism, and fascism. Cited as an inspiration for events such as the war in Donbass. ³⁰
RUSSKIY MIR	The core culture of Russia. Includes the diverse cultures of traditions, history, and the Russian language. ³¹
RUSSKIY MIR FOUNDATION	Created by Vladimir Putin as a government-sponsored organization that promotes the Russian language worldwide, “forming the Russian World as a global project.” ³²

Figure by Jonathan S. Dingler

PEOPLE	DESCRIPTION	
ALEKSANDR DUGIN	Known for his fascist views, was the main organizer of the National Bolshevik Party, National Bolshevik Front, and Eurasia Party. Author of <i>The Fourth Political Theory</i> . ³³	<i>Проблемы Национальной Стратегии</i> , 2018, 122–143.
IGOR GIRKIN	Played a key role in the Russian Federation's Annexation of Crimea, and later in the war in Donbass as an organizer of the Donetsk People's Republic's militant groups. ³⁴	10. Samuel P. Huntington, "The Clash of Civilizations?" <i>Foreign Affairs</i> 72, no. 3 (1993): 22–49.
KONSTANTIN KNYRIK	Editor of the propaganda news agency News-Front. A pro-Russia activist in Crimea. Thinks of himself as an information warrior for the digital age. ³⁵	11. Polunin, "Проблема Информационной Безопасности."
		12. Smirnov, "Информационно- психологическая война."
		13. Vladimirov, <i>Основы общей теории войны</i> .
		14. Smirnov, "Информационно- психологическая война."
		15. Kuchinskaya, "Феномен Гибридизации"; and Sivkov, "Анатомия гибридной войны."


Figure by Jonathan S. Dingler

Endnotes




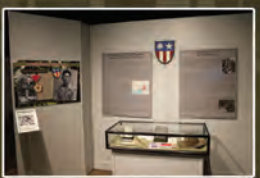



1. " 'Полит-Ринг' Игорь Стрелков vs Николай Стариков. Такие разные патриоты. Особенности патриотической 'кухни' " ["Polit-Ring" Igor Strelkov vs Nikolai Starikov. Different Patriots. Peculiarities of Patriotic "thought"], Нейромир-ТВ [Neuromir-TV], January 22, 2015, <https://neuromir.tv/tsentrily-silatsentra/>.
2. Aleksandr Ivanovich Vladimirov, *Основы общей теории войны Vol I* [Fundamentals of the General Theory of War] (Moscow: University "Synergy," 2018).
3. Знание сила [Knowledge is power] Konstantin Sivkov, "Анатомия гибридной войны" [Anatomy of hybrid warfare], August 9, 2017, YouTube video, 59:50, https://www.youtube.com/watch?v=gvD_V9jsjAA; and Alexander Smirnov, "Информационно- психологическая война" [Psycho-informational war], *Свободная мысль* [Free Thought], 2013, 81–96.
4. Sergey I. Makarenko, "Информационные конфликты - анализ работ и методологии исследования" [Information warfare—analysis of works and methods of research], *Systems of Control, Communication and Security*, 2016, 95–178.
5. Sirotkin Dmitry Viktorovich, Martyanov Anatoly Nikolaevich, Novikov Vladimir Kuzmich, and Ponomarenko Anatoly Viktorovich, "Модель Информационного Противоборства в Вооруженных Силах Российской Федерации" [Model of Information Warfare in the Armed Forces of the Russian Federation], *Отечественная Юриспруденция*, no. 8 (2016): 49–51.
6. Vladimirov, *Основы общей теории войны*.
7. Sergey I. Makarenko, *Информационное противоборство и радиоэлектронная борьба в сетевых войнах начала XXI века* [Information and Electronic Warfare to Network-Centric Wars of the Early XXI Century] (St. Petersburg: Наукоемкие технологии, 2017); Eugene S. Polunin, "Проблема Информационной Безопасности Государства в Современных Научных Исследованиях" [The Issue of Governmental Informational Security in Scientific Studies], *Воздушно-космические силы, Теория и практика*, no. 7 (2018): 43–54; and Viktorovich et al., "Модель Информационного."
8. Polunin, "Проблема Информационной Безопасности"; and Vladimirov, *Основы общей теории войны*.
9. Vladimirov, *Основы общей теории войны*; and Marina Kuchinskaya, "Феномен Гибридизации Современных Конфликтов: Отечественный и Западный Военно-Политический Дискурс" [The Hybridization Phenomenon of Current Conflicts: Domestic and Western Military-Political Discourse],
10. Samuel P. Huntington, "The Clash of Civilizations?" *Foreign Affairs* 72, no. 3 (1993): 22–49.
11. Polunin, "Проблема Информационной Безопасности."
12. Smirnov, "Информационно- психологическая война."
13. Vladimirov, *Основы общей теории войны*.
14. Smirnov, "Информационно- психологическая война."
15. Kuchinskaya, "Феномен Гибридизации"; and Sivkov, "Анатомия гибридной войны."
16. Vladimirov, *Основы общей теории войны*.
17. Ibid.
18. ITV News, "Актуальное интервью с Константином Кныриком" [indepth interview with Konstantin Knyrik], September 3, 2014, YouTube video, 20:04, <https://www.youtube.com/watch?v=ZJI9zRT6WAs>.
19. Телеканал ICTV, "Novorossiya. The Price of the Project—film about the war in Donbass," May 2, 2016, YouTube video, 48:55, https://www.youtube.com/watch?v=2dzgMKM_gbU&list=PLuKigYPS-KRaQY30SqJ0qCBIAwRw6Lz1.
20. Andreas Rossbach, "meetTheKremlin's Keyboard warrior in Crimea: is konstantin knyrik the new star of Russia's information war?" *Coda Story*, 29 May 2018, <https://www.codastory.com/disinformation/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/>
21. ITV News, "Актуальное интервью"; and PolitWera, "Константин Кнырик: Русское движение Украины было или есть?" [Konstantin Knyrik: Is the Russian Movement still present in Ukraine?], July 25, 2018, YouTube video, 1:26:45, <https://www.youtube.com/watch?v=UtgO-fBcPxo>.
22. Дмитрий Гордон [Dmitry Gordon], "Гиркин (Стрелков). Донбасс, МН17, Гаага, ФСБ, полудохлый Путин, Сурков, Божий суд. ГОРДОН (2020)" [Girkin (Strelkov). Donbass, MN17, The Hague, FSB, half-dead Putin, Surkov, God's judgment. GORDON], May 18, 2020, YouTube video, 3:41.51, https://www.youtube.com/watch?v=hf6K6pjK_Yw&list=PLuKigYPS-KRZfoY6uZsAjO9LdZ0P5RzW&index=36&t=12s.
23. Oleksiy Pivtorak, "Dugin-Hubarieva on Ukraine. Дугин-Губарева про Україну," April 3, 2014, YouTube video, 34:57, <https://www.youtube.com/watch?v=UL6nphPhSAw>.
24. Телеканал ICTV, "Novorossiya."
25. Ibid.; and Gordon, "Гиркин (Стрелков)."
26. Dennis McQuail and Sven Windahl, *Communication Models for the Study of Mass Communication* (New York: Routledge, 1993).
27. Wikipedia, s.v. "Essence of Time (movement)," last modified 28 March 2021, 18:42, [https://en.wikipedia.org/wiki/Essence_of_Time_\(movement\)](https://en.wikipedia.org/wiki/Essence_of_Time_(movement)).
28. Wikipedia, s.v. "Eurasia Movement," last modified 24 February 2021, 17:58, https://en.wikipedia.org/wiki/Eurasia_Movement.
29. Wikipedia, s.v. "Eurasian Youth Union," last modified 15 April 2021, 19:54, https://en.wikipedia.org/wiki/Eurasian_Youth_Union.

30. Wikipedia, s.v. "The Fourth Political Theory," last modified 15 April 2021, 17:00, https://en.wikipedia.org/wiki/The_Fourth_Political_Theory.
31. Wikipedia, s.v. "Russian World," last modified 25 March 2021, 13:59, https://en.wikipedia.org/wiki/Russian_world.
32. Wikipedia, s.v. "Russkiy Mir Foundation," last modified 15 February 2021, https://en.wikipedia.org/wiki/Russkiy_Mir_Foundation.
33. Wikipedia, s.v. "Aleksandr Dugin," last modified 22 April 2021, 14:48, https://en.wikipedia.org/wiki/Aleksandr_Dugin.
34. Wikipedia, s.v. "Igor Girkin," last modified 20 April 2021, 15:21, https://en.wikipedia.org/wiki/Igor_Girkin.
35. U.S. Department of State, *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem* (Washington, DC: Global Engagement Center, August 2020), 31, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf; and Simon Shuster, "Russia Has Launched a Fake News War on Europe. Now Germany Is Fighting Back," *Time*, August 9, 2017, <https://time.com/4889471/germany-election-russia-fake-news-angela-merkel/>.

SFC Sergei Volodin serves as a military science instructor at Purdue University's Reserve Officer Training Corps. He previously served at the U.S. Army Asymmetric Warfare Group as an operational advisor supporting the U.S. European Command and U.S. Central Command areas of responsibility.



Military Intelligence Soldier Heritage Learning Center

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

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

Preparing for the Future of Cyberspace and Electromagnetic Activities Support to Corps and Below

U.S. Army illustration

by Major Wallie G. Lacks

The Defense Advanced Research Projects Agency's PlanX program is working to help military cyber operators visualize the cyber battlespace and perform missions there based on an established cyberspace framework and a common operational picture.

Introduction

As a participant in the U.S. Army Intelligence Development Program—Cyber, I often heard much debate about the term “intelligence support to cyber.” The phrase itself should be easily understandable and translatable to any intelligence professional. However, I have found that not to be the case. Too often, it breaks down into nondescript ideas of what “support” means. Those ideas often lead to confusing intelligence requirements, further impeding any agreed-upon meaning between intelligence and operational cyberspace planners about support.

As a member of the Combined Joint Task Force—Operation Inherent Resolve's cyberspace electromagnetic activities (CEMA) cell embedded within the joint fires section from December 2017 through July 2018, I came to view the term as a nuanced way of saying, “providing commanders a situational understanding of cyberspace.” ADP 6-0, *Mission Command: Command and Control of Army Forces*, defines situational understanding as, “the product of *applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables*” to facilitate decision making.¹ Therefore, the intelligence professional must understand what data is needed to build a situational picture and consider which intelligence elements at the appropriate echelon translate and synchronize the data to ease CEMA utilization into a commander's plan.

Finding the Intelligence Data

The quote cited from ADP 6-0 is what an intelligence professional must do to turn data into a situational understanding of cyberspace for commanders and staff. Identifying operational and mission variables builds an understanding of a given operational environment.² This means building an understanding of how the enemy, friendly, and neutral parties operate in the cyberspace environment. These variables become the refinements necessary in linking the mission facts, constraints, and assumptions of not only probable enemy cyberspace courses of action but also possible friendly actions and counteractions. This requires knowing how to achieve understanding through the arrangement of collected data.

The intelligence professional should arrange data to identify, characterize, and monitor enemy and friendly activity within the cyberspace and electromagnetic spectrum environment. The data necessary to identify, characterize, and monitor enemy and friendly cyberspace activity resides in three keys layers of cyberspace—physical, logical, and cyber-persona.³ Figure 1 (on the next page) shows these three layers and their relationship to the data collected for analysis to provide situational understanding to CEMA.

Physical Layer. The figure visually arranges the data in such a way as to focus it on the end state of situational understanding. The first data point of a cyberspace-collection

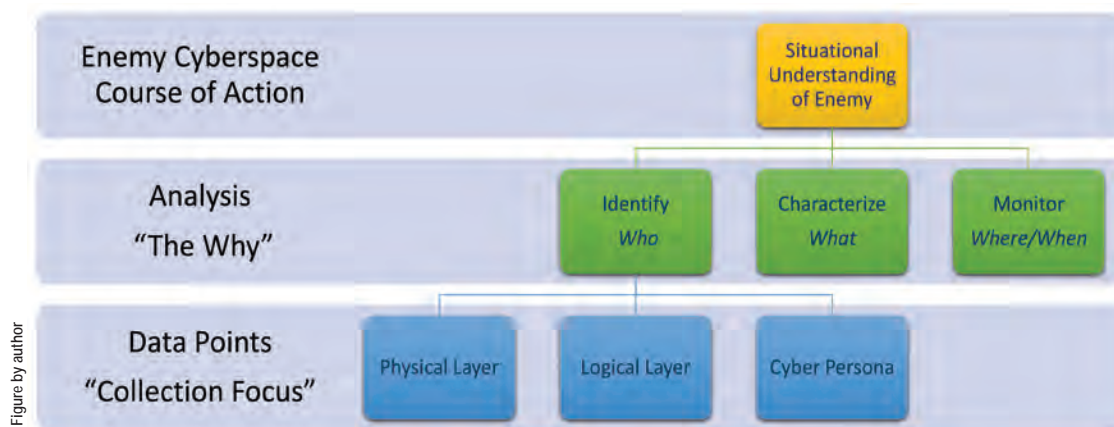


Figure 1. Organizing the Data

erating within cyberspace. This means that the ability to identify, attribute, and act upon individuals and entities is possible. Identities in cyberspace include email addresses, social networks, web forums, and computer IP addresses of end user devices such as tablets, computers, portable computers, smart watches,

focus is the physical layer. The physical layer of cyberspace is just that—physical. It is the location (and components) where elements that create a logical network reside. The physical layer consists of hardware such as computers, smartphones, small office and home office wireless routers, personal Wi-Fi routers, telecommunication fiber hubs, and satellite point of presence. This physical infrastructure is the backbone upon which the logical layer exists.⁴

Logical Layer. The next layer is the logical layer. This layer consists of devices allowing data on the physical layer to move between different networks. The devices are physical, but their primary purpose is to support the transportation of data via logical addressing. This address at its most basic concept consists of a source internet protocol (IP) address and a destination IP address. It contains the data that makes up a transmitted message known as the payload. This framed data routes through cyberspace by devices that decipher the best method to get to the destination IP address. This routing is carried out by devices known as switches, routers, or multilayer switches.⁵

These logical layer devices are necessary in allowing data to go from one end user device (computer, tablet, smartphone, etc.) to another end user device across a single or series of networks. The switch electrically and logically connects devices together while the router and/or multilayer switch allows for connections between networks. Understanding the logical addresses and ports used for communications on the devices' operating systems within a network provides a way to visualize a mapped path between networks and end devices.⁶

Cyber-Persona Layer. The third layer is the cyber-persona layer. The cyber-persona layer is the digital representation of an individual or entity (organization) op-

and mobile device numbers.⁷

The cyber-persona layer can be complex because of its elements that touch multiple virtual locations at once without having a solid link to a physical location or form.⁸ The intelligence professional must understand that knowledge gained from any form of targeting or analysis to identify attribution requires significant diligence. This diligence is key to understanding the cyber-persona layer and its linkages to the physical and logical layer. The criticality of summarizing all three layers into an intelligence whole during analysis is the essence of developing the cyberspace situational awareness for commanders. Figure 2 shows this construct.

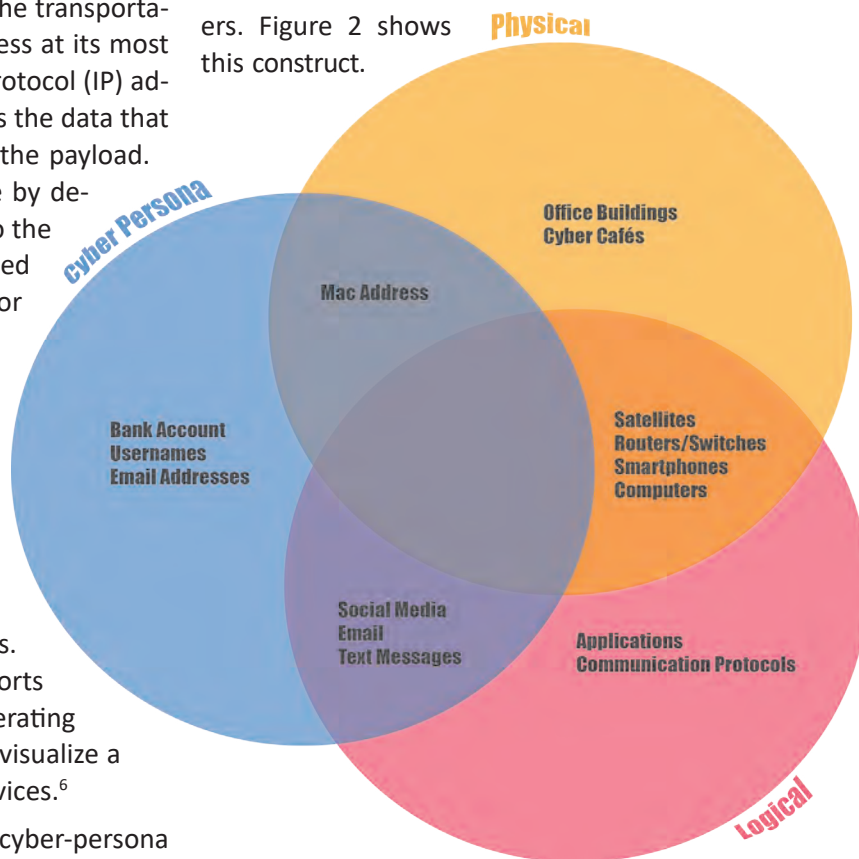


Figure 2. Understanding the Data

Figure by Jonathan S. Dingler

Arranging the Data

The data-collectable aspects of the physical, logical, and cyber-persona layers of cyberspace are not mutually exclusive to just one form of collection. For instance, an IP address at the logical layer or an email address at the cyber-persona layer can come from either human intelligence (HUMINT) or signals intelligence (SIGINT). Physical locations housing components of a network's physical layer can be collected via imagery, HUMINT, or SIGINT as well. Therefore, an intelligence professional should not fall into the trap of thinking that the information necessary to build a picture should come from only one intelligence discipline.

However, given the nature of the intelligence collection enterprise architecture from the corps level down to the maneuver brigades and battalions, the ability to build a shared situational understanding of cyberspace shrinks at each command echelon. For instance, the intelligence enterprise structure from the corps down through brigade focuses on the land domain and the enemy's physical formations. This makes intuitive sense because lower echelon formations are or should be in constant contact with the enemy in a more kinetic fight. Therefore, the capacity of intelligence database network resources such as the SECRET Internet Protocol Router Network and Joint Worldwide Intelligence Communications System, as well as access to national-level data sets, shrinks as it goes from corps down to divisions and brigades.⁹ The ability to build a robust situational understanding of cyberspace and the electromagnetic spectrum becomes ever more difficult the lower in the command echelon it is attempted. It is for these reasons that the corps intelligence staff must be the foundation of the translation point for the enemy's electronic order of battle and cyberspace courses of action for the area of operations.

The corps intelligence section can pull together the infrastructure necessary to cross-collaborate with national agencies as well as lower echelons. Additionally, it is at the corps where the tactical formation's situational awareness of cyberspace needs to begin because of today's cyberspace threat. The corps commander's guidance on offensive and defensive cyberspace operations, based upon awareness from the G-2/G-6, baselines not only the corps but also the echelons down to brigade. This essential guid-

ance begins the process of ensuring cyberspace operations nest from corps to brigade and back up through the corps and into collaborating agencies. It is essential that the translation of the cyberspace fight start at the corps headquarters. The corps intelligence staff is the cornerstone that secures the process of ensuring lower-echelon intelligence staffs account for cyberspace effects while also aiding in shaping tailored processes that incorporate echelon above corps support.¹⁰ This tailored process must be more than just a communications link to the Army Cyber enterprise.¹¹ Rather, the process must be a well-rehearsed and routinely employed endeavor that operates both in garrison and in the field. Additionally, the established relationship must account for communication with combatant command joint cyber cells. There must also be an understanding of what cyberspace elements (cyber combat mission teams supporting combatant commands) are actively posturing, collecting, and reporting in a potential future corps area of responsibility within a combatant command's region. The corps intelligence staff must also build relationships with the U.S. Army Intelligence and Security Command's theater military intelligence brigade supporting that region.

Theater military intelligence brigade designs can support not only the combatant command and Army theater command but also the corps headquarters. The theater military intelligence brigade intelligence capabilities could serve the purpose of assisting the corps with synchronizing strategic and operational-level intelligence collection and analysis necessary for building an understanding of the cyberspace domain within a corps assigned area of operations. Figure 3 shows this concept and the expected benefits of this construct.

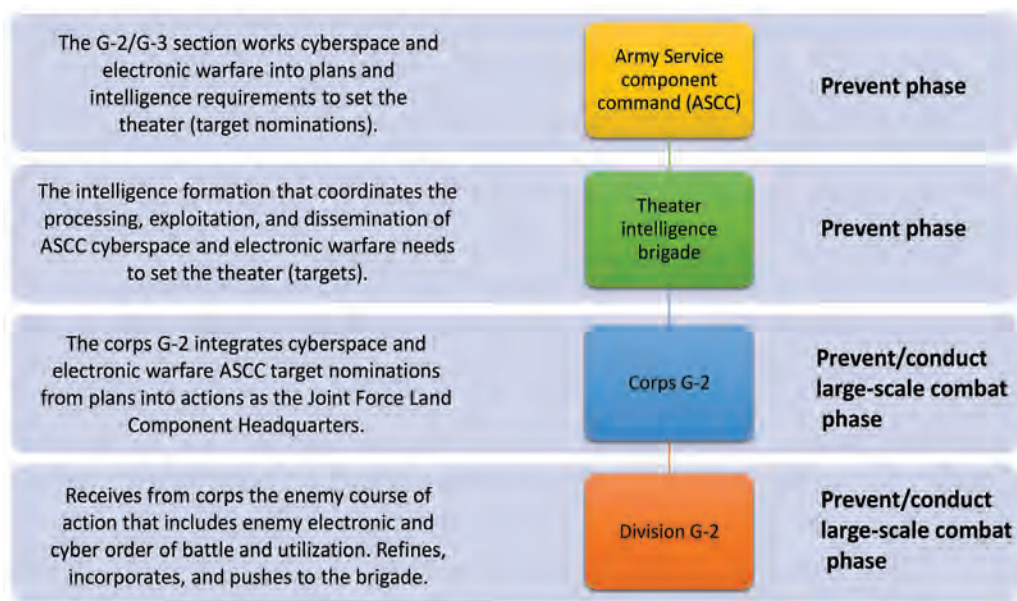


Figure 3. Aligning Intelligence Elements

Figure by author

Benefits of an Aligned Ensemble

There are both positive and negative aspects to aligning or not aligning where the intelligence translation for cyberspace and electronic warfare begins. The proper aligning of intelligence translation will force intelligence sections to construct and collaborate more in developing virtual target folders for cyberspace effect nomination.¹² This is a critical step in developing targeting aim points against enemy military systems that use cyberspace. Just as critical is that the alignment normalizes intelligence elements at all echelons on how to request, systematize, support, and employ cyberspace-based information efficiently. A solid process set up in this manner would reassure commanders and result in clear cyberspace planning and targeting guidance for the staff.

By not having this solid process, organizations run the risk of pitting cyberspace against unrealistic requirements. Worse, it also results in little to no intelligence development toward a virtual target nomination that should accompany a cyberspace fires request. When intelligence alignment is off and not collecting to build a situational understanding of cyberspace, there is a tendency for cyberspace support requests to read, “Deny the enemy use of the internet on objective A within the next 96 hours.” This type of request is indicative of the staff’s and commander’s limited understanding of the cyberspace domain and all the coordination necessary as it pertains to a tactical problem. It is symptomatic of staffs seeing cyberspace as a dynamic tool that delivers battlefield effects much like other fire support elements rather than a deliberate tool necessitating greater synchronization.

These overly broad requests with no accompanying intelligence information or virtual target targeting folders become cold starts for the cyber force. The basic through advanced target development and intelligence to build the target becomes the task of a small limited intelligence sec-

tion that supports the cyber mission team. This increases the amount of time the cyber force needs to build an understanding of an adversarial network to deliver effects. It also causes cyber mission teams to have a lack of refined target guidance. This leads to teams being bogged down with additional considerations regarding the target, such as determining the targeted area’s redundant internet connectivity. Do you target the internet service provider and its internal infrastructure, the local cellular provider, or the very small aperture terminal satellite points of presence?

Cyberspace operations are not a panacea for all things internet-related. Because of this, the cyber force must go back to the requestor and seek a more refined target aim point. In short, this results in intelligence staff work that should have been conducted during the targeting process, before the request was made, happening after the fact. The outcome is wasted time, effort, and man-hours.



Cyber operations specialists from the Expeditionary Cyber Support Detachment, 782nd Military Intelligence Battalion (Cyber), from Fort Gordon, GA, provided offensive cyber operations as part of the Cyber Electromagnetic Activities Support to Corps and Below Program during the 1st Stryker Brigade Combat Team, 4th Infantry Division, National Training Center Rotation 18-03, January 18 to 24, 2018.

U.S. Army photo

Conclusion

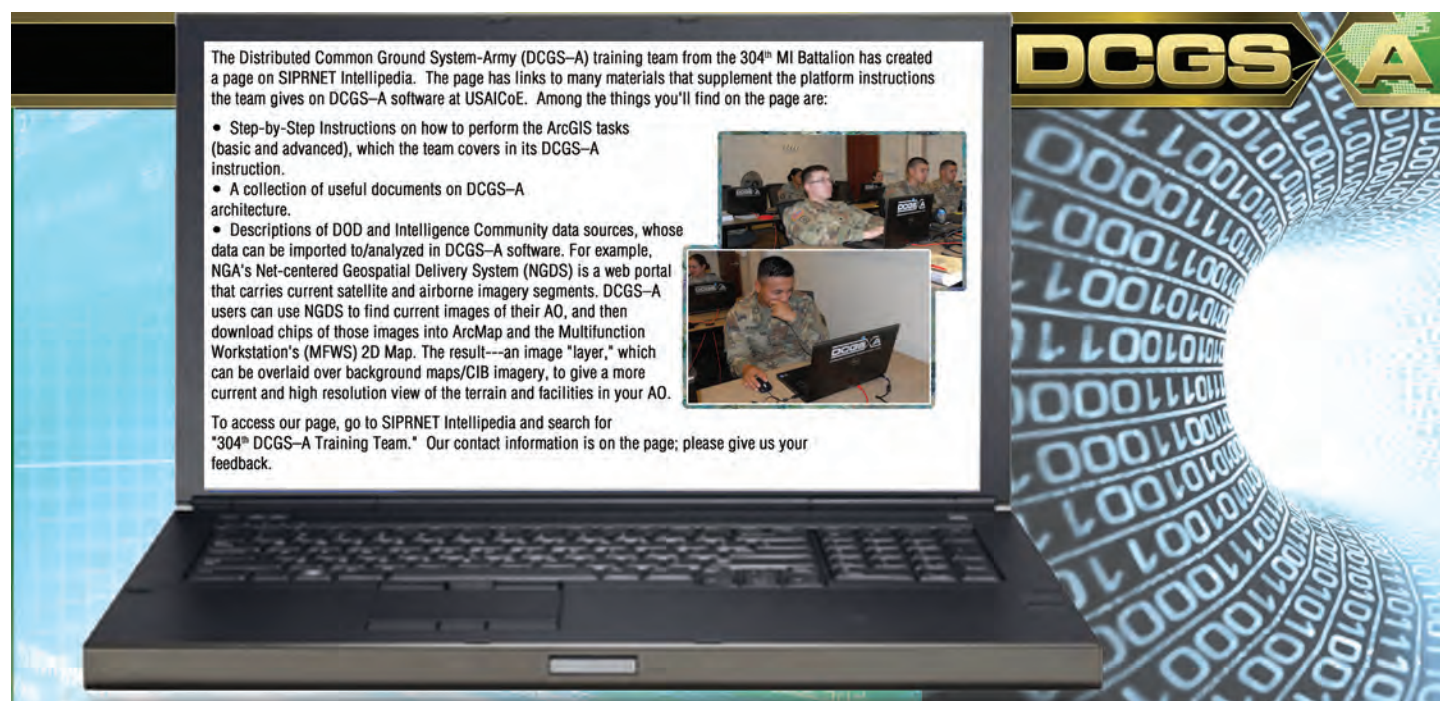
The Army is moving to integrate cyberspace support to tactical formations from the corps level to the brigade. This endeavor will not work unless the intelligence warfighting function understands its role and rethinks *where cyberspace translation begins*. Additionally, if intelligence translation begins at the corps or joint task force level, so too should operational implementation translation.

Intelligence support to cyber is the term often used. Yet the intelligence role in cyberspace is much larger than that. Rather, by thinking of how to build a situational understanding of cyberspace for staffs and commanders at the right organizational echelon, intelligence is not only supporting cyber but also easing its utilization and transition from a strategic, operational asset to a tactical tool. 🌟

Endnotes

1. Department of the Army, Army Doctrine Publication 6-0, *Mission Command: Command and Control of Army Forces* (Washington, DC: U.S. Government Publishing Office [GPO], 31 July 2019), 2-3 (emphasis added).
2. Department of the Army, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. GPO, 11 April 2017).
3. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: The Joint Staff, 8 June 2018), I-3.
4. 30 Bird Media, *CompTIA A+ Certification 220-901/220-902 Comprehensive* (Rochester, NY: 30 Bird Media, 2016), 298, 312, 329.
5. 30 Bird Media, *Network+ Certification Exam N10-006 Student Edition* (Rochester, NY: 30 Bird Media, 2016), 165.
6. Ibid., 174–175.
7. Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, 1-13.
8. Ibid.
9. Department of the Army, Army Techniques Publication (ATP) 2-19.3, *Corps and Division Intelligence Techniques* (Washington, DC: U.S. GPO, 26 March 2015), C-3 (common access card [CAC] login required); and ATP 2-19.4, *Brigade Combat Team Intelligence Techniques* (Washington, DC: U.S. GPO, 25 June 2021), C-8 (CAC login required).
10. Isaac R. Porche III, Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below* (Santa Monica, CA: RAND Corporation, 2017), 71–72.
11. Department of the Army, ATP 2-19.3, *Corps and Division Intelligence Techniques*, A-6.
12. Joint Staff, Chairman of the Joint Chiefs of Staff Instruction 3370.01B, *Target Development Standards* (Washington, DC: U.S. GPO, 6 May 2016) (CAC login required).

MAJ Wallie Lacks is a graduate of the U.S. Army Intelligence Development Program–Cyber. He currently serves as the executive officer of the 308th Military Intelligence (MI) Battalion, 902nd MI Group. His previous cyber-affiliated assignments include Commander, Counterintelligence Cyber Activity, 310th MI Battalion, 902nd MI Group; cyber-planner for the Combined Joint Task Force-Operation Inherent Resolve cyberspace electromagnetic activities (CEMA) team; and deputy CEMA chief, cyber operations, 8th Army G-3 Fires. MAJ Lacks is a graduate of the Joint Network Attack Course and Joint Cyber Planners Course. He has completed A+, NET+, and SEC+ courses and earned certifications in A+ and SEC+.



The Pathway to Multi-Domain Intelligence Proficiency: The I2CEWS Approach

by Major Owen Ryckman and First Lieutenant Erica Forktus

Photo courtesy of MAJ Ryckman



Soldiers of the Multi-Domain Military Intelligence Company, Intelligence, Information, Cyber, Electronic Warfare, and Space Battalion, 1st Multi-Domain Task Force, on September 21, 2020.

The Army builds and sustains multi-domain formations through the selection, training, and education of the leaders, Soldiers, and teams in them. Employing multi-domain capabilities requires the Army to attract, retain, and employ leaders and Soldiers who collectively possess a significant breadth and depth of technical and professional expertise.

—TRADOC Pamphlet 525-3-1,

The U.S. Army in Multi-Domain Operations 2028

As a profession, Army intelligence traditionally focuses institutional training and collection and analytical efforts on the ground domain while, for the most part, leaving the air, maritime, space, and cyberspace domains to other branches of Service, functional commands, and government agencies. With the transition from counterinsurgency to multi-domain operations (MDO) and large-scale ground combat operations, this paradigm is untenable because Army intelligence professionals must also shift alongside the larger Army.

As the command team for the Multi-Domain Military Intelligence Company in the Intelligence, Information, Cyber, Electronic Warfare, and Space (I2CEWS) Battalion, 1st Multi-Domain Task Force, we quickly identified training gaps for our intelligence Soldiers that affect the Army's desired transition to MDO and large-scale ground combat operations. Our Soldiers came into the organization confident and capable when working with ground domain target systems, yet lacked the institutional training to understand the threats resident in the other domains, the electromagnetic spectrum, and the information environment. We found that multi-domain intelligence requires integration across all intelligence disciplines, domains, and the joint

force to support situational understanding and inform the commander's decision making. To keep pace with the increasing complexity of the post-counterinsurgency intelligence problem set, intelligence analysts and producers must increase their knowledge of the various domains and address training gaps to support operations across the conflict continuum.

To address our identified training shortfalls, the Multi-Domain Military Intelligence Company in the I2CEWS Battalion developed an analyst progression training program and established an internal training standard (see figure on the next page). The program exposes Soldiers to new knowledge and focuses on core and elective courses complemented by on-the-job training. The purpose of the training program is for our intelligence professionals to remain grounded in their core competencies while simultaneously broadening their exposure, knowledge, and analytical capability across all domains, the electromagnetic spectrum, and the information environment. Training within the system is different for each military occupational specialty and is scalable to balance the experience of all ranks from junior to senior enlisted as well as officers and warrant officers. Additionally, given our collaboration with various Centers of Excellence, the training includes several core classes that teach Army intelligence Soldiers to understand the information environment, electromagnetic spectrum, different domains, joint targeting standards, and tools used by our joint, interagency, intergovernmental, and multinational partners.

Our combination of knowledge enhancement and core course requirements creates the crux of our training pipeline, but our internal training standard also places emphasis on an analyst's continued growth and is an important part of the solution to our identified training gaps. The organization's training and education standard differs from that of traditional organizations: after Soldiers complete their designated core courses, we strive for every Soldier (enlisted, warrant, and officer) to attend at *least* two additional courses each calendar year. This standard of continuous training serves three primary purposes. First, it ensures our Soldiers have recent and updated knowledge regarding the technologies, systems, and techniques that various areas use within the Department of Defense. Second, it educates our Soldiers how to think critically within a domain or topic where traditional "intelligence support to x" does not exist. Third, it holistically improves the Army intelligence enterprise because our Soldiers will eventually leave our organization and proliferate their knowledge and experience across the Army. When a Soldier shows an interest in continuing to develop advanced skillsets in any of the domains, electromagnetic spectrum, or information environment, they become the resident expert within the formation and increase the unit's proficiency in MDO. Our training pipeline and our standard of continuous training generate tenable, though not perfect, solutions to mitigate intelligence train-

ing gaps to keep the intelligence profession able to support the commander's decision making as the Army moves toward MDO and large-scale ground combat operations.

It is our hope that other intelligence professionals can leverage our hard-earned knowledge and apply it in their formations. The I2CEWS Battalion keenly feels the multi-domain training deficit because of our mission set while the rest of the Army is only just beginning to conceptualize MDO and work toward multi-domain readiness. The lessons learned by the I2CEWS Battalion vis-à-vis training are becoming increasingly relevant to the rest of the force. While not the solution to all of the problems MDO and large-scale ground combat operations bring us, our lessons learned began in late 2018 with the genesis of the I2CEWS and continue to evolve as our mission set, force structure, and capabilities mature. We will continue to update our analyst progression and share the results via the Center for Army Lessons Learned and the Multi-Domain Operations Lessons Learned Forum. To participate in the forum contact usarmy.huachuca.icoe.mbx.lessons-learned@mail.mil. 🌟

Epigraph

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

ANALYST PROGRESSION PROGRAM		
Core Courses by Discipline	Core Courses by Domain	Elective Courses by Domain
<p><u>All-Source</u></p> <ul style="list-style-type: none"> All-Source Production Course Gunner Entry Program <p><u>SIGINT</u></p> <ul style="list-style-type: none"> Apprentice Operational Electronic Intelligence Course (SIGE 2120) Fusion Analysis Development Effort/Multi-INT Spatial Temporal (FADE/MIST) toolsuite <p><u>GEOINT</u></p> <ul style="list-style-type: none"> Target Mensuration Only Intermediate Operations Course Geospatial Intelligence (GEOINT) Advanced Operations Course GEOINT <p><u>Systems Maintenance and Integration</u></p> <ul style="list-style-type: none"> Security Plus Computing Environment Courses 	<p><u>Joint Training</u></p> <ul style="list-style-type: none"> Joint Intermediate Target Development FADE/MIST toolsuite <p><u>Information Environment</u></p> <ul style="list-style-type: none"> Information Operations Fundamentals Course Information Operations Integration – Military Information Support Operations Open-Source Intelligence 301 <p><u>Space Domain</u></p> <ul style="list-style-type: none"> Army Space Basic Cadre Course <p><u>Cyber Domain</u></p> <ul style="list-style-type: none"> Cyber Threat Training for Intelligence Professionals <p><u>Air/Maritime</u></p> <ul style="list-style-type: none"> Formal Army courses do not exist. Currently conducting live environment training to supplement. 	<p><u>Joint Training</u></p> <ul style="list-style-type: none"> Still developing <p><u>Information Environment</u></p> <ul style="list-style-type: none"> Army Information Operations Planners Course Open-Source Intelligence 302 <p><u>Space Domain</u></p> <ul style="list-style-type: none"> Space Control Planners Course <p><u>Cyber Domain</u></p> <ul style="list-style-type: none"> Cyber Mission Forces Training Pipeline <p><u>Air/Maritime</u></p> <ul style="list-style-type: none"> Still developing

MAJ Owen Ryckman is the commander of the Multi-Domain Military Intelligence Company in the Intelligence, Information, Cyber, Electronic Warfare, and Space (I2CEWS) Battalion, 1st Multi-Domain Task Force (MDTF), since July 2019, and was the senior intelligence officer for the MDTF until late 2020. While assisting the stand-up of the MDTF, he earned the 3Y additional skill identifier (Space Badge), has taken Information Operations and Military Information Support Operations courses, and is scheduled for Joint Intermediate Target Development.

1LT Erica Forktus is the executive officer of the Multi-Domain Military Intelligence Company in the I2CEWS Battalion, 1st MDTF, since June 2020. She has taken the Army Space Basic Cadre Course and the Information Operations and Military Information Support Operations courses. She is scheduled for Joint Intermediate Target Development, the Gunner Entry Program, and the Information Collection Planners Course (Q7).

A Mathematical Probability of Success for Soviets in Cold War Confrontation

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

Editor's Note: This article is part one of a two-part series on the Soviet correlation of forces and means.

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

Introduction

Who will be in the Final Four during March Madness? Which horse will win in the Kentucky Derby? Who has the better tank, the Americans or the Russians? The answer to these questions is based on past performance, statistics, hype and, too often, wistful guessing or a hunch. This may be adequate when the bet is ten dollars in an office pool, but bet-

ter analysis and predictability are necessary when lives and national survival are at stake.

The notion that the inherent values of various weapons and systems (and the personnel who man them) can be measured and compared against a single quantitative standard is as contentious as is developing an infallible system for the quantification of battle. Yet the Soviets long pursued mathematizing battle. Intuitively, the military practitioner may suspect the existence of such a relationship, but proving it is very difficult. Historical studies have not yet revealed an infallible system for determining the total quantification of combat or operations, and perhaps they never will. Regardless, Soviet military scientists searched for objectivity and optimization in military affairs by using

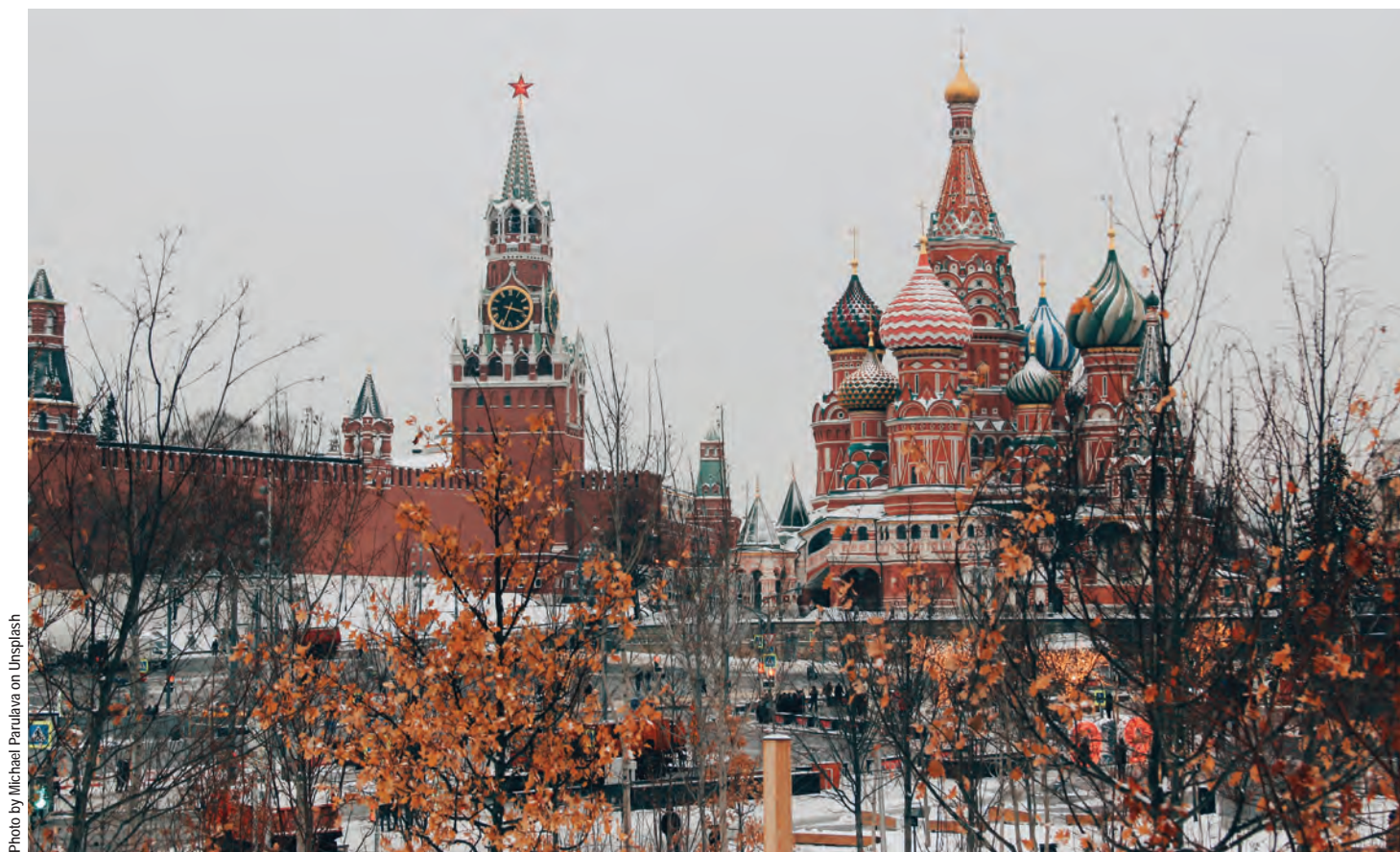


Photo by Michael Parulava on Unsplash

The Kremlin, Moscow, Russia, on January 14, 2019.

military operations research to reduce tactical and technical aspects of military science to measurable, objective indices from which decisions could be made or otherwise substantiated. A sub-element of Soviet military operations research was the correlation of forces and means (COFM) methodology. COFM was considered a powerful tool for helping operational- and tactical-level commanders in their decision-making processes. The Soviet definition of COFM was—

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

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

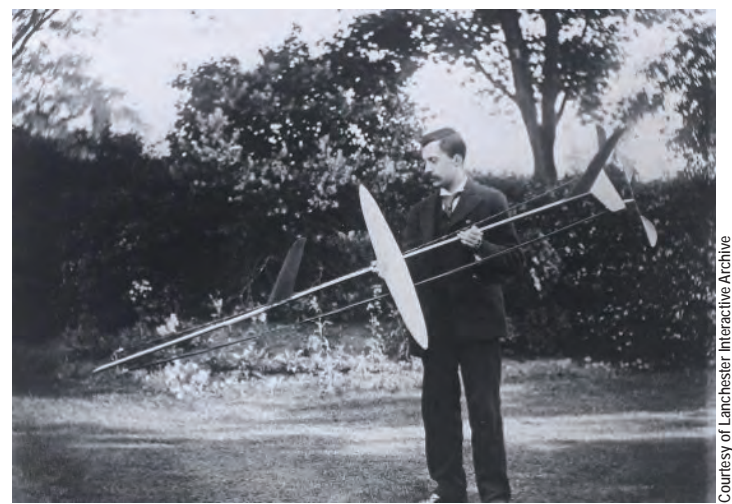
Pre-Soviet and Soviet Development of Strategic Decision Models

The Russians have a long history of developing the mathematical determination of combat.³ Beginning in the 1850s, military wargames employing rudimentary mathematics were part of the training of general staff officers. In 1884, Nikolai Volotsky directly applied mathematical means (including probability theory) to solving wartime ammunition supply problems.⁴ By the outbreak of World War I, prominent military and civilian writers were mathematizing the theories of modern combat. Of particular significance were the contributions of M. Osipov,⁵ working independently of Frederick W. Lanchester,⁶ which derived a series of finite difference equations for predicting combat outcomes. He developed his "theory of losses" from an analysis of 38 historical battles fought between 1805 and 1905. Osipov's formulae were an excellent starting point for forecasting battle outcomes and optimizing one's forces. Osipov's work served as historical substantiation of the interrelationship of mathematics and armed conflict. Several decades later,

Soviet mathematicians would expand and refine his basic equations to include the consideration of randomness and battlefield variables.⁷

By the mid-1950s, the Communist Party and state leadership determined that it could not resolve complex national security issues without serious scientific support. This resulted in the creation of a wide network of scientific research institutes (SRIs), which were charged with providing support for preparing and making strategic decisions. Their structures corresponded to the structures and missions of the organizations to which they belonged. The fundamental areas that SRI research and development focused on were methodologies, quantitative methods, and mathematical models to support decision making at all command levels in the Ministry of Defense, General Staff, and armed services. Automation of command and control for the higher-level staffs and field units was particularly important.⁸ SRI research topics in support of the General Staff included developing—

- ◆ A system of models and mathematical methods to support planning strategic nuclear strikes and evaluating the results.
- ◆ Systems of mathematical models to forecast the course and outcome of conflict in theater operations; front and army operations; and tactical combat of ground force divisions, air defense, and aviation. (A *front* is roughly an army group of three to five armies.)
- ◆ Models to automate and provide information support to the General Staff and high-level staffs.
- ◆ Systems of models to support mobilization, weapons development, and military technology.⁹



Frederick Lanchester experimenting with his glider at his home in Birmingham, UK, 1894. Frederick W. Lanchester (1868–1946), an English mathematician and engineer who designed automobiles, postulated the theory of aerodynamics.

Courtesy of Lanchester Interactive Archive

Well-known scientists led the SRIs, and they gathered the top talent from among the graduates of the Soviet Union's leading civilian and military universities and academies. The SRIs offered good working locations and top salaries. A supporting infrastructure of computer, communications, information, and database centers was developed to support their work. Modeling helped design and optimize this infrastructure.¹⁰

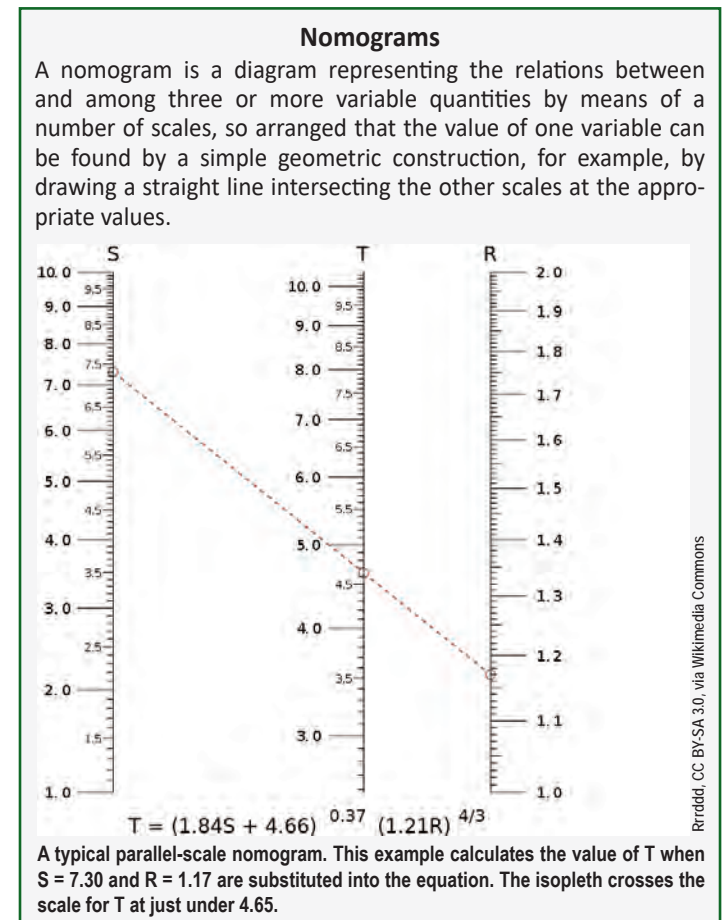
In the early 1960s, the Lanchester and Osipov mathematical models of combat were studied and applied to the problems of strategic nuclear war using mathematical optimizing methods and game theory. This approach proved impossible in modeling the high degree of uncertainty and complexity of modern ground forces operations. A new approach was needed and developed. It did not attempt to formalize fully the modeled processes. Combat at different scales was represented with algorithmic descriptions of real-time space dynamics or armed combat considering the—

- ◆ Specific location of troop formations of both sides.
- ◆ Interaction of forces and means in time and space to achieve missions.
- ◆ Maneuver of forces and means, the dependence of the outcome on the effectiveness of combat support, and rear area support.
- ◆ Uncertainty under which both sides decide and operate.¹¹

The algorithmic model describes the sequential nature of logical and quantitative procedures with sufficient accuracy for staff work. An SRI working for the Main Operational Directorate of the General Staff undertook development of the model. It developed models of front and army operations and combined arms combat. The accuracy of the model was tested over a 2-year period by modeling 10 successful Red Army front ground forces operations against the Germans in 1944. Since Soviet and German archival documents exaggerated enemy losses and underreported own losses, the actual manpower losses were determined from supply records indicating daily unit requests for food and ammunition.¹²

The COFM model was supposed to measure combat potential based on calculation units. Depending on the scale, the calculation units could be individual systems, or aggregates of systems in units. At the strategic level, calculation units were divisions while battalions and companies were calculation units at the operational/tactical level. The characterization of division calculation units was in terms of time needed to prepare for operations, rate of movement, time

needed to deploy into combat positions, allocation of ammunition and daily support needs, time required to reconstitute combat capabilities after various degrees of losses, and so on. These characteristics are aggregates of the characteristics of lower-level units. Models of the operational and tactical levels represent aspects of armed conflict with sufficient precision to determine the characteristics of the calculation units.¹³ This modeling effort was supported by various nomograms, tables, reference books, and developing computer systems.¹⁴



Tactical, Operational, and Strategic COFM of the Cold War Era

North Atlantic Treaty Organization (NATO) Operations Research/Systems Analysis (ORSA) practitioners spent a lot of effort trying to determine Soviet coefficients of combat power and their formulae for determining attack widths; loss of combat effectiveness; effects of terrain, training, morale, nationality, and days of combat; and effects of battlefield reconstitution.¹⁵ Soviet coefficients of combat power were developed for different Soviet and Western weapons systems using fire power, survivability, rates of fire, and mobility. The T-55 tank was used as base one against which to measure other systems.

Coefficient of Combat Power

Assigning a coefficient of combat power to a system against which to measure other systems is hardly a new concept. Beginners to the ancient game of chess learn that the combat potential of a pawn is one. A bishop and a knight are both threes. A rook is a five and a queen is a nine. The king has a combat power of one, but because his capture determines the contest, the king also has a power of infinity. There is a COFM between varying pieces depending on positioning.¹⁶



Game of Worlds

Table 1 (on the next page) provides details from a 1980 United States intelligence information report on the Soviet coefficients of combat power of tanks, infantry fighting vehicles, infantry personnel carriers, artillery and mortar systems, and antitank weapons.¹⁷ Table 1 lists the coefficients of combat power for individual weapons systems. These coefficients would normally be incorporated into friendly and opposing unit tables of organization and equipment (TO&E) before hostilities. They would be updated based on intelligence as to combat losses and reinforcements. Non-TO&E units would be a concern and require input from intelligence and analysis. Irregular warfare is a challenge for the COFM system. Guerrillas fight as small groups and may have unrated weapons systems such as “technical” vehicles mounting a machine gun, small mortar, or recoilless rifle. Furthermore, guerrillas do not match the conditions of conventional maneuver war—their positions are usually one deep rather than multiple positions incorporated into an integrated defense extending 5 kilometers or more. Table 1 provided the basis for the mathematical determination of tactical and operational COFM, but determining how many enemy systems of what quality will confront the friendly systems is only the beginning, as it aggregates the combat power available to both sides prior to the fight. This merely describes upcoming combat on a billiards table. The

friendly and enemy forces would need to be adjusted by the application of mathematical “K” factors—terrain; morale; nationality; training; days of prior combat; logistics support; width of attack sector; whether defending troops are in the open, dug in, or part of a well-engineered defense; current strength; combat losses, and so on. This adjusted COFM could then be used to determine mathematically the width of an attack sector and rate of advance. Soviet officers were well schooled in mathematics and relied on mathematical tools to verify the commander’s decision or to adjust the plan to meet the mathematical coefficients that quantify success. The K factors of that time are still not available in open-source—and these made higher tactical and operational calculations possible.

Table 1 provided the ability to determine the aggregate combat power of opposing units for tactical combat and operations. There was no combat potential value for individual soldiers, just weapons systems. The value of soldiers was in the aggregate that is modified by K factors. The combat power model does not allow for cowards or heroes; however, soldiers must be alive and armed to man systems. Mathematical planning at the tactical level was further supported by planning tables, formulae, and nomograms.¹⁸

Table 1 also supported the determination of tank versus anti-tank combat, air versus air defense combat, and air versus air combat, as well as combined combat/operations using the organic and attached systems of the opposing forces.

Table 2, on page 34, provides details from a 1980 United States intelligence information report on the Soviet coefficients of combat potentials of Warsaw Pact and NATO divisions (and the Canadian Battle Group).¹⁹ The Soviet TO&E Motorized Rifle Division equipped with T-55 tanks and BMP infantry fighting vehicles was the base one unit against which other units were valued. The table was developed for the possibility of war in Central Europe; therefore, it does not include the NATO forces of Norway, Italy, and Turkey, nor does it include the Warsaw Pact forces of Hungary, Romania, and Bulgaria. These undoubtedly existed in the planning files of other strategic axes. Again, this information describes operations on a billiards table. The values were adjusted by their own series of “K” factors. Table 2 was the starting point for operational and strategic planning, as it provided the coefficients of combat power of large ground units. Again, without their operational K factors, Table 2 remains as the basic piece of a larger process.

Conclusion

The COFM modeling system was a central tool for Soviet tactical, operational, and strategic planning. It provided mathematical certainty and predictability for conventional

maneuver warfare under nuclear-threatened conditions and provided a degree of stability and rationality to maintaining the status quo of the Cold War. The COFM model did not disappear with the collapse of the Soviet Union. Russia has upgraded their COFM model and enhanced its value as a planning tool with improved computing capability and capacity. 🌟

Table 1. 1980 United States data on combat potentials of the armament and combat equipment of the ground forces and aviation of the Soviet Union and of the armies of their probable enemy			
Ground Forces and Aviation of the USSR		Armies of the Probable Enemy	
Nomenclature of Armament	Combat Potential	Nomenclature of Armament	Combat Potential
Tanks, Self-propelled Artillery, Infantry Combat Vehicles, Armored Personnel Carriers			
T-55+	1.00	M60A3	1.40
T-62	1.00	XM-1 experimental	2.50
T-64A	1.50	Leopard-1A4	1.50
T-80	1.80	Leopard-2	2.40
T-64B	2.10	Chieftain Mark-5	1.50
T-72	1.50	AMX-30	1.10
T-72 with D-kl tank gun	1.70	Leopard-1	1.10
T-80 improved	2.80	MBT-80	1.60
T-54B	0.90	M60A2	2.20
T-44	0.75	M60A1	1.10
T-34 with 85mm gun	0.49	Leopard-1A1	1.40
T-10M	1.51	M48, M48A1	1.00
IS-2M	0.70	M47	1.10
IS-3	0.83	M41	0.36
IT-1	0.80	M551	0.83
PT-76	0.48	AMX-13/75mm gun, SS-11B1	0.80
ISU-152	0.79	AMX-13/90mm gun	0.54
SU-122	0.60	T-59	0.90
SU-100	0.55	T-62 (85mm gun)	0.42
SU-85	0.48	T-34 (76mm gun)	0.43
ASU-85	0.21	T-54A	0.90
ASU-57	0.18	T-54	0.87
BMP-1	0.80	Pz-61	0.60
BMD-1	0.80	Pz-68	1.00
BTR, BRDM	0.10	SU-76	0.32
		Marder IFV w/o ATGM	0.10
		Marder IFV w/ ATGM	0.50

Ground Forces and Aviation of the USSR		Armies of the Probable Enemy	
Nomenclature of Armament	Combat Potential	Nomenclature of Armament	Combat Potential
Field Artillery and Mortars			
76mm gun, gun howitzer	0.38	105mm howitzer	0.63
85mm gun	0.42	105mm SP howitzer	0.70
122mm SP howitzer 2S1	0.81	155mm howitzer	0.66
122mm howitzer	0.70	155mm SP howitzer	0.90
122mm gun A-19	0.61	175mm SP gun	0.75
122mm gun A-74	0.66	203.2mm howitzer	0.80
152mm SP howitzer 2S3	0.86	203.2mm SP howitzer	0.84
152mm howitzer	0.71	81mm mortar	0.50
130mm gun	0.70	51mm mortar	0.30
152mm gun-howitzer	0.74	81mm SP mortar	0.58
152mm gun	0.66	106.7mm mortar	0.54
203mm howitzer	0.62	106.7mm SP mortar	0.65
203mm SP gun 2S7	0.66	120mm mortar	0.56
82mm mortar	0.45	120mm SP mortar	0.71
82mm SP mortar Vasilek	0.60	110mm LARS rocket launcher	0.77
107mm mountain mortar	0.42	115mm MRL	0.77
120mm mortar	0.60		
160mm mortar	0.60		
240mm mortar	0.74		
240mm SP mortar 2S4	0.80		
30mm AGS-17	0.12		
122mm BM-21 MRL	0.87		
140mm BM-14 MRL	0.56		
240mm BM-24 MRL	0.70		
122mm BM-21 Grad-1	0.90		
220mm BM-27 MRL	0.95		
200mm BMD20 MRL	0.73		
132mm BM-13 Katyusha	0.40		
122mm BM-21B MRL	0.75		
140mm RPU-14 MRL	0.42		
Ground Forces and Aviation of the USSR		Armies of the Probable Enemy	
Nomenclature of Armament	Combat Potential	Nomenclature of Armament	Combat Potential
Antitank Weapons			
Konkurs AT-5 Spandrel	0.93	HOT	0.98
Fleyta AT-2 Swatter	0.95	TOW	0.95
Falanga-M	0.70	SS-12	0.80
Malyutka-P AT-3 Sagger	0.67	MILAN	0.78
Fagot AT-4 Spigot	0.62	SS-11B1	0.70
Malyutka AT-3 vehicle mount	0.60	SS-11SP	0.60
Malyutka AT-3PK	0.55	DRAGON	0.52
Falanga vehicle mount	0.50	ENTAC SP	0.48
Shmel AT-1 Snapper	0.31	VIGILANT	0.40
Shmel AT-1 vehicle mount	0.37	Cobra	0.40
T-12 100mm AT gun	0.65	SS-10	0.34
BS3 100mm AT gun	0.46	Jagdpanther 90mm SP gun	0.63
D-44 85mm AT gun	0.44	120mm recoilless rifle	0.23
ZIS-2 57mm AT gun	0.30	106mm recoilless rifle	0.28
B-10 82mm recoilless rifle	0.15	75mm recoilless rifle	0.20
SPG-9 73 MM recoilless gun	0.25	90mm AT rocket launcher	0.12
RPG-7	0.12	88.9mm shoulder-fired AT rocket	0.10
		66mm 4-barrel AT rocket launch	0.15
		66mm AT rocket launcher	0.05

Table 2. Combat potentials of large units					
Designation of Large Unit	Combat Potential of Rated Divisions	Total Combat Potential in Units of Armament	Designation of Large Unit	Combat Potential of Rated Divisions	Total Combat Potential in Units of Armament
Motorized Rifle Division, T-55, BMP	1.00	652	US Infantry Division	0.86	564
Motorized Rifle Division, T-64A, T-72, BMP	1.18	766	US Mechanized Division	1.10	718
Motorized Rifle Division, T-62, BMP	1.04	680	US Armored Division	1.23	803
Motorized Rifle Division, T-54B, BTR	0.82	533	US Airborne Division	0.68	441
Guards Motorized Rifle Division T-64A, BMP, SP Arty	1.29	842	US Non-organic Division	0.72	468
Guards Motorized Rifle Division T-62, BMP, SP Arty	1.13	736	FRG Infantry Division	1.22	795
Motorized Rifle Division T-64A, T-72, BTR	1.05	684	FRG Motorized Infantry Division	1.30	849
Motorized Rifle Division T-62, BTR	0.92	599	FRG Tank Division	1.27	825
Motorized Rifle Division T-62, BMP	1.01	660	FRG Mountain Infantry Division	1.04	682
Tank Division, T-64A, BMP	1.22	793	UK Infantry Division	0.39	257
Tank Division, T-62, BMP	1.01	656	UK Armored Division	0.77	503
Tank Division, T-72	1.21	787	Belgian Mechanized Infantry Division	0.68	445
Polish Motorized Division	0.67	437	Danish Mechanized Infantry Division	0.92	605
Polish Tank Division	0.51	304	Netherlands Mechanized Infantry Division	0.94	614
East German Motorized Rifle Division	0.75	487	French Mechanized Division	0.23	152
East German Tank Division	0.72	466	French Infantry Division	0.23	152
Czech Motorized Rifle Division	0.75	490	French Alpine Infantry Division	0.32	208
Czech Tank Division	0.63	413	Canadian Separate Mechanized Battle Group	0.20	128

Endnotes

1. V. I. Belyakov, "Соотношение Сил и Средств" [Correlation of Forces and Means], *Советская Военная Энциклопедия* [Soviet Military Encyclopedia], Volume 7 (Moscow: Voenizdat, 1979), 445.
2. Michael Chichenski, "Soviet Correlation of Forces and Means" (class lecture, U.S. Army Russian Institute, Garmisch, Germany, 1982).
3. James K. Womack, "Soviet Correlation of Forces and Means: Quantifying Modern Operations" (master's thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, 1990), 41, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a227427.pdf>.

4. Ibid., 11–12; and Jacob W. Kipp, *From Foresight to Forecasting: The Russian and Soviet Military Experience* (College Station, TX: Center for Strategic Technology, Texas A&M University, 1988), 18–19.

5. "Osipov's most unique and important contribution is the explicit and systematic application to quantitative historical data of what, for his time, were fairly advanced formal statistical methods." Robert L. Helmbold and Allan S. Rehm, translators' notes to *Research Paper CAA-RP-91-2: The Influence of the Numerical Strength of Engaged Forces on their Casualties*, by M. Osipov, trans. Robert L. Helmbold and Allan S. Rehm (Bethesda, MD: Army Concepts Analysis Agency, 1991), ix, originally published in Russian as "The Influence of the Numerical Strength of Engaged Forces on their Casualties," *Voenniy*

Sbornik [Military Collection] (June–October 1915). M. Osipov wrote a series of articles in the June to October 1915 editions of the Tsarist military journal *Voennyi Sbornik*. He used differential equations to model the combat losses of opposing sides based on raw historical data from 38 major battles from the Napoleonic Wars to the Russo-Japanese War. There is no trace of Osipov after the Russian Revolution. Most likely, he was Colonel Mikhail Pavlovich Osipov, a topographic engineer. Jacob S. Kipp, “Tracking Down Russia’s Lanchester,” *Journal of Slavic Military Studies* 17, no. 2 (2004): 257–269.

6. Frederick W. Lanchester (1868–1946) was an English mathematician and engineer who designed automobiles, postulated the theory of aerodynamics, and founded the science of operational research. He developed the Lanchester differential equations for calculating relative strengths of military forces.

7. Kipp, *From Foresight to Forecasting*, 87–89, in Womack, “Soviet Correlation of Forces and Means,” 12–13.

8. Vitali Tsygichko, *Models is the System of Strategic Decisions in the USSR* (Riga: Lambert Academic Publishing, 2019), 13–14.

9. *Ibid.*, 14–15.

10. *Ibid.*, 15, 27.

11. *Ibid.*, 28–29.

12. *Ibid.*, 37.

13. *Ibid.*, 47.

14. “Соотношение Сил и Средств” [Correlation of Forces and Means], *Военный Энциклопедический Словарь* [Military Encyclopedic Dictionary] (Moscow: Voenizdat, 1983), 691.

15. John A. Battilega and Judith K. Grange, *The Military Applications of Modeling* (Washington, DC: U.S. Government Publishing Office, 1984), was the foundation document of the U.S. Operations Research/Systems Analysis (ORSA) effort. Allan S. Rehm and Pete Shugart were key researchers in the U.S. effort. British researcher Charles Blandy wrote the best English-language publication on the subject, Charles W. Blandy, *Calculating Combat Outcomes* (Sandhurst, UK: Soviet Studies Research Centre, 1993). Unfortunately, by the time it had cleared the hurdles of security review, it was February 1993. The Soviet Union had collapsed and Blandy’s work has enjoyed a limited readership.

16. For a discussion of this concept, see Clint Reach, Vikram Kilamei, and Mark Cozad, *Russian Assessments and Applications of the Correlation of Forces and Means* (Santa Monica, CA: RAND, 2020), 39–45.

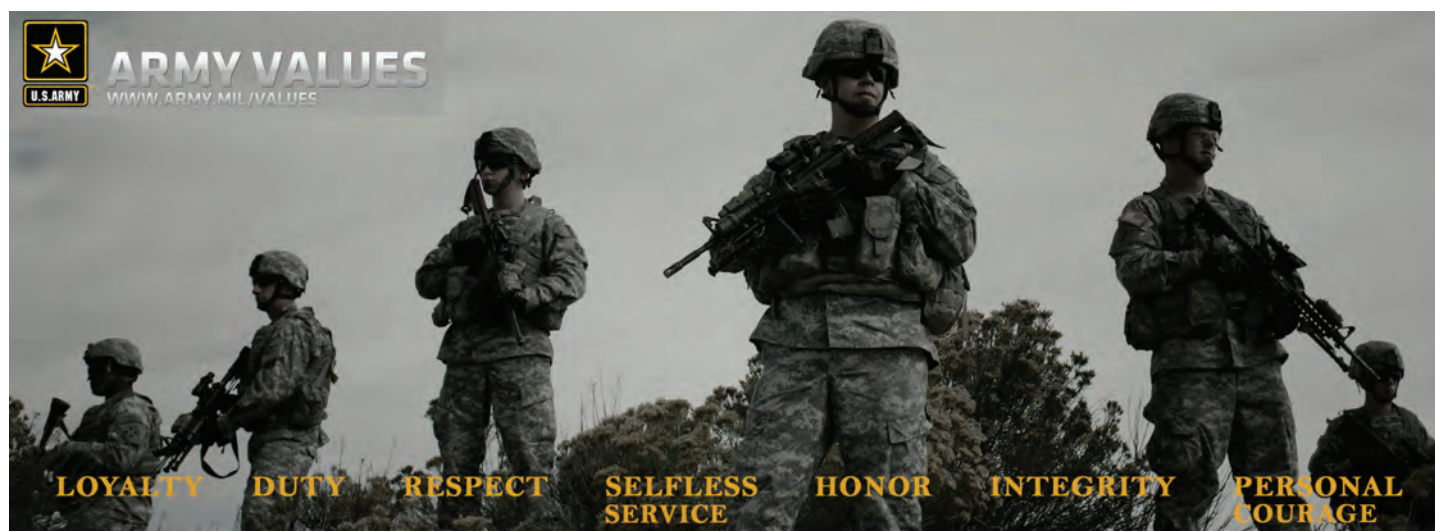
17. Memorandum for Director of Central Intelligence, “Combat Potentials of the Armament and Combat Equipment of the Ground Forces and Aviation of the USSR and the Armies of the Probable Enemy, and Table of the Combat Potentials of Large Units,” 25 August 1980. This document was declassified from Top Secret to Unclassified and approved for release by the Historical Collection Division on 18 August 2012.

18. A. Ya. Vayner, *Тактические расчёты* [Tactical calculations] (Moscow: Voenizdat, 1977) was the primary planning text for battalion and regimental staffs that lacked computer access.

19. Memorandum, “Combat Potentials.”

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

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



The Vitality of Synchronized Intelligence Operations for a Division Support Area Command Post

U.S. Army photo by SPC Daniel Parrott, Operations Group, NTC

by Captain Julee R. Thomas

U.S. Soldiers assigned to 1st Battalion, 24th Infantry Regiment, 1st Brigade Combat Team, 25th Infantry Division, prepare to move a tactical operations center during Decisive Action Rotation 17-03 at the National Training Center (NTC), Fort Irwin, CA, January 18, 2017. Decisive action rotations at the NTC ensure units remain versatile, responsive, and consistently available for current and future contingencies.

Introduction

Effective support area intelligence operations require the centralization of dedicated personnel and military intelligence (MI) equipment. To meet the current need, FM 3-0, *Operations*, established the support area command post (SACP) for corps and division headquarters.¹ Since the SACP is not on the modified table of organization and equipment (MTOE), borrowing personnel and equipment from a unit's MTOE causes a major constraint for resources during an exercise or deployment. The division's support area, shown in Figure 1, consists of tenant brigades composed of company-level or above elements from combat aviation, field

artillery, division artillery, sustainment, military police, and engineers. Most of these units merge intelligence from multiple enablers across a wide geographic area to provide to the analysis and control element (ACE). The presence of a G-2 cell enables the SACP to synchronize intelligence operations in the support area. It also provides commanders and senior intelligence officers with a common understanding of the enemy composition, disposition, and strength in the consolidation area.

Framing the Problem

During Decisive Action Rotation 20-10 at the National Training Center, Fort Irwin, California, the 1st Infantry Division established a G-2 cell to work at the SACP using organic personnel and equipment to resource the command post. Throughout the rotation, the SACP G-2 submitted intelligence collection requests each night to the ACE intelligence collection and management section in the division main command post (CP), which was primarily at the National Training Center. Compared to the priority for intelligence collection over the deep and close fight areas, the division consolidation area was at the bottom of the priority list for collection assets.

To exacerbate conditions during the rotation, one of the G-2 day-shift Soldiers tested positive for the coronavirus disease 2019, resulting in the entire G-2 day-shift section going into quarantine throughout the main phases of the exercise. Rapidly obtained intelligence personnel filled in for G-2 day-shift staff, but their lack of experience in division training made the transition less seamless than intended.

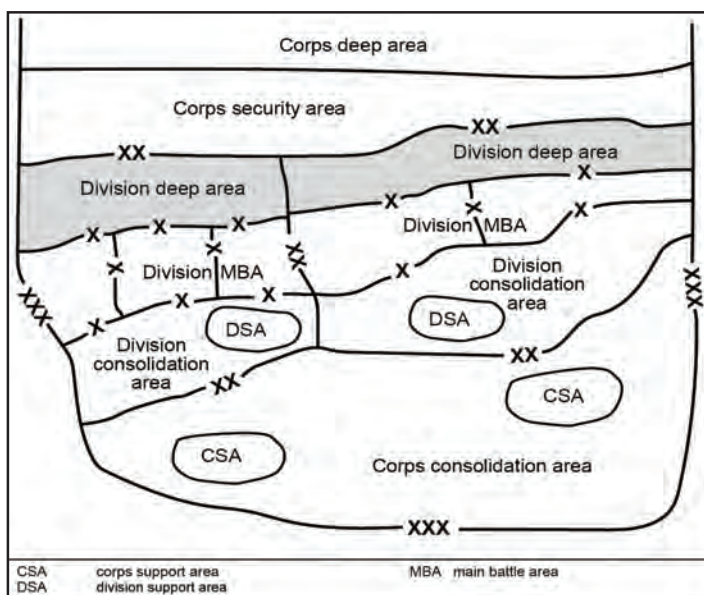


Figure 1. Main Battle Area²

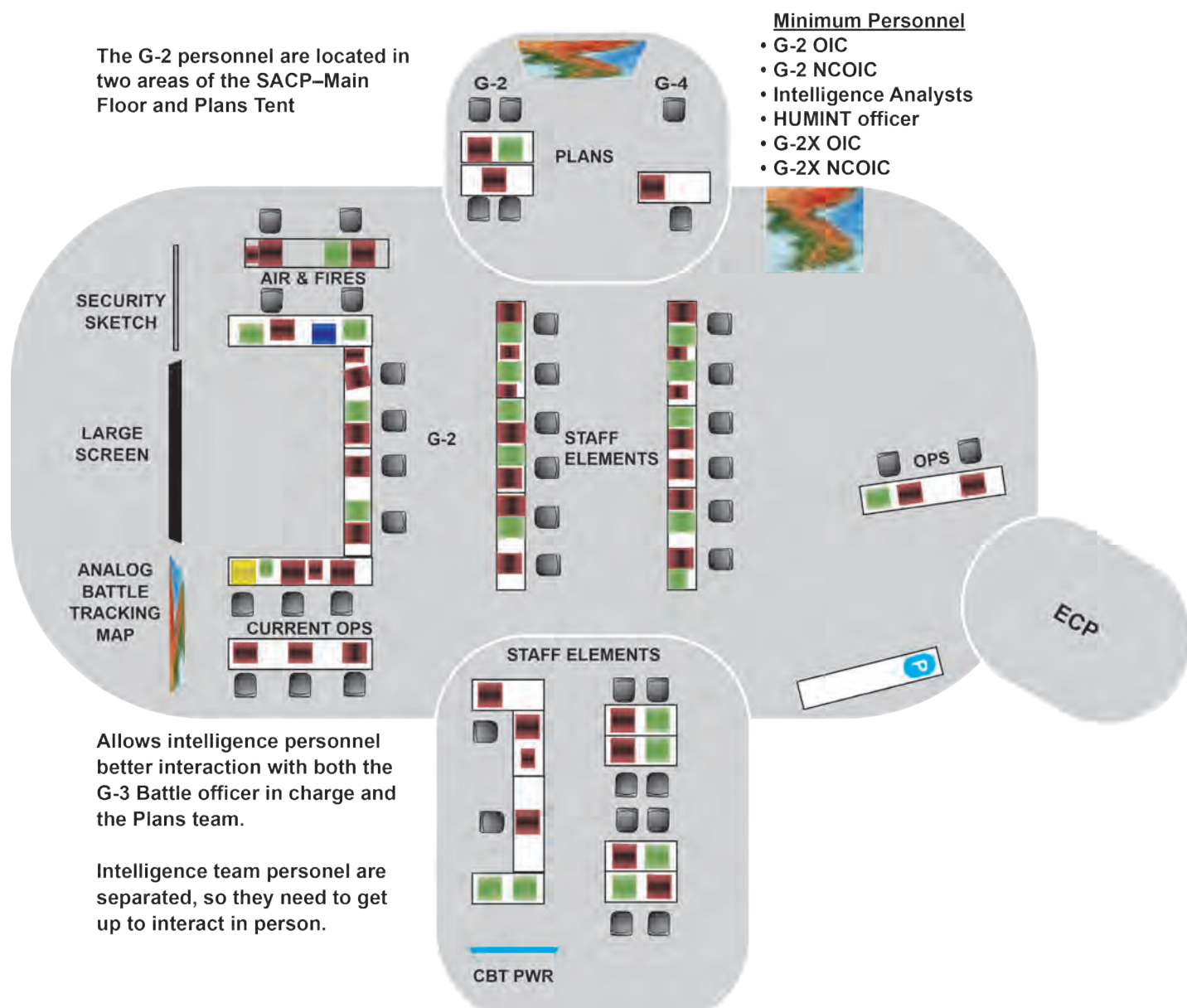
Toward the end of the exercise, when both the division main CP and division tactical CP jumped, the SACP had taken over the fight. Having a reduced staff for the G-2 and not having the resources of an ACE element at the SACP to manage intelligence operations during the fight was an enormous risk to the 1st Infantry Division's mission. The division consolidation area received multiple attacks by enemy threats, which most likely would have been prevented if the G-2 intelligence operations cell was adequately staffed and resourced with the proper intelligence equipment and personnel.

Intelligence Manning and Equipment

Success for a mission begins with the CP. "Commanders arrange CP personnel and equipment to facilitate internal co-

ordination, information sharing, and rapid decisionmaking. They also ensure they have procedures to execute the operations process within the headquarters."³ As mentioned earlier, the SACP does not have personnel or equipment under the MTOE. Recommendations for the G-2 intelligence cell at the division SACP would include properly trained MI (35 series) personnel to fill the roles of a G-2 officer in charge, G-2 noncommissioned officer in charge, a minimum of two intelligence analysts, a human intelligence officer, and a G-2X. Figure 2 shows an example SACP layout.

The G-2 intelligence cell at the SACP would primarily oversee intelligence collection requests integrated by the ACE collection management and dissemination and fusion sections for the division consolidation area but would still have



a shared understanding of the common intelligence picture of the deep and close fight areas. It would provide all-source intelligence and information pictures to the stakeholders while responding to group-specific needs for analysis, assessment, and collection.

Implementation

Following our current 1st Infantry Division tactical standard operating procedure, the SACP G-2 intelligence cell would provide daily intelligence support, including formal daily assessments to the SACP commander, chief of sustainment, chief of operations, primary staff, and all assigned units, satisfying a wide variety of requirements and multiple formats. The cell would manage the day-to-day operations of the section, focusing on structuring and collating intelligence products from the division main CP G-2 and tenant units in both the consolidated and support areas. All intelligence production derives from the division main CP G-2 but receives input from the SACP G-2 assessments specific to the consolidated and support areas. The intelligence cell product used for the sustainment confirmation brief incorporates weather, enemy threats, information collection matrix, and common operational picture for the division support area.

Whether selecting core or contributing members, the G-2 intelligence cell at the division SACP must be staffed with the right personnel with the right military occupational specialty (MOS) skills and experience. This requires that we develop a deeper understanding of the experiences and professional background of personnel on the division staff. At least 30 to 60 days before any exercise that uses the SACP intelligence cell, it is recommended to implement a two-pronged approach to educating and training personnel. The first focuses on staff proficiency with a phased methodology emphasizing individual training on MI systems. Collective training on MI systems would follow the Military Intelligence Training Strategy tier certifications. The second focuses on indoctrinating the various stakeholders affected by the division to reduce any friction and to ensure interoperability across the different CP nodes. This includes a communications exercise to test the installed intelligence equipment at least one week before the start of an exercise. In particular, ensuring the G-2 at the SACP has the proper intelligence equipment to support the intelligence cell along with the personnel trained in operating these systems.

Assessment and Feedback

The RAND Corporation summarizes these constraints and challenges in a 2017 research paper that addresses two interrelated Army projects, “Assessing Analytic Proficiency” and “Proficiency Across the All-Source Analyst Career Life Cycle”:

Intelligence analysts, whether in the Army or the broader U.S. intelligence community, face constraints that present significant challenges for their work. Intelligence problems are ambiguous and unstructured, making it difficult to determine whether information to address the problems is adequate and accurate, and they lack objective feedback, which is a key factor in monitoring performance and developing expertise. Analysts also work under time pressure and in a culture in which there is a fear of failure, which limits their ability to conduct analysis using deliberate, systematic thinking processes. Analysts therefore work under conditions in which cognitive biases can pervade analytic thinking and processes. To combat these biases, analysts require cognitive and noncognitive competencies that are largely intangible, such as critical thinking (CT) and adaptability. Senior Army leaders have emphasized the need for such skills (often referred to as 21st-century competencies) in the force at large, particularly in light of an increasingly complex and dynamic operational environment.⁴

The RAND research paper states that the intelligence analysts develop biases because of the work pressure. To address this added work pressure and fear of failure, it is important to develop these MI Soldiers with skills such as predictive analysis and critical thinking besides the MOS training received from Army courses.

Preparing an intelligence analyst to work at the division SACP or any CP node starts with what they learn and experience at garrison. When a junior enlisted Soldier or junior officer is joining a unit, we must learn their background (education, training, and experiences) to focus on the proper individual development plan. If the Soldier is not trained on the unit intelligence systems and not included in an exercise requiring performance under pressure, one can only expect lackluster performance from this Soldier, and ultimately, it can negatively affect the Soldier’s morale and confidence for future assignments or exercises. Not having the proper MI equipment at the division SACP to conduct proper intelligence analysis will affect the mission of the consolidation area. Factoring these important elements into assessments will help us improve our intelligence processes so that they are supporting the empowerment of the MI Soldiers of tomorrow and yielding “quality” products and processes to support the mission of the G-2 intelligence cell at the division SACP.

Conclusion

Effective support area intelligence operations require some centralization of “dedicated” personnel, mission command information systems, and leadership. In his U.S. Army Command and General Staff College master’s thesis, MAJ Brian Chavis explains it best:

The last seventeen years of counterinsurgency operations saw many of the Army's division-level intelligence analysts and equipment remain in static, centralized tactical operations centers to facilitate intelligence support to ground operations....To support large scale combat, intelligence sections must rebalance personnel, capabilities, and equipment across all CPs a division is capable of establishing to enable the survivability of the division's Intelligence Warfighting Function.⁵

To meet the current and future threats of the operational environment that our U.S. military encounters, it is vital to synchronize intelligence operations for a division SACP. ✨

Endnotes

1. Department of the Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 2-37. Change 1 was issued on 6 December 2017.

2. Ibid., 6-10.

3. Department of the Army, FM 6-0, *Commander and Staff Organization and Operations* (Washington, DC: U.S. GPO, 5 May 2014), 1-8–1-9. Change 1 was issued on 11 May 2015. Change 2 was issued on 22 April 2016.

4. Maria C. Lytell, Susan G. Straus, Chad C. Serena, Geoffrey Grimm, James L. Doty III, Jennie W. Wenger, Andrea A. Golay, Andrew M. Naber, Clifford A. Grammich, and Eric S. Fowler, *Assessing Competencies and Proficiency of Army Intelligence Analysts Across the Career Life Cycle* (Santa Monica, CA: RAND Corporation, 2017), 1.

5. Brian D. Chavis, *Fighting for Intelligence: Preparing Division Intelligence Operations for Large Scale Combat* (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 2019), iii.

CPT Julee Thomas serves as G-2 operations officer, 1st Infantry Division. Her professional certifications include Project Management Professional, Certified Plant Maintenance Professional, and Intelligence Fundamentals Professional Certification. CPT Thomas holds a master of civil engineering degree with a focus on project management and more than 20 years prior civilian career experience working in various federal, state, city, and private sectors both in and outside the continental United States.

Vantage Point

Practical Solutions for Today's Intelligence Challenges



Improve your Vantage Point. Vantage Point is a web-based forum designed for publishing content useful to the MI Corps in a more expedited manner than what is published in *Military Intelligence Professional Bulletin* (MIPB). Specifically, Vantage Point is primarily intended for—

- Articles focused on practical solutions to current MI challenges.
- Well-written, but less formal, short- to medium-length articles.
- Unclassified articles but can include CUI content, unlike MIPB.

If you are interested in submitting an article to Vantage Point, please contact the Vantage Point team at usarmy.huachuca.icoe.mbx.doctrine@mail.mil.

Vantage Point is available on IKN at <https://ikn.army.mil/apps/VantagePoint/>.



A U.S. Army Soldier assigned to 1st Battalion, 2nd Stryker Brigade Combat Team, 7th Infantry Division, Joint Base Lewis-McChord, WA, tactically maneuvers during Decisive Action Rotation 20-05 at the National Training Center, Fort Irwin, CA, March 10, 2020.

The Intelligence Warfighting Function in the Division Cavalry Concept

by Captain Jonathan Guelzo

Introduction

In the fall of 2020, I had the privilege of serving as the S-2 of a reconnaissance squadron during a rotation at the National Training Center. The purpose of this exercise, distinct from a typical brigade combat team rotation, was to test the ability of the division staff to rapidly deploy and control the fight from an expeditionary headquarters. In this construct, the division headquarters, division artillery, and combat aviation brigade all physically deployed to the National Training Center. The cavalry squadron received augmentation to replicate the role of a division cavalry squadron and also deployed to the National Training Center. The remaining maneuver battalions of the division's armor brigade combat teams replicated their effects in a constructive environment at home station. This permitted the live execution of a divi-

sion staff exercise and the opportunity to test the division cavalry concept in real time. This article will discuss the experience of operations using new and old equipment within the structure of a reinforced cavalry squadron from the perspective of the intelligence warfighting function.

Task Organization of the Division Cavalry

Organically, the reconnaissance troops included Bradley Fighting Vehicles and M1A2 Abrams main battle tanks. These elements typically fight in a half-troop concept, providing the troop commander with multiple options during ground reconnaissance. The tank troop kept two platoons and remained in a "reconnaissance in-depth" posture to maneuver on friction points. Additionally, the squadron maintained rotary-wing support of AH-64 Apache helicopters

from the combat aviation brigade as well as an element of M109A6 howitzers in direct support from the brigade field artillery battalion. Lastly, the squadron made use of a dismounted scout platoon. The division's frontage represented the squadron's area of operations, with natural gaps between the troops because of terrain and speed of movement. The squadron commander retained two perpetual decision points related to the enemy's exploitation of these gaps. First, commitment of the tank troop to close a gap, and second, commitment of the aerial reconnaissance troop to close another. If direct fires could not achieve coverage of these gaps, targeted indirect fire and artillery-delivered obstacles provided an additional option.

Task Organization of the Intelligence Warfighting Function

Beyond the augmentation of the squadron's combat power, the intelligence warfighting function received support from across the brigade as well. The squadron is authorized multiple officers, noncommissioned officers, and enlisted personnel to support its intelligence efforts. An additional complement of intelligence Soldiers provided the necessary expertise to support both an expanded mission set and the shift requirements necessary to a larger formation. This support element was tailored to directly address anticipated needs prior to the activation of the task force and with oversight from both the brigade and division intelligence sections. The initial plan was to provide a primary cell of intelligence analysts at the tactical operations center (TOC) for both a day and night shift, a team at the combat trains command post to control operations during TOC movements, and one or more officers free to move with the tactical command post (TAC).

At the G-2 level, the entire division staff deployed forward, with the exception of the support area command post, which remained at home station and was responsible for the largely constructive rear fight. The G-2 divided an intelligence package between the division main and the division TAC. The division main, being the larger, fused the bulk of the intelligence reporting from the squadron with that from the other outstations and largely controlled the deep fight. The division TAC took over when the main jumped or during major operational muscle movements and controlled the close fight.

Intelligence Augmentation

Besides the extra personnel for the S-2 section, the intelligence warfighting function received support from the brigade Shadow platoon equipped with the JUMP 20 future tactical unmanned aircraft system for operational evaluation. This aircraft mirrors the capability of the Shadow with several important improvements. First, the system uses a vertical takeoff and landing capability that permits both launch and recovery without an airstrip or a launcher. Second, the system transports in a box on the back of a light medium tactical vehicle. Third, the motor is significantly quieter than that of the Shadow, to the point that we leveraged this as a deception method in conjunction with the Shadow unmanned aircraft system of the aerial reconnaissance troop. Prior to deployment, the squadron's plans incorporated the use of the JUMP 20 forward with launch sites in the vicinity of the TOC and layered with Shadow coverage from the aerial reconnaissance troop.



A U.S. Army Soldier assigned to 1st Engineer Battalion, 1st Infantry Division, conducts an engine start on the JUMP 20 prior to a launch during the future tactical unmanned aircraft system capabilities assessment at Fort Riley, KS, April 8, 2020.

The intelligence warfighting function also received support from the brigade electronic warfare (EW) team, equipped with vehicle-mounted and manpack systems to provide both detection and limited jamming capabilities to the dismounted force during movement. Additionally, the brigade engineer battalion provided vehicle-mounted systems for further signals intelligence (SIGINT). The pre-deployment plan placed the vehicle systems on the flanks for immediate detection alerts over the next intervisibility line.

The manpack system would dismount with the scout platoon, provide priority intelligence requirement confirmation or denial, and serve to queue information collection assets.

Organic Architecture

The squadron has on its modified table of organization and equipment (MTOE) several Command Post of the Future workstations, One Station Remote Viewer Terminals (OSRVTs), and Capability Drop 1 (CD1) laptops. We planned to use all OSRVTs for processing, exploitation, and dissemination of the live streams from the Shadow, JUMP 20, and any Gray Eagle assets available. We provided additional legacy OSRVT systems to each troop to pull video feeds. We also cross-signed additional systems from an adjacent battalion to include Portable Multifunction Workstations and Geospatial Intelligence Workstations for our geospatial intelligence imagery analysts. My intent at the outset was to distribute multiple OSRVTs and CD1 laptops among the TAC, the combat trains command post, and the TOC to provide a baseline intelligence processing capacity at all outstations and retain the Geospatial Intelligence Workstations at the TOC.

Employment of the Intelligence Warfighting Function by Asset

Details about employment of the following assets are described below:

- ◆ Battle tracking.
- ◆ JUMP 20 unmanned aircraft system.
- ◆ EW/SIGINT.
- ◆ U.S. Army Intelligence and Security Command (INSCOM) Cloud Initiative (ICI).
- ◆ CD1.
- ◆ Sensor to shooter (fusion).

Battle Tracking. Given the mission of the squadron to test an experimental concept, use of enablers evolved over time. Because of the coronavirus disease 2019 (COVID-19) precautions, the squadron conducted expeditionary reception, staging, onward movement, and integration and moved to an initial tactical assembly area within the first 5 days. Despite this rapid schedule, the actual training days would not start for some time, so some integration tasks continued on-site. The squadron successfully executed a TOC jump on the first day, demonstrating the ability to set up a fully functional TOC considerably faster than comparable units with the same MTOE strength.

The squadron TOC consisted of four standardized integrated command post tents with workstations along the

walls, a battle table in the center, and the squadron commander's analog battle map displayed on a flat surface. The S-2 occupied a generous portion of the tent to accommodate the number of systems required. Our location gave us close proximity to both the fires cell and the analog map, so data transmissions received on one system could either transmit digitally over the network to another system or pass verbally to the adjacent warfighting function. Analysts managed reports from the higher headquarters via CD1 and the ICI and maintained the Microsoft Excel spreadsheet significant activities log. Numbered entries with corresponding numbered and color-coded icons represented significant activities on the analog battle map, permitting us to quickly identify the decay time of a given report. This process is similar to that described by 1LT Counihan in the April–June 2020 issue of the *Military Intelligence Professional Bulletin*.¹ To man the systems, the intelligence force split across a day and night shift with an officer in charge of each and leaving the squadron S-2 free to support planning efforts with the staff. Finally, the additional personnel offered an opportunity to embed company intelligence support teams with each reconnaissance troop to refine organic reporting.



Photo by Sarah Tate

A U.S. Army Soldier assigned to 1st Engineer Battalion, 1st Infantry Division, conducts flight operations through a laptop-based ground control station during the future tactical unmanned aircraft system capabilities assessment at Fort Riley, KS, April 8, 2020.

JUMP 20 Unmanned Aircraft System. The JUMP 20 represented multiple challenges for the squadron and division to overcome, particularly concerning airspace. On the whole, however, the system worked admirably. We planned to use it in the same manner as the Shadow, but the flexibility of the vertical takeoff and landing capability vastly increased the degree to which we could accommodate our collection plan. The JUMP 20 launched from any area with a suitably flat surface because it is not constrained by the requirement for a hardball surface or existing runway. Additionally, the compact nature of the system allows a relatively small-sized support team to easily pack up and move the system. This allowed more frequent TOC jumps that increased the operational range coverage of the airframe ahead of our forward line of troops. The JUMP 20 has eliminated another common problem—the challenges of communication with the control station without the TOC tethered by relative communication range to the nearest flight line. With the TOC established within communication range of a feasible launch site, a commander’s operational map opens up dramatically without affecting the information collection capability. The bottom line is that the JUMP 20 is a highly versatile system. By the conclusion of the exercise, the JUMP 20 successfully identified the enemy main defensive belt, TOC, and bivouac area. Given that the JUMP 20 operates from any TOC location, however, it is vital that planners incorporate the development of restricted operations zones during the home station military decision-making process to have available launch points plotted across the area of operations. This provides the commander with ready options and prevents delays and interruptions to the information collection plan.

Electronic Warfare/Signals Intelligence. The dismounted EW team deployed with the scout platoon and provided reports that enabled the platoon leader to cue his observation posts for visual observation. While these did not come back to the S-2 section as EW reports, the detail of the scout platoon’s reporting made them a valuable asset. Largely an afterthought in planning before deployment, the scouts quickly became a primary player in the collection role. According to the observer coach/trainers (OC/Ts), this was the first time a section had successfully dismounted and operated a manpack signal interception and jamming system with a scout team at the National Training Center. The vehicle-mounted system also provided accurate reports of enemy activity, which we used to cue the JUMP 20, positively confirming both targets. In addition to the EW systems, the squadron received information from theater-level SIGINT assets that populated reports through the ICI and the ChatSurfer app embedded within ICI. This capabil-

ity provided clarity on the overall disposition of the enemy; however, exercise limitations prevented full employment of the capability, artificially limiting the results, particularly in relation to targeting.

INSCOM Cloud Initiative. ICI’s collective data sourcing helped to quickly establish a picture of the enemy on the battlefield when we first got on the ground. The benefit of having live data in a system and seeing it instantly when turning on a computer cannot be overstated. The squadron was quickly able to identify the general areas of enemy concentration. Even in situations where reports did not fully reflect ground reality, the program served as an effective “heads-up display” to the intelligence planner and the commander. It also provided an excellent depiction of natural lines of drift even when using historical data.

The benefit of ICI is that, as a web-based platform, any computer can run it. As such, it remained open on our CD1 laptops, an easy point of reference when the upper tactical internet ran, and easily minimized and out of the way when it did not. If exercise refinements are possible within ICI, it will be an excellent augmentation of traditional reporting, but it should never fully replace a hardened, offline system.

Capability Drop 1. I found the CD1 system to be excellent; however, the impression I gained when speaking with leaders outside of our organization was that the momentum within the intelligence community is moving us to internet-based systems because of the difficulty experienced at every echelon in maintaining the Intelligence Fusion Server (IFS) stacks. After working with CD1 in a field environment for a month, I think this conclusion is premature for two reasons. First, and more important, is that there is no replacement at the battalion level, so if the upper tactical internet fails, the unit loses connection to web-based platforms. Second, there is not enough data to determine whether it is effective because few units have truly used CD1 in the field. We fielded ours in January 2020, and this was our first opportunity to use it in a major training event. Nevertheless, our OC/Ts told me this was the first time a unit had published an overlay to a higher unit’s IFS, which we did in the first 24 hours. Our motivated warrant officer and talented junior Soldiers proved it could work. They made it talk to fires and showed what an excellent capability it is.

The CD1 in stand-alone mode worked well when the network was down. Battle tracking still occurred, and the common intelligence picture remained up to date. The ability to use the Geospatial Intelligence Workstation and CD1 for planning was excellent. Using imagery on the Geospatial Intelligence Workstation, our geospatial intelligence imagery technician created obstacle overlays of the training



U.S. Army Soldiers rely on the Distributed Common Ground System-Army (DCGS-A) for timely, relevant, and accurate information to understand their operational environment, assess threats, and achieve their missions. DCGS-A consolidates the functions of multiple intelligence, surveillance, reconnaissance, geospatial, and weather systems in a secure, distributed, and collaborative environment.

box on the CD1. This allowed me to provide pre-mission updates to troop commanders and platoon leaders, giving specific information on dead space, intervisibility lines, and elevation. Providing this kind of data gives credibility to the warfighting function and increases the trust a junior officer has in their intelligence support cell. More importantly, it allowed precision targeting for the use of artillery-delivered obstacles. Observing three valleys in the north of the National Training Center box, the Geospatial Intelligence Workstation imagery gave us exact grids for the start and end points of the obstacle belt, preserving ammunition and limiting the occupation time of our guns.

Sensor to Shooter (Fusion). Improvements are always an upshot of any major training exercise, and this one is no different. Our augmented team for this National Training Center exercise, cobbled together from across the brigade, did admirable work as a team without prior operational experience, and the limited issues I encountered were primarily professional growing pains rather than systemic issues. Most of the shortcomings in data processing and transmission at the squadron level are solvable at the brigade level, in the form of the brigade intelligence support element. If the division cavalry squadron continues to be authorized the assets we received for the National Training Center, a separate fusion element must exist to translate this data for the

user. Whether we call it a brigade intelligence support element or something else, it is important to process the information received into actual intelligence before dissemination. It is also important that this information make it into deliverable reports that the intelligence team provides directly to the troops.

In spite of these challenges, by the final 48 hours of the exercise, the intelligence warfighting function reached a new level of fusion. With the JUMP 20 airborne, the geospatial intelligence imagery analysts would identify a target, hold the unmanned aircraft system over it, and pass the grid to an intelligence analyst who would plot it on the CD1. With a click of a button, the analyst generated an electronic fire mission and sent it to the Advanced Field Artillery Tactical Data System (AFATDS) in the fires cell. The

AFATDS operator processed the data, cleared ground with the battle captain, and sent the mission to the guns. The smoothness of the largely automated process prevented unnecessary side chatter in the TOC, reduced the chance of mistakes through manual transmissions of data, and dramatically accelerated the fires process. Key to this is the role of the CD1 as a carrier of actionable intelligence.

Conclusion

Replete with the assets provided to it, the reinforced cavalry squadron is an intimidating force on the modern battlefield. As such, it needs a practiced structure through all warfighting functions. Fortunately, equipment exists to improve this process, and improvement comes with practice and repetition. Critically, this rotation proved that the division cavalry, and specifically the intelligence warfighting function within it, is a viable, feasible, and practicable solution to a division reconnaissance problem. A small intelligence support element proved it could control an unmanned aircraft system platoon at the squadron level in an austere, expeditionary environment. We showed that CD1 is a functional, user-friendly, and fast intelligence processing system. We used EW and SIGINT to cue multiple battlefield assets and improve the enemy assessment. We demonstrated our ability to maintain a common intelligence picture during periods of communications

degradation and in tactically vulnerable locations. Most importantly, given that the squadron developed this structure without a formal written doctrine and staffed it during the COVID-19 pandemic, I am confident in the increasing success of future evolutions of the division cavalry at the National Training Center. ✨

Endnote

1. Christopher K. Counihan, "How to Make Sense of Battlefield Reports Using Analog Methods," *Military Intelligence Professional Bulletin* 46, no. 2 (April–June 2020): 32–35.

CPT Jonathan Guelzo is the squadron S-2 for the 1st Squadron, 4th Cavalry Regiment, 1st Armored Brigade Combat Team, 1st Infantry Division, Fort Riley, KS. Among his previous assignments, he served as an executive officer in the 1st Squadron, 1st Cavalry Regiment, 1st Armored Division, and as a tank platoon leader in the 1st Battalion, 6th Infantry Regiment, 1st Armored Division. His professional education includes the Army Reconnaissance Course and the Cavalry Leader's Course.

U.S. Army photo by SGT Russell Youmans, Operations Group, NTC



A U.S. Army Soldier assigned to 1st Infantry Division, Fort Riley, KS, performs radio operations atop an M1A2 Abrams Tank during Decisive Action Rotation 20-10 at the National Training Center, Fort Irwin, CA, September 20, 2020.

Russia's Military Police and the Syrian Campaign

by Mr. Charles K. Bartles



Russian military police at Khmeimim Air Base in Syria, 11 December 2017.

Introduction

In August 2020, United States officials were dismayed when a video surfaced of an altercation between American and Russian forces near Dayrick, Syria.¹ The video appeared to show a Russian vehicle sideswiping a United States Mine-Resistant Ambush Protected vehicle, reportedly injuring four of our Service members. Another video of the encounter shows a Russian helicopter hovering over American vehicles.² This was not the first time American and Russian patrols in Syria had experienced unfriendly contact. Earlier that year, online observers of the war in Syria were amused and perhaps unsettled by a 45-second video depicting an American armored vehicle running a Russian patrol vehicle off the road.³ Whatever this might say about United States–Russian tensions in Syria, it is interesting that the Russian forces involved in both incidents were not Spetsnaz, elite Airborne Troops, or even standard Ground Forces motorized rifle (infantry) personnel. Instead, these forces were members of Russia's military police, which are taking on a growing role in both Syria and the Russian military. The institution of a military police corps is a relatively new concept for the Russian armed forces, and the path to its establishment has been a long one.

The Soviet and Russian armed forces had no historical experience with an organic military police corps to provide internal security and discipline for service members. The

initial impetus for the formation of an internal security element was a dramatic increase in the number of high-profile *dedovshchina*—brutal hazing that occurred after the collapse of the Soviet Union. This increase was blamed on the Russian military reforms that took place after the collapse of the Soviet Union, which inhibited a commander's right to impose certain punishments—especially extrajudicial jailing. In order to clamp down on *dedovshchina*, embezzlement, and graft (which became increasingly common during the economic crises of the 1990s), the establishment of a military police corps was proposed.

In 2012, after some false starts, General Nikolay Makarov—as chief of the Russian General Staff—announced that by December 1, 2012, military police units would begin operations and that Russia had already established a Defense Ministry main directorate with units in the military districts and the fleets. On March 25, 2015, Presidential Edict Number 161 confirmed the charter that defined the military police structure, functions, and tasks.⁴ The Russian Federation planned to form military police platoons in every brigade and regiment, and the Russian Navy added military police to their force structure. Three years later, 76 such platoons had already been created.⁵

In many respects, this new Russian military police corps is quite similar to its Western counterparts because Russian military police serve as traffic controllers, security guards,

criminal investigators, prison guards, and peacekeepers. However, in the Syrian campaign, Moscow decided to create a new role for the Russian military police—expeditionary peacekeeper. In this capacity, Russian military police are not simply supporting the combat arms (infantry, armor, artillery) but are themselves the main instrument of Russian force projection on the ground in Syria. Interestingly, the military policemen fulfilling this new role are of a very different variety than those serving in the more traditional roles, indicating that two very different organizations may come under the term “Russian military police”—one of which United States troops may encounter more often when operating in areas where both Washington and Moscow deem ground-power force projection important.

Role in the Armed Forces

Russian military police perform a wide range of tasks that are similar to those of United States military police, such as investigating disciplinary and criminal misconduct; operating military jails, route security, and traffic enforcement; conducting facility and personnel security; performing law enforcement activities; promoting good order and discipline in the ranks; and conducting expeditionary security. Russian military police are also an agency of inquiry in the armed forces, which gives them the authority to conduct inquests. In terms of command and control, the approximately 10,000-strong military police originally operated under the authority of the Russian Armed Forces’ prosecutor general and his subordinate military prosecutors; however, the respective military district commander now operationally controls them.⁶ To facilitate this transition of operational control, in March 2019 new positions were created on the military district staffs, such as a deputy chief of staff for military police, with the intent that the position would supervise military police activities. Although operational control of the military police has transferred to the military districts, Russian military police still maintain a close working relationship with the prosecutor’s office. This command and control relationship between the regular military hierarchy and the prosecutor’s office gives the military police special powers, such as the ability to cordon off or blockade military garrisons and areas without consulting the respective unit commander. (Although in practice, this action would almost certainly occur in consultation with the next higher-level unit commander.) This capability underscores the importance of the Russian military police in the Russian system because a Russian commander’s authority has far fewer limitations than his Western counterparts. Responsibility for training and equipping military policemen resides in the military police main directorate of the Russian General Staff.⁷

Russian military police units can now be found in each regiment and brigade of the Military Districts, the Northern Fleet, and Airborne Troops, as well as in a few stand-alone units in the North Caucasus region that were apparently created for the primary purpose of supporting the Syrian campaign. Perhaps one of the more important but less glamorous roles of the Russian military police is that of traffic control. The Russian Federation has extremely high vehicle accident and fatality rates, which decrease military readiness.⁸ The Military Motor Vehicle Inspection Administration, now under Russian military police control, has enforced new preventive measures for personally owned vehicles. This has reportedly contributed to a 7 percent drop in road traffic accidents.⁹



A Russian military policeman of the Central Military District participates in an inspection to determine the state of combat readiness of units, to develop the practice of ensuring security at military sites, and to maintain the skills of possession of firearms.

Training and Equipping

The Russian military police is a type of military occupational specialty, and it is in the process of developing its own training program similar to other branches of arms (such as motorized rifle and engineer). Eventually, it will have a 4-year military academy to educate and train new lieutenants. Contract soldiers (who are somewhat equivalent to the U.S. Army noncommissioned officers) will attend a 2-year 10-month course at the Ryazan Higher Airborne Command School or a shorter course at a regional training facility.¹⁰ In terms of equipping, Russian military police wear distinctive red berets and are typically well equipped to fulfill various missions. Russian military police units may have unmanned aerial vehicles, long-distance mobile communications systems, night-vision devices, and modern thermal imaging devices—depending on mission requirements. In terms of vehicles, they have UAZ Patriot and UAZ-3962 patrol vehicles for garrison operations and have Tigr, Tayfun, and UAZ-394511-03 Yesaul armored vehicles for

expeditionary operations. Maritime-oriented units have the BL-680 patrol boat.¹¹

Russian Military Police as Expeditionary Peacekeepers

Russia's use of peacekeepers in Abkhazia, South Ossetia, and Transnistria has taught Russia that the international community considers the use of military force to be abhorrent but finds it acceptable to use the same military force in the context of peacekeeping.¹² Russia has used peacekeepers or, more accurately, the threat of peacekeepers, in eastern Ukraine to temper Ukrainian efforts to crush the ongoing Russian-sponsored insurgencies in Lugansk and Donetsk. Chief of the Russian General Staff, General Valery Gerasimov, observed that peacekeeping forces could rapidly transition to the open use of force to achieve success in the final stage of a conflict; therefore, it is clear that the Russian leadership sees the value in using its peacekeeping activities for more than foreign internal defense and conflict resolution.¹³

It is no surprise, therefore, that Russia has chosen to invest heavily in "peacekeeping" units. (In Russia, peacekeeping units are often considered elite units and receive some of the best equipment.) This niche has been filled by the Russian Airborne, which has one dedicated peacekeeping brigade (31st Air Assault Brigade at Ulyanovsk) and dedicated battalions in each of the four airborne divisions. In the last few years, Russia has expanded the number of peacekeeping forces by designating dedicated peacekeeping battalions in each of its naval infantry brigades and transitioning the 15th Motorized Rifle Brigade in Samara and the 41st Motorized Rifle Brigade in Kyzyl into peacekeeping units.

In Syria, the Russian military police started filling a new and very high profile role by serving as expeditionary peacekeepers. Interestingly, the Russian military police are in a role that was filled by elite peacekeeping-designated motorized rifle, airborne, or naval infantry units; these units are now rarely mentioned as serving in this capacity. This transition may have something to do with the multilateral nature of how Russia traditionally uses peacekeepers. Russian peacekeeping units are usually associated with supporting specific international organizations, such as the United Nations or the Collective Security Treaty Organization, and

are trained accordingly. The shift in the use of military police as peacekeepers could indicate the Kremlin's greater emphasis upon developing a unilateral expeditionary capability without ties to organizations that require a multilateral consensus. Whatever the reasoning behind the shift in Russia's peacekeeping system, it is clear that Russian military police are taking the lead on this activity in Syria. According to Lieutenant General Vladimir Ivanovsky, Chief of the Military Police Main Directorate of the Russian General Staff, about 60 percent of Russian military police personnel have served in Syria.¹⁴

New Russian Military Police Battalions

One Russian point of concern regarding the Syrian conflict is the large number of Russian citizens who have joined the Islamic state. According to one estimate, at the beginning of 2017, more than 2,000 Russian citizens from

the Caucasus were fighting in Syria. The majority of these people were from Dagestan (1,200 people) and Chechnya (600 people). In December 2015, the Russian Ministry of Internal Affairs and Russian Federal Security Service reported that more than 2,800 Russian citizens were fighting in Syria and Iraq. According to the Russian Ministry of Internal Affairs, by the end of 2015, 899 criminal cases were pending against people returning from Syria.¹⁵ In order to provide sufficient numbers of military policemen to support the Syrian campaign, the Russian Federation has activated two new military police battalions, with approximately 600 personnel each.¹⁶ Considering that at least one of these battalions was reported as simply being



Lieutenant General Vladimir Ivanovsky, Chief of the Military Police Main Directorate of the Russian General Staff, 25 December 2016.

a reflagged Spetsnaz battalion, these new military police battalions likely have more of a direct action mission than the military police platoons in other regiments and brigades, where the focus is on internal security, discipline, and investigations.

Another interesting aspect of the new Russian military police battalions is their location. These battalions have been formed in the same areas where many of the Islamic state fighters have emerged, and in a few cases, both fighter and military policeman are from the same families. This situation has been attributed to a few terrorism-related incidents in the Caucasus, in protest of Russian actions against the Islamic State of Iraq and the Levant.¹⁷ It is difficult to

surmise why the Russians use this recruitment approach to form military police battalions. It may be because military service in the Caucasus is so highly desirable and prestigious that conscription quotas are usually exceeded, resulting in some young men being turned away from compulsory military service. Additionally, the Head of the Chechen Republic, Mr. Ramzan Kadyrov, has stated, “Tatars, Russians, Chechens—together, they protect the Muslims there. They prevent different denominations from setting at variance among themselves.”¹⁸ This implies that both Christians and Muslims from Russia are protecting Syrian Muslims and that these protectors can dissuade some of the ongoing sectarian violence between the Sunni and Alawites. Considering these battalions are already on their fourth rotation in Syria, it seems clear that Russia is deploying these predominately Muslim military police battalions to alleviate religious concerns in Syria and to provide a suitable outlet for the martial cultures found in the Caucasus.¹⁹

Duties of Russian Military Police in Syria

Russian military police units are currently conducting peacekeeping missions, escorting and providing security for humanitarian aid distribution, and performing traffic control operations throughout the Syrian Arab Republic at battalion level and smaller independent units. Their duties in Syria include conducting base security, manning checkpoints and observation posts, monitoring ceasefire agreements, ensuring passage to/from de-escalation and de-confliction zones, performing security patrols, and guarding command posts. The Russian Federation has well publicized its Russian military police humanitarian activities. These activities include escorting United Nations humanitarian convoys and protecting Russian medical units and mobile hospitals when they are rendering medical assistance to the civilian population. There has also been much publicity about their support of mine-clearing units. Military police traffic control activities include enforcing traffic regulations, inspecting registration documents and state license plates, conducting mechanical inspections of military transport vehicles, and providing convoy security.²⁰

Conclusion

The Russian armed forces have shown little interest in emulating United States/Western processes and institutions, as evidenced by their enlisted professionals and special op-

erations forces; however, their military police system may be the exception to this rule. The role of the Russian military police is serving as traffic controllers, security guards, criminal investigators, prison guards, and peacekeepers—duties that are very familiar to military police in the U.S. Armed Forces. Where Russian military police begin to diverge from their Western counterparts is their role as expeditionary peacekeepers. Unlike the West, where military police are typically part of larger peacekeeping formations, in Syria the Russians are using the military police as the primary tool for Russian ground-power force projection. This is a significant change in how Russia has typically conducted peacekeeping operations. Additionally, Russia is not simply deploying existing military police units; it is raising special military battalions with a direct action focus and capability for this specific purpose. This means that Russia appears to be using two very different types of military police. (The military policemen who serve in the platoons assigned to the regiments and brigades have a much different focus than the military policemen who serve in the military police battalions formed in the Caucasus.) Although both types of military police are now serving in Syria, one type functions as a criminal investigator and maintainer of military discipline, while the other focuses on the expeditionary peacekeeping.

If Russia’s experiment with the use of military police as expeditionary peacekeepers and force projectors is deemed successful, this may not be the last time United States troops encounter the red beret and brassard of the Russian military policeman. ✱



Great emblem of Military Police of Russia²¹

Endnotes

1. Rob Lee (@RALee85), “U.S. forces appear to be blocking a road and then attempt to block the path of the Russian patrol (video),” Twitter, August 26, 2020, <https://twitter.com/RALee85/status/1298624477014765572>.
2. Rob Lee (@RALee85), “Russian helicopter hovering over American forces (video),” Twitter, August 26, 2020, <https://twitter.com/RALee85/status/1298581804249681922>.
3. Shawn Snow, “Russian patrol vehicle in clash with US convoy in Syria violated deconfliction rules, OIR says,” Military Times, 20 February 2020, <https://www.militarytimes.com/flashpoints/2020/02/20/centcom-reviewing-road-clash-incident-between-us-and-russian-forces-in-syria/>; and Mohammad (@Mo_Herdem), “US army vehicle pushes Russian police vehicle off the road (video),” Twitter, February 19, 2020, <https://twitter.com/CanShino/status/1230218147938082818>.

4. "Putin Approves Charter for Russian Military Police," Ministry of Defense of the Russian Federation, 27 March 2016, http://function.mil.ru/news_page/country/more.htm?id=12011886@egNews; "Putin Signs Law on Military Police," RIA Novosti, 4 February 2014, http://ria.ru/defense_safety/20140204/992897811.html#ixzz2sMiubPrC; Ivan Safronov and Viktor Khamrayev, "Anatoliy Serdyukov Has Prepared Bill 'On Military Police,'" *Kommersant*, 10 October 2012, <http://www.kommersant.ru/doc/2041082>; and "Three of Five Penal Battalions Disbanded in Russian Armed Forces," Interfax, 21 September 2011.
5. "In 2019 Platoons of Military Police Will Appear in Every Division and Army," *Krasnaya Zvezda*, 21 November 2018, <http://redstar.ru/v-2019-godu-vzvodny-voennoj-politsii-poyavyatsya-v-kazhdoj-divizii-i-armii/>; and Roman Kretsul, Aleksey Ramm, and Aleksey Kozachenko, "Red Berets and Gray Catch: Military Police Will Combat Fishermen Poachers," *Izvestiya*, 12 February 2019, <https://iz.ru/840553/roman-kretcul-aleksei-ramm-aleksei-kozachenko/krasnye-berety-i-seryi-lov-voennaia-politciia-budet-borotsia-s-rybakami-brakonerami>.
6. Yuri Belousov, "Order Will Be Ensured," *Krasnaya Zvezda*, 28 August 2019, <http://redstar.ru/poryadok-budet-obespechen>.
7. Aleksandr Kruglov, Aleksey Ramm, and Bogdan Stepovoy, "Military Police Being Decentralized: Armed Forces Law Enforcement Subdivisions Facing Reform," *Izvestiya*, 5 June 2018, <https://iz.ru/747937/aleksandr-kruglov-aleksei-ramm-bogdan-stepovoi/voennui-politcii-detcentralizuiut>.
8. Ksenia Zubacheva, "Why do so many Russians die on the road?" *Russia Beyond*, 9 April 2019, <https://www.rbth.com/lifestyle/330210-traffic-accidents>.
9. Alexander Tikhonov, "Military Police's Confident Advance," *Krasnaya Zvezda*, 18 February 2019, <http://redstar.ru/uverennaya-postup-voennoj-politsii/>.
10. Alexander Alexanderov, "Military Police: New Challenges," *Krasnaya Zvezda*, 22 February 2017, <http://redstar.ru/index.php/newspaper/item/32349-voennaya-politsiya-novye-zadachi>.
11. Alexander Tikhonov, "Military Police's Confident Advance," *Krasnaya Zvezda*, 18 February 2019, <http://redstar.ru/uverennaya-postup-voennoj-politsii/>.
12. Charles K. Bartles, "Russia's Indirect and Asymmetric Methods as a Response to the New Western Way of War," *Special Operations Journal* 2, no. 1 (June 2016), <https://www.tandfonline.com/doi/full/10.1080/23296151.2016.1134964>.
13. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Voyenno-Promyshlennyy Kuryer*, 26 February 2013, <http://vpk-news.ru/articles/14632>.
14. "60% of Russian military police officers have Syria service record," Interfax, 18 February 2019.
15. Kirill Bulanov, Yevgeniya Kuznetsova, and Polina Khimshiashvili, "Military Police Battalion Sent to Syria from Ingushetia," *RosBiznesConsulting*, 13 February 2017, <https://www.rbc.ru/politics/13/02/2017/58a1c09e9a79475806d0095d>.
16. The structure of these military battalions can vary, but at a minimum, there are three companies (up to 100 servicemen each) plus operational and logistic-support elements. Vladimir Mukhin, "Moscow Is Beefing up the Military Police Contingent in Syria," *Nezavisimaya Gazeta*, 13 January 2019, http://www.ng.ru/world/2019-01-13/2_7480_syria.html.
17. Yelena Milashina, "Attack on Grozny. What Was It?" *Novaya Gazeta*, 20 December 2016, <https://www.novayagazeta.ru/articles/2016/12/20/70958-napadenie-na-grozny-hto-eto-bylo>.
18. "Kadyrov explains why he sends Chechens to Syria," *Crime Russia*, 11 February 2017, <https://en.crimerrussia.com/gover/kadyrov-explained-why-he-sends-chechens-to-syria/>.
19. Mukhin, "Military Police Contingent in Syria."
20. Andrey Ontikov and Aleksey Zabrodin, "Russian Federation Military Police Will Go to Deescalation Zone in Idlib," *Izvestiya*, 11 September 2017, <https://iz.ru/642260/andrei-ontikov/rossiiskaia-voennaia-politciia-otpravitsia-v-zonu-deeskalatsii-v-idlibe>.
21. This image is from the website of the Ministry of Defense of the Russian Federation. Its use is licensed under the Creative Commons Attribution 4.0 International License via Wikimedia Commons.

Mr. Charles Bartles is a Russian analyst and linguist at the Foreign Military Studies Office, Fort Leavenworth, KS. His specific research areas include Russian and Central Asian military force structure, modernization, tactics, officer and enlisted professional development, and Russian military cartography and map symbology. Chuck is also a Space Operations Officer (FA40) in the Army Reserve at U.S. Northern Command/North American Aerospace Defense Command, Colorado Springs, CO. He is currently a doctoral candidate at the University of Missouri-Kansas City. His most recent book is The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces, coauthored with Dr. Lester W. Grau.

344th Military Intelligence Battalion's Tactical Signals Intelligence Training Exercise



U.S. Army photo

344th Military Intelligence Battalion Advanced Individual Training Soldiers practice tactical signals intelligence collection skills at Camp Sentinel, Goodfellow Air Force Base, TX.

**by Mr. Brandon Allen, Mr. Brian Lemaster,
Chief Warrant Officer 4 Christopher Banks,
and Sergeant First Class LeeAnn Seitz**

Introduction

The 344th Military Intelligence Battalion (MI BN) is a driving force of the future in military intelligence. Located at Goodfellow Air Force Base, San Angelo, Texas, the 344th MI BN serves as the Advanced Individual Training (AIT) site for the Army's signals intelligence (SIGINT) military occupational specialties (MOS)—35N (SIGINT Analyst), 35P (SIGINT Voice Interceptor), and 35S (Signals Collector/Analyst). Recently, a realignment of tactical training at Camp Sentinel, Goodfellow Air Force Base, is helping to bridge the training gap between Skill Level 10 institutional and operational training requirements. Conducted in an austere and rigorous environment, this training focuses on the skills and fieldcraft needed for brigade-level SIGINT operations.

During the last 19 years, real-world operations and the Global War on Terrorism focused SIGINT AIT on counterinsurgency operations. At one point, the flash-to-bang of a newly minted SIGINT Analyst or SIGINT Voice Interceptor from graduation to boots on the ground in Iraq or Afghanistan was less than 100 days. Today, in accordance with modern doctrine, the training has shifted from counterinsurgency-centric to multi-domain large-scale ground combat operations. The 344th MI BN provides intelligence Soldiers the foundational, transferable concepts of tactical SIGINT skills while inculcating basic analysis and reporting proficiencies through schoolhouse instruction and tactical operations. Our critical tasks as an organization must meet the Army's operational and force modernization demands

in support of multi-domain large-scale ground combat operations. Based on this premise, delivering quality instruction to Soldiers will provide quality intelligence.

Training Requirements

Within the 344th, SIGINT training requirements fall under two authorities. The driving documents for establishing the program of instruction and subsequent lesson plans come primarily from the National Security Agency's Cryptologic Training System Training Standards and the Army's Individual Critical Task List. The MOS 35N, 35P, and 35S courses are Department of Defense Executive Agency courses. This means that the Executive Agency sets the requirements and appoints a Responsible Training Authority to execute and oversee the implementation of those requirements. For SIGINT analysis and reporting (35N) and cryptologic language analysis (35P), the Air Force is the National Security Agency's Responsible Training Authority. For signals collection and analysis (35S), the Navy is the Responsible Training Authority. This limits the 344th from being able to select training objectives exclusively for Army SIGINT Soldiers.

Additionally, between 65 and 70 percent of all Skill Level 10 MOS 35N and 35P billets in the Army are in U.S. Army Intelligence and Security Command (INSCOM) units. The percentage is even higher for Skill Level 10 MOS 35S billets. As such, the course programs of instruction place a heavy emphasis on strategic-level intelligence tasks and requirements found at INSCOM. All of these critical tasks are institutionally trained. However, the 25 to 30 percent of Soldiers who graduate and go to U.S. Army Forces Command or U.S. Army Special Forces Command assignments desperately need the training and skillcraft associated with both institutional and operational tasks found at brigade-level tactical SIGINT operations. While the Tactical SIGINT/Prophet Course at Fort Huachuca, Arizona, does address some of these training requirements, not every SIGINT Analyst or SIGINT Voice Interceptor attends this course, and the course focuses primarily on giving Soldiers sets and reps on operating the Prophet system. Dismounted, low-level voice intercept or Special Operations Team-Alpha training and fieldcraft associated with multi-domain large-scale ground combat operations do not receive as much emphasis.

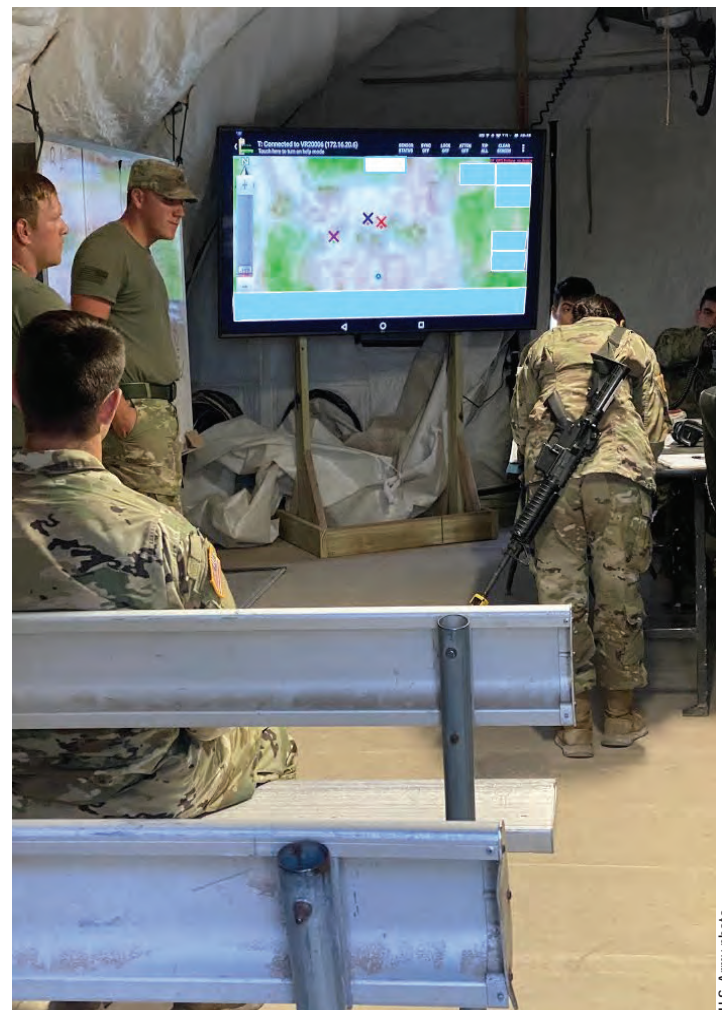
Cadre Training

Cadre arriving at Goodfellow Air Force Base present an array of skillsets in conjunction with their newly assigned roles as AIT instructors. Talent management is key for cadre assignment. For example, in the Basic Analysis and Reporting Course, an interview process with the course manager, chief instructor, and block supervisors determines the specific block of instruction to which a new cadre

member will be assigned based on previous military experience. Often their recent experience and assignment history provide an opportunity for fellow instructors to gain real-world relevant and current information, update their skillsets, and learn the latest application theories. After completing the Air Force Basic Instructor Course and the required Subject Matter Qualification and Initial Qualification Training processes, an instructor is fully qualified to deliver the course material according to the Army University and the Air Education Training Command. When opportunities allow, continual and ongoing education is encouraged and expected because cadre need to remain proficient in their respective skillsets.

Tactical SIGINT Training Concept

To achieve its goal of bringing a more prepared tactical Soldier to the operational force while meeting its institutional requirements, the 344th uses a tactical SIGINT exercise (TSE). This 5-day training event is exclusively developed and resourced by the 344th and its parent organizations.



344th Military Intelligence Battalion Advanced Individual Training Soldiers establish a tactical operations center to provide real-time situational awareness during a tactical signals intelligence exercise at Camp Sentinel, Goodfellow Air Force Base, TX.

U.S. Army photo

The TSE is conducted at Camp Sentinel in Goodfellow Air Force Base's joint training area. The TSE premise attempts to reinforce items from the Individual Critical Task List and Cryptologic Training System Training Standards trained in the classroom, coupled with an introduction to select operational tasks and warrior task and battle drills reinforcement in a scenario-driven, live signals scenario. The training progressively increases rigor and complexity with observer trainers (instructors) using the "crawl-walk-run" training methodology.

In March 2018, the Army Cryptologic Office approved the concept of operations. This perpetuated a series of improvements and evolutions to the unit's field training process that has been virtually continual for the last 2 years. To ensure mission success, the 344th uses a holistic approach for the concept, process, and execution of the training event. As most of us know, a successful training event requires a quality venue, curriculum, personnel, and equipment.

Resources

In its infancy, the 344th TSE had the good fortune of inheriting a well-developed training environment that previously served as the field training exercise. Camp Sentinel and the joint training area provided adequate housing (tent space), a mock-up village that could be used in a variety of scenarios, and multiple semi-improved roads for main supply routes and alternate supply routes. The curriculum is doctrinally based and written in accordance with standards from the U.S. Army Training and Doctrine Command (TRADOC) and Army University. It is tailored specifically to tie items from the Individual Critical Task List or the Cryptologic Training System Training Standards into a field environment for a Skill Level 10 Soldier serving on a SIGINT collection team (SCT) or a cryptologic support team (CST). This "tie-in" is achieved by the most valuable resource—the instructor.

The TSE has benefited from the battalion's and company leadership's focus on talent management. The developer and instructors are uniquely selected based on experience, drive, and assignment history. This ensures relevance and realism and makes learning transfer achievable and enduring. All instructors participate in the Faculty Development and Recognition Program and are evaluated by a U.S. Army Intelligence Center of Excellence (USAICoE)-trained instructional coach. The emphasis on curriculum and instructor standards results in the professional delivery of adult-learner techniques that allows students to synthesize classroom instruction with hands-on application.

The final piece of the training standard is, of course, equipment. The TSE has remained well-equipped and resourced. Serviceable and relevant training apparatuses ensure that

students receive much needed time and repetition on communications and collection systems currently fielded by units in the force. In turn, this produces a more confident and competent Soldier who can contribute expeditiously upon arrival at their first assignment.

Process

On a biweekly basis, MOS 35N students rotate from the schoolhouse to Camp Sentinel. They spend the next 5 days of their training in the field. They deploy to Gorgas where they find themselves as members of a ground collection platoon. There they conduct low-level voice intercept missions near the forward line of troops supporting a brigade combat team that is attempting to clear remnant forces from a Donovanian mechanized infantry battalion and enabling U.S. forces to consolidate gains. Barracks are tents. Meals are meals, ready to eat. Beds are cots. Rucksacks are household goods. Training days are from 0600 for physical training until 2000 when the final element of training for the day is complete.

The first 2 days of training are a blend of cognitive and psychomotor skills on requisite pre-mission training. More than 20 common tasks are introduced or reinforced during this time. Training includes but is not limited to intelligence oversight, map reading, frequency modulation communications, tactical combat casualty care, grenade assault course, and react to contact. Early on day three, students are assigned to small teams. They establish a tactical operations center with CST personnel. Depending on class size, the remaining Soldiers are assigned to three to six SCTs. For the next 3 days they conduct five missions and rotate as teams through a variety of "hide sites" that include a subsurface site, a hasty site, an urban structure, and a roving team. The groups receive an operation order/fragmentary order each morning that describes the mission for that day. Student team leaders employ troop-leading procedures to ensure that all pre-combat checks and inspections are complete and that the team is prepared for the mission and situation.

Observer trainers become increasingly hands-off as students demonstrate proficiency with the equipment, troop-leading procedures, and pre-combat checks. While on mission, students must be able to extract essential elements of information and provide indications and warnings. They are required to apply radio wave theory concepts to improve collection and communication. Ultimately, they will conduct analysis and use direction finding to locate an enemy combatant. They will also use their warrior tasks and battle drills training in a series of opposing force (OPFOR)-related events that include a casualty evacuation, a call for fire, a squad assault, and the clearing of a building.

Collection and analysis drive each of the OPFOR events and, ultimately, determine the outcome.

During the entire mission process, the tactical operations center provides real-time battle tracking via the integrated mesh radios, a large screen display, and an analog map with an overlay. CST members assist the CSTs with intelligence fusion and mission control. They are ready to provide a sanitized “situation update” at any time. This blended concept of SIGINT collection and warrior tasks and battle drills allows cadre to assess the Soldiers’ knowledge, skill, and performance of a wide variety tactical SIGINT tasks.



344th Military Intelligence Battalion Advanced Individual Training Soldiers participate in a grenade assault course as part of a tactical signals intelligence exercise at Camp Sentinel, Goodfellow Air Force Base, TX.

Sustainable and Enduring

While the concept and process have been important for the TSE, the functionality of the course is a necessity to keep it relevant. This is key for training value and the motivation of trainers and trainees. A training event with equipment or facilities that are outdated or unserviceable does not often achieve the intended takeaway. Obviously, new and/or updated equipment in the inventory improves the learning outcome and the transfer of skill to the gaining unit.

In early 2019, the 344th upgraded its collection system training apparatus from a Wolfhound V9 to the Versatile Radio Observation and Direction (VROD) V2. Select units continue to field the highly reliable and capable system across the force as of this writing. Allowing students to train on equipment that their future leaders have not yet trained on increases the students’ ability to contribute upon entry

at their respective units. While the VROD cannot make a claim as a program of record, it does allow for valuable skills training on dependable equipment.

Beyond the “big dollar” equipment, the continual logistics and high throughput of the exercise require a variety of tools—such as all-terrain vehicles, power equipment, communications equipment, simulators, and storage facilities. Prudent requests from cadre, coupled with a willingness to contribute from the battalion, brigade, and Center of Excellence, have directly affected the quality and durability of training.

Internal resources are also a valuable commodity. Cadre for the exercise readily point to the fact that self-resourcefulness has enabled the growth. Observer trainers are responsible for grounds maintenance, facilities maintenance, and any small-level construction projects. The TSE cadre completed many of the recent innovations to the training area. These projects include the 300-meter, seven-obstacle grenade assault course; a two-room military operations in urban terrain (MOUT) house in the pre-mission training area; and a small five-house village that allows for an alternative ending to the prescribed scenario. The combination of this resourcefulness, an actively engaged S-4 section, and contributions by unit and headquarters leadership have made

the exercise functional, but more importantly, sustainable.

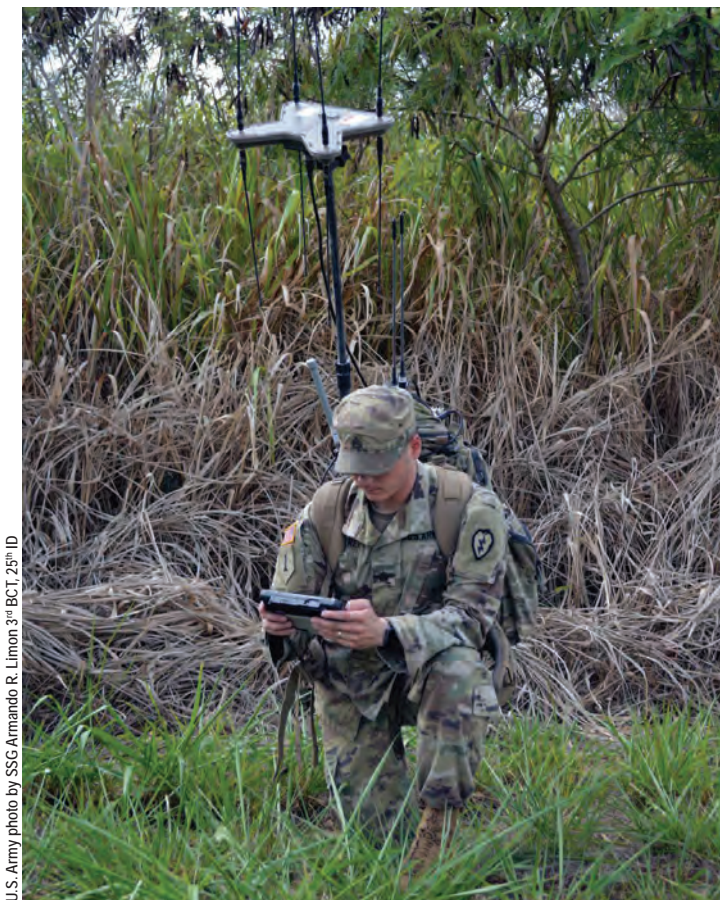
Way Ahead

As the Army shifts from counterinsurgency to multi-domain large-scale ground combat operations, the role of the SIGINT operator will continue to serve as a force-multiplier for commanders. MOS 35N, 35P, and 35S Soldiers will provide tactical, regional, and strategic-level commanders with time-sensitive reporting, indications and warnings, and active SIGINT support. As our potential adversaries change, so will our training to best give decision makers the intelligence needed to win on the battlefield.

MOS 35S Tactical SIGINT Exercise. Incorporating MOS 35S Soldiers into the TSE serves as a new initiative to support the force. As of 1 October 2020, MOS 35S Soldiers attend their AIT at Goodfellow Air Force Base rather than Corry Naval Air Station, Florida. Previously, when MOS 35S training occurred

at Corry Station, only 3 to 5 students started in any one given class, and the program of instruction occurred entirely in a joint service environment with Sailors. There was no program of instruction time for tactical training or even time to practice warrior tasks and battle drills. As a result, TRADOC created a separate 40-hour Warrior Sustainment Course to give MOS 35S Soldiers time to practice and execute warrior tasks and battle drills requirements common to all Soldiers graduating AIT. However, the small class size and limited resources prohibited an austere, robust field training event.

The Warrior Sustainment Course also shifted to Goodfellow Air Force Base with the MOS 35S training. Additionally, because of the need to work with the Air Force and USAICoE registrars, class sizes will be 9 to 10 Soldiers. Having a squad-sized element go through training together not only enables students to participate in a week's worth of warrior tasks and battle drills training but also helps them to integrate seamlessly into the TSE. This provides them hands-on experience with the VRODs and allows them to perform Individual Critical Task List-based institutional and operational signals collection and analysis duties in support of an SCT or a CST alongside MOS 35N Soldiers.



U.S. Army photo by SSG Armando R. Limon 3rd BCT, 25th ID

An electronic warfare specialist receives training on the Versatile Radio Observation and Direction finder on 12 September 2017.

Integrated Training. The move of MOS 35S training to Goodfellow Air Force Base has presented the 344th MI BN with a unique opportunity to mesh and integrate MOS 35N, 35P, and 35S tactical SIGINT training under a single, unified exercise with mutually supportive roles. The MOS 35P schoolhouse is divided into seven separate courses, and six of those are joint with Airmen and Marines. Aligning the limited time available for MOS 35P students to train at Camp Sentinel has proven difficult. However, the SIGINT Voice Interceptor committee has recently developed a course of action to integrate SIGINT Voice Interceptor training into the TSE. As the MOS 35P portion of TSE matures, every MOS 35P student will find themselves participating in an integrated exercise with fellow MOS 35N and 35S Soldiers, or in a stand-alone TSE with MOS 35N injects provided by cadre. In instances where schedules align, MOS 35P collectors in the field will report to MOS 35N CST members who will provide battlefield updates in support of the scenario. When the integration of all three SIGINT specialties is complete in calendar year 2021, it will be the first TSE in AIT in which MOS 35Ns, 35Ps, and 35Ss work together in supporting roles and missions.

This integration of MOS 35N, 35P, and 35S tactical training will also usher in another first—every MOS 35N, 35P, or 35S student who graduates AIT will arrive at their first unit of assignment having had hands-on training on the VRODs. Additionally, all of these Soldiers will have practice and experience performing brigade-level tactical SIGINT operations in an austere and rigorous training environment. This is a great leap from three MOSs with programs of instruction that focused only on strategic-level training and had no, or very little, emphasis on tactical training.

Joint Training. Recent upgrades at Camp Sentinel have also presented opportunities to bring in our joint partners at Goodfellow Air Force Base. The Marine Corps and Air Force have expressed interest in sending their students through the Grenade Assault Course. The smoke, the .50 caliber machine gun simulators, and the artillery simulators bring realism and add rigor and stress that is not often replicated in any AIT. Looking ahead, it is not too difficult to imagine incorporating Air Force lieutenants or Intelligence, Surveillance, and Reconnaissance Course students into our training facility at Camp Sentinel to replicate a joint operations center in support of joint multi-domain large-scale combat operations.

Outreach. As the 344th continues to modify and refine training, we will engage with regional partners such as Fort Hood or Fort Bliss, Texas, to see if they would like to

send their SCTs or CSTs to Goodfellow Air Force Base for training. Building on these successes, we may even engage with the INSCOM Foundry program to gauge their interest

in partnering with the 344th to send Soldiers to some live environment training before deployment downrange or to a combat training center. ✨

Mr. Brandon Allen is a supervisory training specialist (intelligence) for the 344th Military Intelligence Battalion. He is a retired military occupational specialty (MOS) 35Z (Intelligence Senior Sergeant) first sergeant, who spent 22 years working within the U.S. Army Intelligence and Security Command, U.S. Army Special Forces Command (USASFC), and U.S. Army Training and Doctrine Command (TRADOC). He is a graduate of the Department of Defense Executive Leadership Development Program and holds a master's degree in security studies from Angelo State University.

Mr. Brian Lemaster is an MOS 35N (Signals Intelligence [SIGINT] Analyst) training instructor and is currently the block supervisor for the 344th tactical SIGINT exercise. He is a retired MOS 35Z first sergeant who served approximately 16 years of his 20-year career as a member of dismounted SIGINT collection teams in both U.S. Army Forces Command (FORSCOM) and USASFC. He has spent the majority of the last 7 years as a contract or Department of the Army Civilian instructor at Camp Sentinel, Goodfellow Air Force Base, TX.

CW4 Christopher Banks has served as the MOS 35N course manager at Goodfellow Air Force Base, TX, since September 2017. During his 21-year career in the Army, he has had strategic, FORSCOM, and TRADOC assignments, including Fort Meade, MD; Korea; Germany; and the 3rd Infantry Division at Fort Stewart, GA. He has served on multiple deployments as a small teams officer in charge and division SIGINT officer in charge. He holds a bachelor of science in psychology from the University of Maryland University College.

SFC LeeAnn Seitz serves as the chief instructor for the MOS 35N course at Goodfellow Air Force Base, TX. She has also served as a senior instructor and evaluator for the course for over 4 years. She was previously assigned to Fort Meade, MD, as the Foundry noncommissioned officer (NCO) in charge and brigade S-3 training NCO at the 704th Military Intelligence Brigade. She holds a master of public administration from Norwich University.





What is Foundry

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

Funding

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

Foundry Training Types

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

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

Schedules

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



Points of Contact

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



U.S. Soldiers with the 75th Ranger Regiment scale the cliffs at Omaha Beach, Pointe du Hoc, Normandy, France, June 5, 2019, to commemorate the 75th anniversary of Operation Overlord, the World War II Allied invasion of Normandy, commonly known as D-Day. The lessons of World War II still provide valuable insights into how the Army needs to operate now and in future large-scale combat operations.

Deceivingly Decisive: U.S. Army Military Deception and Counterintelligence

by First Lieutenant Will Rector

Introduction

After almost two decades of conducting counterinsurgency operations, the U.S. Army is shifting its focus to prepare for large-scale combat operations. Historical experience suggests that one staff function that will likely play a significant part in such potential conflicts is military deception (MILDEC). For example, the U.S. Army engaged in several MILDEC operations against Axis forces in the European theater of operations during World War II. The success of those operations was due in large part to the support they received from U.S. counterintelligence (CI). Given this historical precedent, this article seeks to answer the question

of what support CI can provide to MILDEC in future large-scale combat operations. The findings suggest that CI capabilities can enable opportunities for MILDEC by denying the adversary knowledge of essential elements of friendly information (EEFI) from both U.S. and multinational partners. Primarily, this includes friendly actions, intentions, and capabilities.¹ Additionally, it suggests CI can provide conduits for MILDEC and feedback indicators for assessing its effectiveness.

To demonstrate this argument, this article will rely largely on the Army's experience in the European theater of operations during World War II. While a limited number of

examples of CI and MILDEC coordination can be found in more contemporary large-scale combat operations, World War II is the optimal case to examine for this purpose. This is mainly because the scale and duration of the conflict provided more opportunities for CI and MILDEC coordination relative to the Army's other historical large-scale combat operations.²

The organization of this article consists of four parts. The first part provides a general overview of MILDEC and CI. The second part discusses CI functions that can support aspects of MILDEC that emphasize denying the adversary true information pertaining to friendly forces. This contrasts with the third part, which discusses CI functions that can support aspects of MILDEC in providing untruths to adversaries about friendly forces. Lastly, the final part provides a summary of the article's findings, recommendations, and implications for the future.

Defining the Concepts

MILDEC is a type of information-related capability that consists of activities designed to mislead adversary decision makers, with the goal of influencing the adversary to take actions that are advantageous to the friendly mission.³ These operations consist of more than a cover plan to conceal the actual friendly plan. Rather, they are actions that influence adversary decision makers by either increasing or decreasing ambiguity about the strength, disposition, intentions, or other information pertaining to friendly forces.⁴ While both goals are acceptable, operations designed to decrease an adversary's ambiguity (i.e., making the adversary think they are certain about the friendly plan) are the optimal of the two because it decreases the adversary's perceived need to collect additional intelligence on friendly forces.⁵ In addition, a MILDEC activity that seeks to confuse or make friendly forces' intentions harder to interpret for the adversary, but does not focus on generating a specific adversary action or inaction, is known as deception in support of operations security (OPSEC).⁶ MILDEC accomplishes these goals by controlling the flow of information or disinformation through intelligence gateways known as conduits. These conduits act as pathways to the adversary for introducing a deception story.⁷

The success of MILDEC relies on two factors: 1) denying the adversary knowledge of the true friendly operation and 2) identifying and leveraging suitable conduits that

are likely to influence adversary decision makers. Moreover, success is more likely when the deception story is mixed with true information and tailored to mesh with the enemy's existing assumptions or interpretations of friendly forces.⁸ If successful, MILDEC has the potential to greatly influence operations on the battlefield. Perhaps the most notable example of successful MILDEC is found in Allied deception activities before the invasion of Western Europe as part of Operation Overlord during World War II. Through MILDEC, the Allies were able to convince the Germans to divert crucial reinforcements to Calais and away from the true objective, Normandy.⁹ As such, these operations are typically highly sophisticated and rely on coordination with multiple staff elements.

In addition to staff elements and liaison officers, MILDEC planners must coordinate with the supporting CI elements. CI is an intelligence discipline that seeks to detect, identify, neutralize, or exploit the activities of foreign intelligence entities (FIE). FIE activities include acquiring U.S. information, blocking or impairing U.S. intelligence collection, influencing U.S. policy, or disrupting U.S. systems and programs.¹⁰ In terms of scope, this article focuses specifically on FIE activities of state actors that target U.S. Army and Department of Defense interests. To execute this mission, Army CI conducts operations, investigations of national security crimes, collection, analysis and production, technical services, and support activities. In a large-scale combat operations context, doctrine and historical experience suggest that



A U.S. Army Counterintelligence Corps agent takes a report from a local French national following the withdrawal of German forces from the area.

Courtesy of the U.S. Army Intelligence and Security Command Historical Collection

during defensive and offensive operations Army CI will be primarily tasked with establishing checkpoints to screen internally displaced persons.¹¹ In addition to internally displaced persons, Army CI will likely screen enemy prisoners of war for any information they might have pertaining to FIE activities. Doctrine and history also suggest that when the Army transitions to stability operations in an area of operations, Army CI will likely conduct investigations and collection activities to counter FIE activities.¹² Like MILDEC, the success of CI activities has major implications for the security of Army operations. For example, the Army counterespionage operation against Clyde Conrad stopped the further compromise of sensitive Army war plans to the Soviet bloc during the late Cold War era.¹³

Outside the four CI mission areas—counterespionage, CI support to force protection, CI support to research and development, and cyber—one aspect of CI that is often overlooked is CI support to MILDEC. To emphasize this role, the following sections discuss how CI can contribute to the success of MILDEC operations.

Denying the Adversary

The first service CI can provide to MILDEC operations is denying the adversary knowledge of friendly forces' EEFI. CI can achieve this by promoting OPSEC as well as conducting CI operations and investigations that exploit and/or neutralize FIE activities. OPSEC is crucial to the success of MILDEC operations because it limits FIE ability to accurately identify actual friendly intentions and protects operations from being compromised. Effective OPSEC ensures security measures are in place to limit the amount of mission-critical information that the adversary can observe and collect on that is contradictory to the deception story.¹⁴ To support this effort, Army CI conducts Covering Agent Program activities. These activities mitigate threat collection efforts by promoting OPSEC and increase vigilance by providing CI Threat Awareness and Reporting Program briefings to Army personnel. These briefs are essential for educating Soldiers on how to identify indicators of FIE and insider threat activities to protect critical EEFI pertaining to friendly actions, intentions, and capabilities.¹⁵ In addition, CI capabilities briefs inform local commanders, security managers, and other leadership in the area of operations about what support CI can provide them. Furthermore, an effective Covering Agent Program can advise supported units of the FIE threat and assist them in developing threat reporting awareness and relationships.¹⁶

Despite efforts to enhance Threat Awareness and Reporting Program measures, widespread accessibility to smartphones and wireless internet access poses chal-

lenges to maintaining adequate OPSEC in the contemporary operational environment. In 2018, several media outlets identified the location of United States forces operating in Afghanistan by leveraging a popular running app.¹⁷ Similarly, open-source analysis leveraged social media to identify Russian soldiers deployed in eastern Ukraine in 2015.¹⁸ Such examples demonstrate that the Army will likely face considerable difficulties in maintaining OPSEC in future large-scale combat operations. Because FIE can easily take advantage of such situations, adequate CI assets are essential for investigating any potentially damaging lapses in OPSEC. To this end, CI can support MILDEC in large-scale combat operations by neutralizing FIE human intelligence efforts to collect on friendly forces. By investigating espionage and other related national security crimes, CI can deny the adversary knowledge of EEFI and thereby protect the deception story.

Deceiving the Adversary

A second service that CI can provide to MILDEC operations in large-scale combat operations is identifying and leveraging suitable conduits for the deception story. Allied deception conduits in World War II included using technical means such as false signal communications and decoy or "dummy" units, in addition to human means such as controlled enemy agents (CEA).¹⁹ While technical means were highly successful in the execution of MILDEC in World War II, adversary capabilities may limit their effectiveness in future large-scale combat operations. For instance, adversaries such as Russia have heavily invested in electronic warfare capabilities to counter the United States Army's superior technical-communications infrastructure.²⁰ If the Army is unable to emit signals for real communications, it is unlikely it will be able to do so for false communications. As a result, these systems have the potential to disrupt not only U.S. maneuver operations but also MILDEC operations. The implication of such adversary capabilities is that MILDEC conduits that rely on technical means such as false communications may not be available to the Army in a large-scale combat operations environment. In such a scenario, the Army may need to rely on low-technology means, such as CEAs, for establishing MILDEC conduits.

In World War II, the Army was successful in establishing low-technology conduits for MILDEC by using CEAs.²¹ CEAs were FIE-tasked human sources that Allied CI leveraged to operate on behalf of friendly forces via the following process. FIE typically tasked human sources to operate in friendly controlled areas as "stay-behind" agents. Once in place, these enemy agents would collect on friendly forces and send their reports back to FIE via radio transmission. Upon detecting and arresting enemy agents for espionage



U.S. Army military deception units position dummy tanks as part of Operation Fortitude in preparation for the invasion of Normandy.

or sabotage, local Army CI detachments screened them to determine whether they possessed the potential for use as a CEA.²² If they identified an individual with such potential, the CI detachment transferred the enemy agent to the custody of the Special Counterintelligence detachment.²³ These units consisted of a team of officers from the X-2 (not to be confused with the Army 2X staff position) section of the Office of Strategic Services that were attached to an Army Group headquarters.²⁴ If the Special Counterintelligence detachment determined that the enemy agent was suitable, it would task him or her with feeding the adversary disinformation to FIE as a CEA.²⁵ Such operations were particularly aggressive in nature relative to deception in support of OPSEC in that they sought to influence the adversary's actions. As X-2 historian Timothy Naftali explains:

With [CEAs] under your control you could supply your enemy with information of your own choosing. Assuming you could prevent him from forming a word-picture from uncontrolled sources—air reconnaissance, signals interception, etc.—then manipulation of his assessments of the military, political and diplomatic situation lay within your grasp. Moreover, under these conditions, there was the opportunity to compel him to take steps that would materially improve your own situation, by weakening his.²⁶

Naftali's assessment suggests FIE can be a useful conduit for passing disinformation as part of a deception story. This

is largely because they constitute the adversary's primary means of obtaining knowledge of the true friendly plan.²⁷ Therefore, CEA operations are more likely to be successful when CI can prevent or neutralize FIE recruitment of non-CEA (i.e., uncontrolled) penetrations among Army personnel that could result in the adversary's collection of EEFI.²⁸

An example of the use of CEAs in World War II MILDEC operations is Operation Jessica. This MILDEC operation from late 1944 to early 1945 intended to deceive German decision makers into retaining a substantial force along the Franco-Italian border rather than commit them as reinforcements to other fronts.²⁹ To support this operation, Special Counterintelligence detachments leveraged CEAs within the network they had developed in

France. Two specific CEAs, Paul Jeannin and a source codenamed FOREST, provided false reports to German intelligence pertaining to troop movements and other information that would indicate preparations for an Allied offensive in northern Italy.³⁰ Through these efforts, at least two German divisions badly needed elsewhere were held on the Italian front.³¹ Thus, in this capacity, Army Group Special Counterintelligence detachments successfully exploited CEAs to support MILDEC operations during World War II.³²

Since effective deception stories typically use multiple conduits, relying on a single conduit is not optimal but nonetheless may be the most practical choice depending on the difficulty of penetrating the target.³³ When the operational environment negatively impacts the number of available conduits for MILDEC, CI can provide a low-cost and low-technology method of providing the adversary decision makers with disinformation through the use of sources similar to the World War II-era CEAs.³⁴ Furthermore, these types of sources provide CI the ability to assess whether the adversary has accepted the MILDEC disinformation as truth, as well as other critical information about friendly forces of which the adversary is aware.³⁵ Based on this assessment, CI can also analyze and assess what information the FIE

tasked the CEA to collect. This in turn provides a feedback indicator for MILDEC planners to determine if the deception story is effectively influencing the adversary's perception of friendly forces.

Conclusion and Recommendations

MILDEC faces several challenges as the Army shifts from fighting counterinsurgencies to large-scale combat operations in the contemporary operational environment. Historical experience suggests active and aggressive CI support to MILDEC can help resolve some of these challenges. Particularly, this article has devoted much of its discussion to how FIE can influence MILDEC operations. Since engaging FIE is primarily a CI mission, it is essential that MILDEC planners leverage and coordinate with Army CI.

As one of the initial steps to increase coordination between these disciplines, this article recommends that CI support to MILDEC be designated as an additional/fifth CI mission area. The support CI can provide MILDEC includes denying FIE the ability to collect intelligence on friendly forces while simultaneously providing FIE disinformation to propagate a deception story. As this article discussed, CI support significantly contributed to the success of MILDEC operations in World War II. If the Army can learn from such lessons and implement them in how it plans to fight in future conflicts, it will be better prepared to operate in complex large-scale combat operations. ✨



Courtesy of the U.S. Army Intelligence and Security Command Historical Collection

Army Counterintelligence Corps agents searching for items of intelligence value among captured German documents.

Endnotes

1. Department of the Army, Field Manual (FM) 3-13.4, *Army Support to Military Deception* (Washington DC: U.S. Government Publishing Office [GPO], 26 February 2019), 1-5.
2. For a limited discussion of U.S. Army counterintelligence support to military deception in the Gulf War, see Douglas L. Tystad, *The Role of the Media in the Operational Deception Plan for Operation Desert Storm* (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army Command and General Staff College, 3 April 1992), 20, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a258285.pdf>.
3. Department of the Army, FM 3-13.4, *Army Support to Military Deception*, 1-1.
4. Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception* (New York: Pergamon Press, 1981), 5.
5. Robert M. Clark and William L. Mitchell, *Deception: Counterdeception and Counterintelligence* (London: Sage Publications, 2019), 13.
6. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-13.4, *Military Deception* (Washington, DC: The Joint Staff, 26 January 2012), I-2.
7. Ibid., viii.
8. Daniel and Herbig, *Strategic Military Deception*, 42.
9. Jonathan Gawne, *Ghosts of the ETO: American Tactical Deception Units in the European Theater, 1944-1945* (Havertown, PA: Casemate, 2014), 12.
10. Department of the Army, Army Techniques Publication (ATP) 2-22.2-1, *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)* (Washington, DC: U.S. GPO, 11 December 2015), Glossary-4 (common access card login required).
11. U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: Volume XV* (Fort Holabird, MD: U.S. Army Intelligence Center, 1959), 22.
12. John Schwartzwalder, *We Caught Spies: A History of the U.S. Army's Counterintelligence Corps* (New York: Duell, Sloan and Pearce, 1946), 108.
13. For an exceptional account of the Conrad case from the U.S. Army's perspective, see Stuart Herrington, *Traitors Among Us: Inside the Spy Catcher's World* (Novato, CA: Presidio Press, 1999).
14. Office of the Chairman of the Joint Chiefs of Staff, JP 3-13, *Information Operations* (Washington, DC: The Joint Staff, 27 November 2012), II-12. Change 1 was issued on 20 November 2014.
15. Department of the Army, Army Regulation 381-12, *Threat Awareness and Reporting Program* (Washington, DC: U.S. GPO, 1 June 2016).
16. Department of the Army, ATP 2-22.2-1, *Counterintelligence Volume I*, 2-2.
17. Alex Hern, "Fitness tracking app Strava gives away location of secret US army bases," *Guardian*, January 28, 2018, <https://www.theguardian.com/>

[world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases](https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases).

18. Dmitry Volchek and Claire Bigg, "Ukrainian bloggers use social media to track Russian soldiers fighting in east," *Guardian*, June 3, 2015, <https://www.theguardian.com/world/2015/jun/03/bloggers-social-media-russian-soldiers-fighting-in-ukraine>.

19. Donald J. Bacon, "Second World War Deception" (master's thesis, Air Command and Staff College, 1998), 20.

20. Asymmetric Warfare Group, *Russian New Generation Warfare Handbook* (Washington, DC: U.S. GPO, 2017), 17.

21. Robert Cowden, "OSS Double-Agent Operations in World War II," *Studies in Intelligence* 58, no. 2 (2014): 65.

22. U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: Volume XVIII* (Fort Holabird, MD: U.S. Army Intelligence Center, 1959), 85.

23. Ibid.

24. George C. Chalou, *The Counter Intelligence Corps in Action* (New York: Garland, 1989), 290.

25. U.S. Army Intelligence Center, *History of the Counter Intelligence Corps: Volume XVI* (Fort Holabird, MD: U.S. Army Intelligence Center, 1959), 8.

26. Timothy Naftali, "X-2 and the Apprenticeship of American Counterespionage 1942-1944" (PhD diss., Harvard University, 1993), 3.

27. Clark and Mitchell, *Deception*, 13.

28. Abram Shulsky, "Elements of Strategic Denial and Deception," *Trends in Organized Crime* 6, no. 1 (2000): 22.

29. Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Skyhorse Publishing, 2007), 650.

30. Cowden, "OSS Double-Agent Operations," 70.

31. Ibid., 71.

32. William Hood, "Angleton's World: Lessons for U.S. Counterintelligence," in *U.S. Intelligence at the Crossroads*, ed. Ernest May, Roy Godson, and Gary Schmitt (New York: Potomac Books, 1995), 74.

33. Department of the Army, FM 3-13.4, *Army Support to Military Deception*, 2-10.

34. Robert W. Stephan, *Stalin's Secret War: Soviet Counterintelligence against the Nazis, 1941-1945* (Lawrence, KS: University Press of Kansas, 2003), 13-14.

35. Michael I. Handel, "Intelligence and Deception," *Journal of Strategic Studies* 5, no. 1 (1982): 126.

1LT Will Rector is the executive officer of Charlie Company, 301st Military Intelligence Battalion, where he was previously the counterintelligence platoon leader. He is a Ph.D. candidate in political science at Arizona State University. He holds a master's degree in security studies and a bachelor's degree in international relations and German.

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



APD | ARMY PUBLISHING
DIRECTORATE

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

-or-



Directorate of Training

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

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

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



Soldiers and Civilians of the 389th Military Intelligence Battalion (Special Operations) (Airborne) pose for a group picture after the unit activation ceremony on 16 September 2019.

1st Special Forces Command Has a Military Intelligence Battalion

by Lieutenant Colonel Sapriya Childs

Introduction

Did you know that 1st Special Forces Command has a military intelligence (MI) battalion? This was the rollout question on the 1st Special Forces Command's Facebook and Twitter 5 months after the battalion's activation on September 16, 2019. It was the question that officers asked as they saw this new unit in the Assignment Interactive Module cycle. Soldiers and noncommissioned officers asked the same question when they received orders to the 528th Sustainment Brigade.¹ What was missing in the question, and on those orders, was that the 389th MI Battalion (Special Operations)(Airborne) has, since 2015, been building toward the day we would officially get our numerical designation and be doctrinally tasked as the operational intelligence arm for the 1st Special Forces Command.²

"Illuminate to Action"

Many have asked, "Why build an MI battalion in the 1st Special Forces Command when each Army special operations forces element has organic intelligence at the group/brigade and below?"³ The answer is *connection*. In today's competitive global environment, with a greater focus on peer and near-peer adversaries, the command was missing

an operational intelligence connector to bridge the seams across regions where our adversaries operate and a dedicated reach-back structure to connect with the rest of the intelligence community, interagency, Army, and joint special operations forces. ADP 3-05, *Army Special Operations*, describes the 389th MI Battalion as the "nexus for continental United States-based intelligence support, integrating the efforts of each U.S. Army Special Operations Command component...support for the full range of missions."⁴

In comparison to other MI formations across the Army, think of the 389th as the expeditionary-MI brigade of the 1st Special Forces Command, with the worldwide coverage and regional alignment requirements of each MI brigade-theater. Our motto is "Illuminate to Action," symbolizing the purpose of our mission to highlight transregional threat activity and inform Army special operations forces' decision makers. We execute that mission through four complementary lines of effort:

- ◆ Line of Effort One: Provide intelligence support to the component subordinate units.
- ◆ Line of Effort Two: Serve as the core intelligence element of a special operations joint task force contingency.

- ◆ Line of Effort Three: Develop the processing, exploitation, and dissemination (PED) platform for Army special operations.
- ◆ Line of Effort Four: Conduct intelligence training and support standardization of intelligence support to Army special operations forces.

Line of Effort One

Provide intelligence support to the component subordinate units. This line of effort is the most dynamic. We provide tailorable support to the Special Forces Groups, Psychological Operations Groups, and Civil Affairs brigade whenever and however they require. This support includes connecting regional Special Forces elements to intelligence community and interagency analysts and providing specialized reach-back support and/or individual deployment augmentation. Recently, the battalion transitioned to building capacity for continental United States–based intelligence support to information operations through the newly established Information Warfare Center under the 8th Psychological Operations Group.

Line of Effort Two

Serve as the core intelligence element of a special operations joint task force contingency. In this capacity, the battalion stands trained and ready to support the 1st Special Forces Command G-2's transformation into the joint intelligence element for a two-star-level operational special operations forces headquarters. This requires a constant awareness of global instability factors, threat activity, and pre-established connections and relationships to the intelligence community and theater special operations commands.

Line of Effort Three


Develop the PED platform for Army special operations. The 389th serves as the foundational PED capability for the U.S. Army Special Operations Command. Aligned against the Gray Eagles from the 160th Special Operations Aviation Regiment, we are growing this capability in conjunction, and cooperatively, with the joint special operations forces and Army PED enterprise. We are building the baseline for PED expansion and evolution, incorporating data science and artificial intelligence to synchronize intelligence from all sensors (aerial to human).

Line of Effort Four

Conduct intelligence training and support standardization of intelligence support to Army special operations forces. We built this effort on the back of the Special Warfare Signals Intelligence (SIGINT) Course, a baseline training for tactical SIGINT elements within the Special Forces Groups. We will expand in this line of effort to support the U.S. Army Special Operations Command's codification and implementation of the Army special operations forces' Military Intelligence Training Strategy, as well as development of the intelligence training pathway for intelligence support to information operations. Our goal is to build lasting relationships between the U.S. Army Intelligence Center of Excellence and the U.S. Army John F. Kennedy Special Warfare Center and School, capturing Army special operations forces' intelligence requirements in Army and joint multi-domain doctrine.

Conclusion

So, yes, the 1st Special Forces Command has an MI battalion. With our core values of delivering quality, reliability, collaboration, flexibility, professionalism, and learning and growing, we stand ready to evolve, as the environment evolves, in support of the regiment. **Illuminate to Action!**

For inquiries or to contact the 389th Military Intelligence Battalion (Special Operations) (Airborne), email 389th.MI.BN.Leadership@socom.mil. 

Endnotes

1. The 389th Military Intelligence Battalion is the operational intelligence arm for the 1st Special Forces Command and is subordinate to the 528th Sustainment Brigade (Special Operations) (Airborne).
2. For more history, see Christopher E. Howard, "From Leyte to the Levant: A Brief History of the 389th Military Intelligence Battalion (Airborne)," *Veritas* 15, no. 1 (2019). Available at https://arsof-history.org/articles/19_aug_389_leyte_to_levant_page_1.html.
3. The 1st Special Forces Command is the division-level headquarters for the Army's seven Special Forces Groups, two Psychological Operations Groups, and the Civil Affairs brigade. These units are regionally aligned and have varying numbers of intelligence Soldiers providing tactical intelligence support from the team level to the group/brigade headquarters. These elements serve as the base intelligence capability; when deployed, they often require additional augmentation.
4. Department of the Army, Army Doctrine Publication 3-05, *Army Special Operations* (Washington, DC: U.S. Government Publishing Office, 31 July 2019), 5-4. Change 1 was issued on 26 August 2019.

LTC Sapriya Childs served as the 389th Military Intelligence Battalion Commander from August 2018 to June 2021. She held numerous positions in the Army and special operations tactical and operational forces. Her intelligence assignment highlights include 17th Combat Sustainment Support Battalion S-2; military intelligence company commander, 3rd Brigade Combat Team, 3rd Infantry Division; signals intelligence officer, Department of the Army G-2 Staff; Army Geospatial Intelligence Battalion executive officer; and Joint Intelligence Support Element Chief, Special Operations Joint Task Force-Afghanistan. LTC Childs is a graduate of the National Intelligence University.

ATP 2-19.4,

Brigade Combat Team Intelligence Techniques: The Update

Introduction

It is vital that the U.S. Army maintain readiness by being manned, trained, and equipped to respond to the most significant readiness requirement, conducting large-scale ground combat operations against a peer threat. ATP 2-19.4, *Brigade Combat Team Intelligence Techniques*, is the Army's doctrinal publication describing those techniques that the brigade combat team's (BCT) intelligence warfighting function uses when providing intelligence support to BCT operations. The techniques described in this publication, published 25 June 2021, apply across the Army strategic roles, with an emphasis on large-scale ground combat at echelons brigade and below within the infantry, armored, and Stryker BCTs. Intelligence Soldiers are highly encouraged to use the baseline information contained in ATP 2-19.4 while tailoring it to their specific unit and mission.

ATP 2-19.4 focuses on large-scale ground combat operations that require the BCT intelligence warfighting function to conduct intelligence operations continuously in order to provide commanders and staffs with detailed knowledge of threat strengths, vulnerabilities, organizations, equipment, capabilities, and tactics. This information enables commanders to plan for and execute operations.

In order to ensure successful operations, BCT commanders require intelligence about the enemy and other conditions of the operational environment (OE). Intelligence assists commanders in the tasks of visualizing the OE, organizing forces, and executing operations to achieve the desired tactical objectives or end state. As

an element of visualizing the OE, intelligence supports the commander by providing situational understanding of the threat and predicting possible threat courses of action. In regard to the most significant readiness requirement, 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.

The information contained in ATP 2-19.4 provides the doctrinal duties and responsibilities of the BCT intelligence

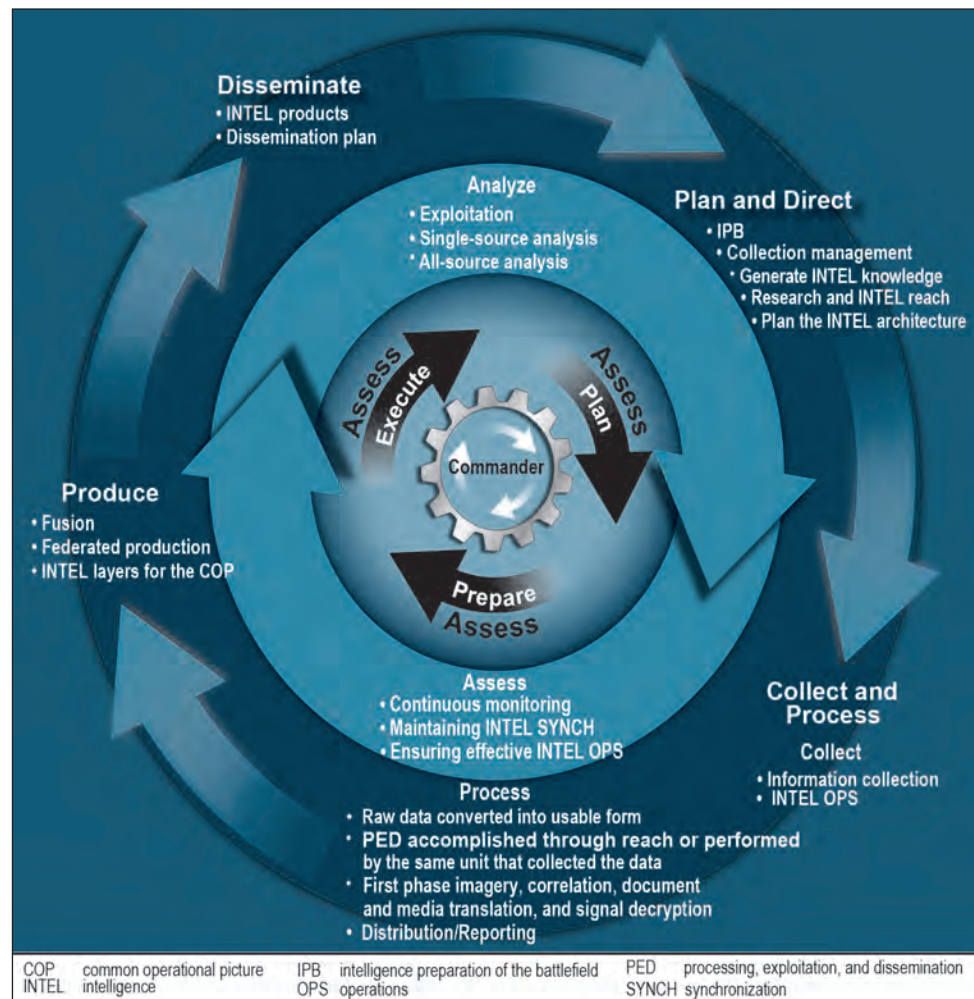


Figure 1. Integrating Intelligence into the Operations Process

warfighting function and describes the intelligence process within the context of the operations process (Figure 1). The goal of the ATP 2-19.4 update is to empower those intelligence Soldiers with the knowledge necessary to provide effective intelligence support to the BCT.

A New Focus

The Army updated its foundational doctrine to reset the focus on large-scale ground combat operations against a peer threat. This shift in Army doctrine, as well as updates to BCT intelligence capabilities, organizations, and structure, was the main driving force behind the update to this Army techniques publication. In order to maintain consistency with validated Army doctrine, ATP 2-19.4 covers—

- ◆ BCT intelligence support to the warfighter through the Army's strategic roles.
- ◆ BCT intelligence support to the operations process.
- ◆ Updated verbiage to ensure consistency with operations and intelligence doctrine and terminology.
- ◆ BCT intelligence considerations such as training; pre-deployment preparation; BCT intelligence architecture and the related topic of primary, alternate, contingency, and emergency (known as PACE) planning; collection management; and targeting.

The update to ATP 2-19.4 contains seven chapters and four appendices outlined below:

- ◆ **Chapter 1** overviews the Army's operational concept of unified land operations and the OE. It also provides an overview of the BCT's intelligence warfighting function and its support to the operations process.
- ◆ **Chapter 2** describes the roles, functions, and structures of BCT intelligence organizations.
- ◆ **Chapter 3** discusses BCT intelligence techniques during the plan and prepare activities of the operations process.
- ◆ **Chapter 4** discusses BCT intelligence techniques during the execute and assess activities of the operations process.
- ◆ **Chapter 5** details BCT intelligence during competition below armed conflict.
- ◆ **Chapter 6** details BCT intelligence during prevail in large-scale ground combat operations in addition to challenges and mitigations during this Army strategic role.
- ◆ **Chapter 7** discusses BCT intelligence during operations to consolidate gains.

- ◆ **Appendix A** discusses intelligence training, the Military Intelligence Training Strategy (MITS), and the intent and execution of each tier within the MITS certification.
- ◆ **Appendix B** describes techniques for predeployment preparation and training of intelligence Soldiers.
- ◆ **Appendix C** discusses the intelligence architecture and communications networks.
- ◆ **Appendix D** overviews intelligence support to targeting for BCTs.

ATP 2-19.4 was last published in 2015. This update describes doctrinal techniques and force redesigns that include new capabilities, organizations, and structures of brigade and below intelligence elements as well as the latest concept of operation for the BCT's military intelligence (MI) company. The MI company is designed to support the various requirements placed on the infantry, armored, and Stryker BCTs. The update to ATP 2-19.4 removes old constructs such as the company intelligence support team and multifunctional platoon, as well as other items that were necessary in facilitating successful counterinsurgency operations. These old constructs are replaced by new concepts designed to help the BCT in large-scale ground combat operations.

The Army techniques publication update now includes force design revisions that resulted from the 2016 MI Bottom Up Review (BUR) conducted by the U.S. Army Intelligence Center of Excellence (USAICoE) and the Army G-2. During this BUR, USAICoE and the Army G-2 analyzed MI capabilities across the Army's three components through the lens of competing against peer threats and the multi-domain operations concept. The review validated the following requirements:

- ◆ Rapid detection, identification, and dissemination of threat high-payoff targets are essential to the timely targeting required to dis-integrate threat antiaccess and area denial.
- ◆ Realignment of the internal MI company structure is required to enable the MI company to support BCT operations in multiple domains.

The doctrinal techniques and force design updates contained in ATP 2-19.4 address how the MI company and BCT intelligence elements meet the challenges of multi-domain operations and the information environment. Figure 2 (on the next page) shows the new structure of the MI company.

A significant aspect of meeting the challenges of multi-domain operations and the information environment is the integration of signals intelligence (SIGINT) and electronic

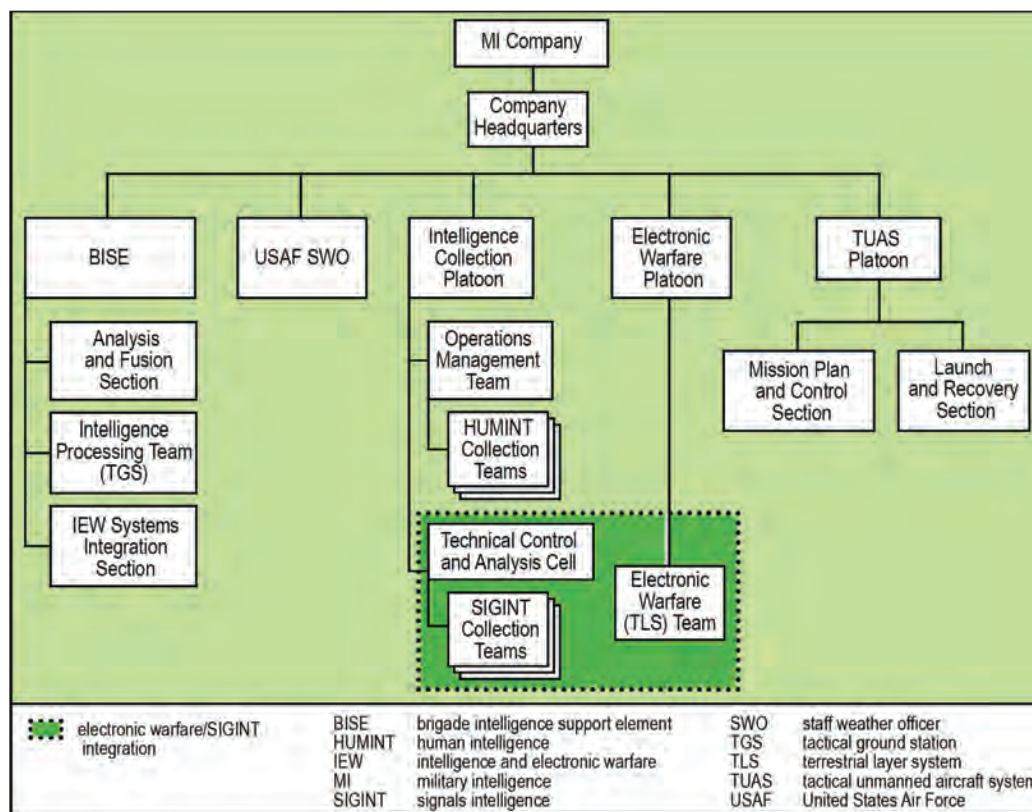


Figure 2. New Structure of the Military Intelligence Company

warfare teams with oversight by the reintroduction of technical control and analysis cells. SIGINT shares close linkages with, and provides much of the foundational intelligence to enable, cyberspace, electromagnetic warfare, and information operations. The ATP 2-19.4 update describes the purpose of integrating electromagnetic warfare with SIGINT—providing complementary capabilities that can result in the following:

- ◆ Recommendations of advantageous terrain for the employment of SIGINT and electromagnetic warfare assets. This is essential to obtain an unobstructed line of sight to suspected enemy emitters.
- ◆ Communications and non-communications emitter mapping across the electromagnetic spectrum for the commander.
- ◆ Options to disrupt enemy signals for the commander.

Other Key Additions

ATP 2-19.4 begins by explaining foundational concepts that intelligence Soldiers should comprehend in order to understand how they fit into the bigger Army picture and why their roles are vital to BCT operations. These basic concepts include an explanation of the BCT, the Army's operational concept of unified land operations, the OE, the Army's strategic roles, decisive actions, and the BCT's

intelligence warfighting function. Also included is a description of how the intelligence warfighting function supports the operations process through the intelligence process. These concepts provide the framework that readers need to progress through the rest of ATP 2-19.4.

In order to help reader understanding, recent intelligence publications have included a tailored graphic displaying a logic map with an overview of the key concepts and processes. It also shows how these pieces fit together. In the same light as these recent publications, ATP 2-19.4 also provides a graphical logic map in the first chapter (Figure 3, on the next page). The purpose of this graphic is to show where BCT intelligence elements fit and how BCT intelligence

elements collaborate with higher-level organizations. In order to maintain consistency throughout the other echelon publications, this same graphic style will also be used in the other intelligence echelon publications, such as ATP 2-19.1, *Echelons Above Corps Intelligence Organizations*, and ATP 2-19.3, *Corps and Division Intelligence Techniques*. The purpose of having this graphical logic chart in the echelon publications is to ensure a common thread exists among them, with each emphasizing the unique aspects of intelligence support at that echelon.

Other key additions to ATP 2-19.4 support the most significant readiness requirement. These additions include the various challenges facing the BCT intelligence warfighting function during large-scale ground combat operations. Challenges discussed in the Army techniques publication that are summarized in the following paragraphs include—

- ◆ Intelligence-on-the-move.
- ◆ Maneuverable intelligence nodes.
- ◆ Degraded information environments.
- ◆ PACE planning.

Intelligence-on-the-Move

ATP 2-19.4 introduces intelligence-on-the-move and its potential effect on intelligence operations. Fighting for intelligence during large-scale ground combat operations

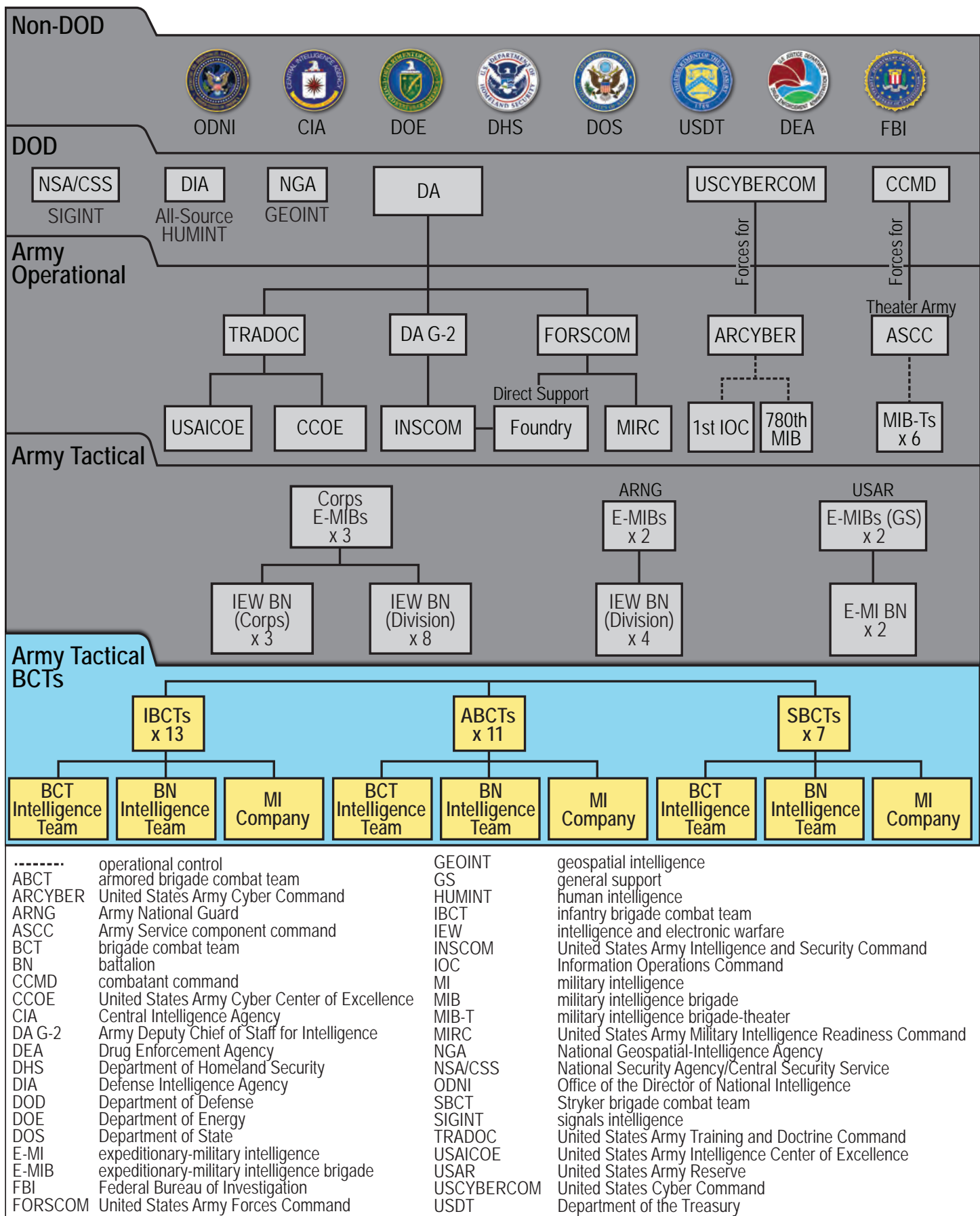


Figure 3. BCT Intelligence Collaboration with Higher-Level Organizations

relies on the effective synchronization of the intelligence warfighting function. Effective synchronization must begin early in the planning process and be continually assessed throughout all phases of an operation. Understanding *when* and *how* intelligence handovers will occur with subordinate, adjacent, and higher echelons is essential for intelligence staffs to ensure there are no gaps in the intelligence process as they maneuver with the unit.

The BCT intelligence cell must be flexible and resilient to meet the demands of the maneuver units in its organization. The cell must be prepared for constant movement and displacement, while maintaining its battle rhythm and processes. Synchronizing intelligence efforts through constant communications with other intelligence units while continually maneuvering through a battlefield during large-scale ground combat may be the key to maintaining situational understanding.

Maneuverable Intelligence Nodes

Mission variables, known as METT-TC, determine command post (CP) displacement (commonly referred to as jumping tactical operations center). As explained in ATP 2-19.4, units will require frequent CP movements during large-scale ground combat operations because of the high operational tempo, risk mitigation measures, and other factors. Displacements can be both planned and unplanned; therefore, CPs must maintain a readiness posture to displace on short notice. When CPs must displace, notable impacts arise from incomplete access to information because of diminished communications capabilities with which to disseminate information and intelligence.

Standard operating procedures covering all aspects of displacement will assist in maintaining a state of readiness. Critical aspects of command and control (C2), such as contact with higher headquarters and subordinate units, must be maintained during displacement. Intelligence staffs must ensure they prepare their specific displacement plan to align with the supported CP's plan. This will facilitate near-seamless transitions when displacing and provide continuity of intelligence support during large-scale ground combat operations.

After a unit establishes its CP, it enables different types of connectivity, including network access at different classification levels, detailed and nested digital common operational pictures, supported intelligence systems, and fully connected intelligence elements at echelon, such as an intelligence support team or the brigade intelligence support element. Establishing a robust intelligence architecture should not limit the ability to move it quickly. Intelligence

staffs accomplish rapid displacements through detailed planning and preparation and by executing deliberate intelligence handovers between the assorted CPs to provide continuity until the architecture is reestablished.

Degraded Information Environments

Just as the commander considers the impact of degraded information environments on C2 systems, the S-2 considers the impact on intelligence operations and systems. ATP 2-19.4 describes degraded information environments and mitigation methods. Intelligence networks may be degraded for various reasons, such as hostile actions to contest the freedom of maneuver in the cyberspace domain and the information environment or because of a lack of resources for sufficient network coverage in an area of operations. The degradation may not be technological in nature, but rather environmental. The possible use of nuclear weapons or adverse weather may create physical conditions that cause electromagnetic spectrum interferences or degraded intelligence networks. All these factors may interfere with the BCT intelligence warfighting function's ability to conduct intelligence operations.

As explained in ATP 2-19.4, to mitigate this risk and successfully conduct intelligence operations in degraded information environments, staffs cannot rely solely on technological capabilities. S-2s should ensure their personnel receive training on analog and manual processes and are comfortable operating in degraded information environments. Ultimately, the solution to operating in degraded information environments is C2. Despite severely degraded conditions, Army forces continue to make decisions and act in the absence of orders, when existing orders no longer fit the situation, or when unforeseen opportunities arise.

Primary, Alternate, Contingency, and Emergency Planning

Intelligence staffs should plan to maintain constant communications throughout operations and should do this through a tailored communications plan, commonly known as a PACE plan. ATP 2-19.4 explains in detail how S-2s should collaborate with S-6s to establish the intelligence architecture in order to determine an efficient communications plan. This plan should be codified in a C2 standard operating procedure and Annex H (Signal). S-2s should also ensure each intelligence discipline and element develops a detailed PACE plan to promote continuous communications, information collection, and intelligence operations. A PACE plan establishes the various communications methods and channels, typically from higher to lower echelons, but it should also consider lateral communications. The PACE concept is

a valuable tool that ensures the availability of backup communication channels if the primary channel fails.

As mentioned in ATP 2-19.4, some OEs are more permissive and have a mature information infrastructure, allowing communications and products to flow relatively freely across mediums such as SECRET Internet Protocol Router Network (SIPRNET) email or SharePoint. In these circumstances, a PACE plan is still necessary because email servers and SharePoint experience outages. S-2s will benefit from a PACE plan in mature communications environments, even if the plan uses different aspects of the same medium (unit SharePoint, email, third-party SIPRNET SharePoint). The update to ATP 2-19.4 provides several example PACE plans that intelligence Soldiers can use as a reference when planning for communication continuity for their units.

Collection Management

ATP 2-19.4 and ATP 2-01, *Collection Management* (formerly known as *Plan Requirements and Assess Collection*), were developed concurrently; therefore, careful coordination ensured these publications would complement each other. The new ATP 2-19.4 provides explanations of collection management from the BCT perspective and includes updated terms and definitions, and features the updated collection management process (Figure 4).

ATP 2-19.4 states that collection management contributes to the overall information collection plan. The publication also states that, in intelligence usage, “*collection management* is the process of converting intelligence requirements

into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required.”¹ (See ATP 2-01 for a detailed discussion on collection management.) Although a collection management team does not currently exist within the MI company or BCT S-2 structure, the BCT S-2 must establish a dedicated collection management team in order to successfully conduct the processes of collection management and appropriately coordinate with the current operations cell, plans cell, and targeting cell.

Spotlight on Intelligence Architecture Appendix

Digital Intelligence Systems Master Gunner Course (DISMGC) and Information Collection Planners Course personnel assisted in rebuilding the intelligence architecture appendix. Collaboration with DISMGC personnel led to the creation of a Microsoft Teams group with the goal of bringing together intelligence architecture subject matter experts from across the force. This Microsoft Teams group is still active with more than 150 members and guests. The group helped update the intelligence architecture appendix and are currently assisting with the update to MI Pub 2-01.2, *Intelligence Architecture*. This effort demonstrated that using a collaboration software platform could be a potential best practice for future publication developmental efforts.

DISMGC is a partnered endeavor among U.S Army Forces Command, U.S. Army Intelligence and Security Command, Army National Guard, and USAICoE to train intelligence leaders to plan, develop, and integrate dynamic digital structures using the Distributed Common Ground System-Army (DCGS-A) family of systems within complex environments. As the DCGS-A is the Army’s intelligence program of record, the update to ATP 2-19.4 contains multiple references to the DCGS-A family of systems. The 2015 version of ATP 2-19.4 contained no such references, making these updates a welcome addition to the revised Army techniques publication.

The new BCT intelligence architecture appendix provides the necessary information that BCT intelligence Soldiers require to understand the basic components of an intelligence architecture, which consists of the

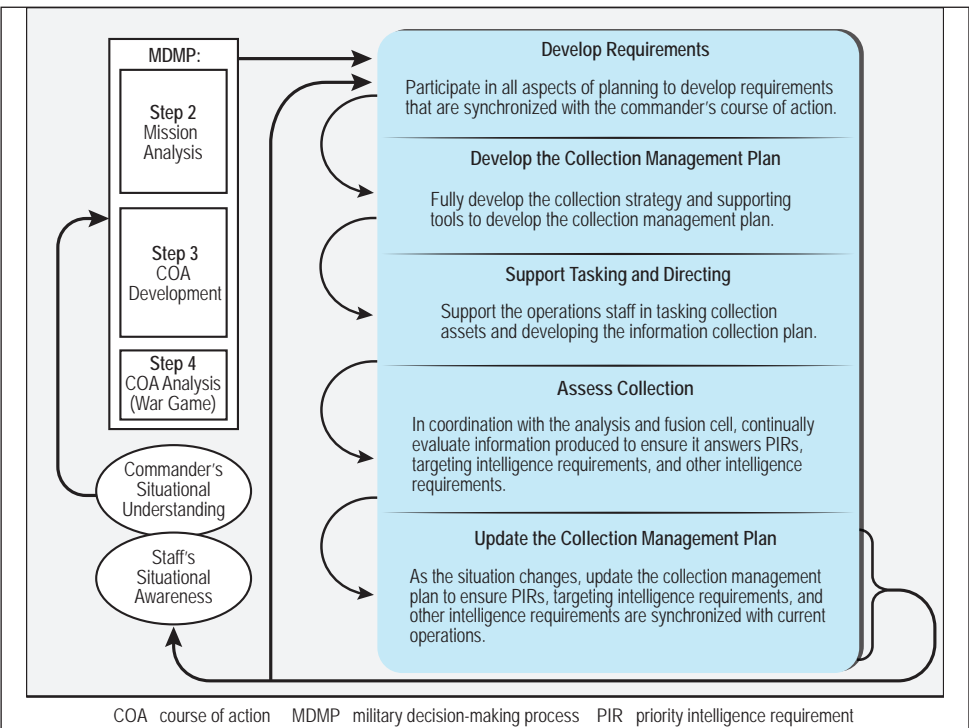


Figure 4. Collection Management Process

source, processor, output, and transport methodology. This methodology, along with the provided examples and explanations, should assist BCT intelligence Soldiers in having a better understanding of the foundations for establishing an intelligence architecture.

Spotlight on Intelligence Training Appendix

ATP 2-19.4 now features MITS, first introduced in 2019. MITS is an intelligence-centric certification event designed to train individuals, crews, and platforms to accurately answer intelligence requirements for the commander and certify respective intelligence disciplines in a field environment. MITS is a standardized certification strategy for commanders to plan training before certifying their tactical intelligence warfighting capabilities in an objective and quantifiable manner.

While there have been many attempts to address intelligence training deficiencies, there was no standardization across the force and no process to ensure certification of intelligence military occupational specialty-specific Critical Task Lists. Without standardization, the intelligence warfighting function lost the ability to have an intelligence professional able to perform their intelligence duties, moving between tactical and strategic level units. To create a standard for MITS, USAICoE developed tasks that applied across the force that would be transferable and translatable across any formation. ATP 2-19.4 describes MITS, the associated tier levels, and the training circulars that provide the in-depth information that BCT MI leaders can leverage and cross-reference to ensure the readiness of the BCT intelligence warfighting function.

Spotlight on Targeting for BCTs Appendix

The targeting appendix includes the most up-to-date intelligence support to targeting information tailored for the BCT level. It was developed by targeting subject matter experts on USAICoE’s doctrine writing team who are responsible for completing various intelligence support to targeting projects. The team has been involved in providing the intelligence-specific portions to FM 3-60, The Targeting Process, which is under develop-

ment. In addition, the intelligence support to targeting writing team is developing a new publication titled ATP 2-01.4, *Intelligence Support to Army Targeting*. Collaboration ensured that ATP 2-19.4 would be relevant and complementary to both Army targeting publications in current production.

The update to ATP 2-19.4 includes refinements to the decide, detect, deliver, and assess (D3A) Army targeting methodology and provides the key intelligence tasks to support targeting:

- ◆ Perform intelligence preparation of the battlefield.
- ◆ Provide intelligence support to target selection and target development.
- ◆ Provide intelligence support to target detection.
- ◆ Provide intelligence support to combat assessment.

The targeting appendix explains how the Army targeting process organizes the efforts of the commander and staff to accomplish key targeting requirements (Figure 5). The D3A process assists the commander and staff in deciding which targets must be acquired and engaged and in developing options to engage those targets.

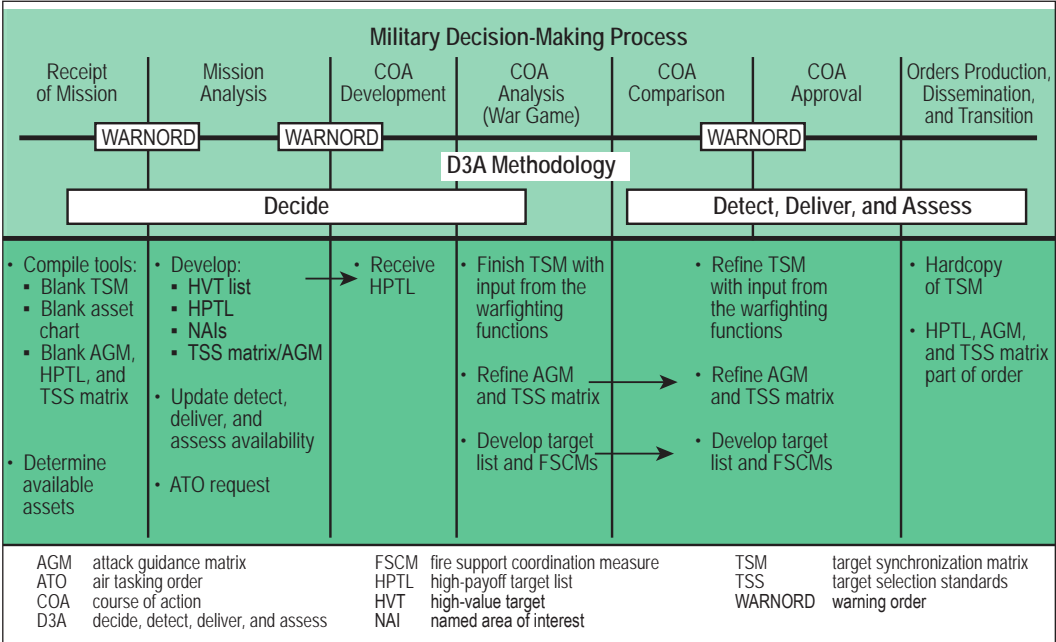



Figure 5. The Military Decision-Making Process and Army Targeting Process

Conclusion

The goal of the ATP 2-19.4 writing team was to produce the best possible doctrine publication for the force—one that contains timely and relevant information despite the changing work environment the team encountered during the coronavirus disease 2019. This endeavor entailed incorporating best practices and lessons learned, leveraging USAICoE’s pool of local subject matter experts, reaching

out to the intelligence community, and integrating a collaboration software platform into the workflow process.

Additionally, the initial and final drafts of ATP 2-19.4 were staffed worldwide and received approximately 600 combined comments as a result. These comments were adjudicated, and the draft publication subsequently underwent multiple senior leadership reviews. The writing team also ensured that the publication would synchronize with other draft publications such as ATP 2-01, *Collection Management*, and ATP 2-01.4, *Intelligence Support to Targeting*, along with the recently published TC 2-19.01, *Military Intelligence (MI) Company and Platoon Reference Guide*, and FM 3-96, *Brigade Combat Team*.

The USAICoE Doctrine Division counts on intelligence professionals like you to provide feedback on doctrinal issues. If you need doctrinal assistance or have important feedback, please contact the Doctrine Division at usarmy.hua-chuca.icoe.mbx.doctrine@mail.mil. 

Endnote

1. Office of the Chairman of the Joint Chiefs of Staff, Joint Publication 2-0, *Joint Intelligence* (Washington, DC: The Joint Staff, 22 October 2013), I-13 (emphasis added).

Check out the MI Professional Bulletin website at <https://www.ikn.army.mil/apps/MIPBW>.



**To access all of our issues back to 1974, click the archive tab.
A CAC is no longer required.**

MI Professional Bulletin



INFORMATION DIMENSION

by Mr. Chet Brown, Chief, Lessons Learned Branch

Introduction

If the pen is mightier than the sword,¹ what does that mean for the relationship between Twitter and the M-4? The sword and the rifle are only able to affect, persuade, or force compliance at the time and place where they are wielded. An individual brandishing either weapon can only influence a direct response from an actual or potential subject, whereas the written or transmitted word (print or electronic) may induce the desired behavior from a distance, asynchronously over time, and without physical risk to the protagonist.

Information is Key

Information is the lifeblood of our profession. Information is the key component that enables us to complete the task for the commander for which no other warfighting function is responsible—to answer intelligence requirements. Any other warfighting function has the capability to answer the intelligence requirements, but we bear the responsibility for estimating an enemy's future activities. We must develop and ensure effective strategies to identify an enemy's current and potential actions and answer the intelligence requirements and other information requirements before the latest time information is of value (LTIOV).

This does not mean we only operate in the information dimension. FM 3-0, *Operations*, states, "To an ever-increasing degree, activities in the information environment are inseparable from ground operations."² This appears in the same paragraph that begins with "Large-scale combat operations are intense, lethal, and brutal."³

Information is also lethal. The combat experiences of the light infantry brigade commander (directly responsible for developing me to be an S-2) would ensure subordinate commanders and staff officers understood the value of intelligence preparation of the battlefield products and estimated enemy courses of action by declaring, "I killed more enemy as an infantry battalion S-2 than I did as a rifle company commander." The clearly understood inference was the commander did not personally action every target; the intelligence information he provided enabled the battalion's success. Information may not be kinetic, but it can definitely be lethal. The absence of information—failing to answer an information requirement before the LTIOV—can also be lethal to our own force.

Current events clearly demonstrate that those who seek to damage, destroy, or dis-integrate segments of our society and/or physical infrastructure are already

operating in the information dimension. Information is being weaponized.

Information is METT–TC Dependent⁴

Providing context sets the stage for the recipient to receive the information in the most appropriate manner. A former boss implemented an information management labeling protocol to help him triage emails from a large number of direct subordinates. When an email subject line started with the appropriate category—such as action, information, for decision, need guidance, or CCIR (commander’s critical information requirement)—the immediately recognizable context allowed him to quickly assign a work priority. The first line in the body of the email provided additional context to the category alert in the subject line.

Subject: FOR DECISION: Tomorrow’s Commanders Update Briefing (CUB)

(Body) Need commander’s decision to hold the CUB in person or online.

Subject: INFORMATION: Tomorrow’s Commanders Update Briefing (CUB)

(Body) Sandwiches and soft drinks will be available at the CUB as we promote 1LT Windscreen to CPT.

Observations from combat training center rotations identify the failure to highlight or categorize the importance of intelligence/information reports or products. This includes available information that answers the intelligence requirements but is left unread, languishing in a message queue indistinguishable from a myriad of other intelligence reports. These are missed opportunities. Providing context to intelligence information or reports results in the rapid recognition and application of critical information.

The additional context provided in the body of the email examples also enables faster comprehension of the report’s significance—answering the why before the recipient has to ask. This technique is also useful when reporting intelligence information. Telling the commander “We’ve received a report of two enemy infantry fighting vehicles and a tank spotted at grid HG108246 at 09:00AM” is not as useful as saying, “Enemy’s lead reconnaissance element observed in NAI 7 moving west.”

Information that two BMP-3s and a T-72—part of the reconnaissance element and perhaps a higher echelon’s reconnaissance detachment—are moving ahead of the battalion tactical group (BTG) is useful; the resulting analysis may lead to the higher priority conclusion that “Within 15



Two people are looking at the same object and interpreting it differently because of a different point of view.

minutes we expect the BTG advance party to enter Kill Box Carol.”

Perspective

The commander and intelligence analyst may view the importance of the preceding intelligence reporting differently. The commander’s requirement may have been answered by identifying where and when the enemy’s lead reconnaissance element would enter the area of operations. The intelligence analyst’s focus (beyond answering the intelligence requirement) may be on learning the composition of the enemy force to determine if the unit spotted the enemy’s fixing or exploitation force.

When people ask us to provide information, and if we fail to understand their various perspectives, do not assume common understanding. Allow me to provide a personal example involving Cinco de Mayo.

So who was this “Cinco de Mayo” guy I kept hearing about on the radio and television commercials? In elementary school, I vaguely remember learning about an explorer named Vasco de Gama, but I could not recall learning about Cinco de Mayo. The resulting humiliation from posing my question aloud, upon my arrival at a California duty station, remains with me to this day. Having studied French for a year and being ignorant of the Spanish language and Mexican history gave me a different perspective from those to whom I posed my question. In my mind, it was Vasco de Gama, Cinco de Mayo, same letter count, same capitalization style, and all non-English words. I knew one was definitely a seafaring explorer. It made sense that Cinco de Mayo was an explorer too, right? I was a No-Go at the analytical conclusion station that day. I also exemplified the “assume” adage.

We’ve seen the same challenges in military intelligence (MI) units when integrating U.S. personnel or augmentation

elements into operations. Some assumptions are necessary in order to plan operations. Valid assumptions take the place of expected future conditions. In the absence of lessons learned collection, I assume we rarely take into account the education, cultural awareness, language proficiency, or experiences of external personnel when task-organized to operate together. Challenges in common understanding and expectations exist when bringing dissimilar U.S. Army units together to operate as a single force. We must address, train, or clarify differing techniques and procedures to enable each force to operate at its optimal level. Heavy-light rotations at the National Training Center were always an opportunity to achieve the benefits of synergy through discovery learning. The effects are multiplied when U.S. and multinational partner elements join together to perform combined operations. Much discovery learning was evident each time the aforementioned light infantry brigade trained with a multinational partner mechanized infantry company. The good news is that several best practices are available to address these challenges:

- ◆ Doctrine as a starting point.
- ◆ Standard operating procedures (SOPs).
- ◆ Terms of reference (ToR).
- ◆ Liaison officer exchange.
- ◆ Knowledge management.

Doctrine as a Starting Point. As in any military endeavor, doctrine provides a foundation on which to build greater understanding and increased interoperability. An airborne infantry ranger officer with multiple tours in Afghanistan confirmed this lesson when receiving orders to a Stryker-equipped cavalry troop in an armored division. Doctrinal understanding provided the initial context that enabled continued self-development and collaboration with subject matter experts (noncommissioned and commissioned officers) after arriving at his unit. Doctrine—it's only useful if you read it.

Standard Operating Procedures. Lessons learned collectors often comment on the superior performance of intelligence elements led by professionals who establish the conditions for success for their subordinates and successors by creating and updating SOPs. The most frequent requests the

U.S. Army Intelligence Center of Excellence Lessons Learned Branch receives from operational force personnel are for SOPs. You should not be surprised when I inform you that Army SOP doctrine is available in ATP 3-90.90, *Army Tactical Standard Operating Procedures*.⁵ This publication's 32 pages provide useful tips, considerations, and techniques to develop and implement an SOP. It lacks the specific information needed to serve as a guide to newcomers or those who assume the duties of an absent (killed in action, wounded in action, or vacant) position. An effective SOP describes the roles, missions, functions, processes, procedures, and positional responsibilities to provide intelligence support to the commander. To obtain this level of detail, one needs to employ the most sincere form of flattery—plagiarism. Excuse me, I meant to say, collaborate with other MI professionals to incorporate components of a successful unit's SOP into your own. Continually updating the SOP during and after operations inherently results in containing best practices informed by lessons learned.



An intelligence analyst assigned to D Company, 326th Brigade Engineer Battalion, 1st Brigade Combat Team, 101st Airborne Division (Air Assault), plots named areas of interest on a map, April 14, 2021, during MITS II certification at Johnson Field at Fort Campbell, KY.

U.S. Army photo by MAJ Vonnie Wright

Terms of Reference. One of the most useful features we've seen incorporated in a tactical SOP was a ToR that an infantry division G-2 established in order to clarify the roles and responsibilities of individuals within the brigade intelligence support element (BISE) for the division brigade combat teams (BCTs). The ToR clarified what BISE members should learn, train, rehearse, or study before being task-organized to the BISE or working in their respective BCT S-2 intelligence cell or MI company units.

The G-2 mentored subordinate BCT S-2s by directing them to develop the ToR tailored to their respective BCT's personnel knowledge, skills and abilities, task organization, concept of operations, and SOPs. The BCT S-2 and MI company commanders refined the ToR to—

- ◆ Establish internal production task/supervision hierarchy among BISE members.
- ◆ Assign scope of responsibility or authority in providing intelligence support.
- ◆ Identify positions responsible for supporting specific events/products.
- ◆ Establish expectations of performance.

The ToR also mitigates duplication of effort and unintended redundancy in intelligence support to operations.

Liaison Officer Exchange. Maneuver units frequently exchange liaison officers to ensure common understanding and expectations. U.S. MI elements of differing (infantry, Stryker, armor) BCT or other unit types infrequently exchange intelligence liaison officers. Exchanging intelligence liaison officers with dissimilar U.S. units may not be viable because of the conditions of the mission variables. The unit's non-MI liaison officers may be capable of performing the requirement for intelligence liaison officers in U.S.-only formations.

Lessons learned observations indicate exchanging intelligence liaison officers in combined operations or multinational partner environments is a best practice. The legal, regulatory, policy, and enabling considerations of differing nations' intelligence operations benefit from clear, accurate, and precise shared understanding. Intelligence liaison officers are able to ensure the increased level of understanding of written or electronic products achieved by personal interaction and elimination of ambiguity.

Knowledge Management. Effective knowledge management techniques that we have observed at the tactical level build upon the synergy achieved by each of the preceding lessons and best practices. We are noticing a reversal of the trend in which BCTs lack a knowledge management officer. More often, tactical units are either assigning an officer as the unit's knowledge management officer or appointing an officer to serve as the knowledge management officer during operations. This is a good first step. Some units continue

to struggle in this area. Here are a few of the challenges we are seeing less of, to help inform your SOP development:

- ◆ The BCT did not implement their knowledge management procedures.
- ◆ Knowledge management procedures delineated in the BCT SOP were not followed.
- ◆ Soldiers did not know they could change, or suggest revisions to, the SOP.
- ◆ The SOP did not specify an electronic file structure or naming convention to facilitate timely collaboration, information dissemination, information retrieval, or exploitation.
- ◆ BCT personnel did not know when intelligence products were available or posted.
- ◆ BCT had no means of tracking the dissemination of intelligence products.
- ◆ Intelligence products were disseminated only on the upper tactical internet.

Conclusion

Developing effective strategies to answer intelligence requirements, and to improve the processes that support them, is an important part of our profession. We look forward to helping you address the challenges in improving your processes as much as we look forward to learning of your successes so that we may share them with others. 🌟

Endnotes

1. Edward Bulwer-Lytton wrote "The pen is mightier than the sword" in 1839 in his historical play about Cardinal Richelieu, chief minister to King Louis XIII. Alison Gee, "Who first said 'The pen is mightier than the sword'?" BBC News, 9 January 2015, <https://www.bbc.com/news/magazine-30729480>.
2. Department of the Army, Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 6 October 2017), 1-2. Change 1 was issued on 6 December 2017.
3. Ibid.
4. METT-TC: mission, enemy, terrain and weather, troops and support available, time available, and civil considerations.
5. Department of the Army, Army Techniques Publication 3-90.90, *Army Tactical Standard Operating Procedures* (Washington, DC: U.S. GPO, 1 November 2011).



by Mr. Kevin B. Gorski

Introduction

The People's Republic of China (PRC) is nearing the end of the "Hundred-Year Marathon," a strategy of modernization efforts across all aspects of the Chinese society, economy, and military, lasting from 1949 through 2049.¹ Key to the PRC's strategy is advancing a comprehensive military modernization program that the PRC would consider complete by 2035 and transforming the People's Liberation Army (PLA) into a "world-class" military by 2049. Through imports, foreign direct investment, talent recruitment, research and development, and academic collaboration, the new PLA will integrate emerging technologies for military application.²

Integration of Technologies

The PRC is integrating numerous emerging technologies to reach its goal. These technology sectors and programs include:

- ◆ **Artificial Intelligence and Advanced Robotics:** The PLA's artificial intelligence and advanced robotics programs consist of enhanced data exploitation; decision support; manufacturing; unmanned systems; and command, control, communications, computers, intelligence, surveillance, and reconnaissance. Additionally, China's military and technology industries will push to dominate the third revolution in weaponry by advancing lethal autonomous weapon systems.
- ◆ **Semiconductors and Advanced Computing:** This advanced technology sector comprises enhanced cyber operations and weapons design, and shortened research and development cycles. China will speed up artificial intelligence and improve counter-jamming capabilities based on cutting-edge computing.
- ◆ **Quantum Technologies:** The goal of the PLA's quantum technology program is enabling secure global communications, enhanced computing and decryption capabilities, undersea target detection, and enhanced submarine navigation. China's quantum research budget is its largest national investment (estimates reveal spending of \$2.5 billion in 2017) and will dominate related computing patents.³ Current programs are in communications, but future ventures are unlimited.
- ◆ **Biotechnology:** The PLA's biotechnology program includes research and development in the fields of enhanced warfighter selection and performance and advanced human-machine teaming. The future of the Chinese soldier is "human enhancement" tied to cognitive, physical, and biochemical improvements.
- ◆ **Hypersonic and Directed Energy Weapons:** The focus of these programs entails developing global strike and defeating missile defense systems, antisatellite missiles, and unmanned aircraft system capabilities.
- ◆ **Advanced Materials and Alternative Energy:** This area includes improved military equipment and weapon systems.⁴ Lunar missions are China's approach to the creation of new metals for use in military applications by 2035.

Potential Fielding Challenges

The Chinese have integrated various technologies with PLA modernization planning, some of which have potential fielding challenges:

◆ **Biotechnology, Advanced Materials, and Computing.**

- ◆ *Application:* Genetic alteration and human enhancement are integrated with advanced digital communications and materials producing the next generation Chinese soldier. Professional and elite soldiers will possess advanced body armor made of lightweight advanced material, enhancing performance and endurance with direct digital tactical and cyber secure communication.
- ◆ *Challenge:* The concept and fielding of next generation Chinese soldier technologies is likely limited to professional and elite soldiers: airborne, marine, and special operations forces (SOF).

◆ **Advanced Artificial Intelligence Robotics with Advanced Materials.**

- ◆ *Application:* Aggressive Chinese lunar exploration/mining and merger of artificial intelligence computing and robotics will create advances in tactically autonomous weapon systems—autonomous sentry and micro-avionic robotics. PLA fielding will expand beyond current lethal autonomous weapon system drones or unmanned aerial vehicles like the CH-4 Rainbow and GJ-2 Wing Loong II.⁵
- ◆ *Challenge:* China will face scientific and political pressures concerning the application of artificial intelligence to weapons. This may be a catalyst for future conflict.⁶

◆ **Artificial Intelligence/Robotic Chemical and Biological Weapon Defense.**

- ◆ *Application:* The advances in artificial intelligence integrated on vehicles are not limited to lethal actions. Autonomous robotic capabilities with advanced computing will enable China to deploy aerial and ground drones that detect explosives, chemicals, and biological threats.
- ◆ *Challenge:* The challenge will be selecting and maintaining older systems, along with ensuring computing is up to date with the latest chemical and biological threats.

◆ **Autonomous Robotics with Global Access.**

- ◆ *Application:* Advances in computing and robotics will give the PLA the needed autonomous logistical backbone to meet global requirements, first supporting civilian and then military ventures.

- ◆ *Challenge:* Learning how to secure and sustain logistics will require a decade or more for an actual autonomous logistics network.

◆ **Artificial Intelligence-Enabled Indirect Fire Systems.**

- ◆ *Application:* The current detection, decision, shooter, and steel-on-target process can take anywhere from a few minutes to several minutes. The PLA desires to interdict an adversary's ability to fire or conduct counter-fire operations at all echelon levels.
- ◆ *Challenge:* Heavy reliance on artificial intelligence acquisition and engagement may dismiss established indirect fire tactics. The PLA may reveal this capability near the Sino-Indian border.

◆ **Directed Energy.**

- ◆ *Application:* Directed energy anti-air and missile technologies are not far from reality. The adoption of anti-air and naval directed energy weapons may produce capabilities for ground forces.
- ◆ *Challenge:* The challenge of directed energy is the energy source required to integrate as a tactical maneuvering system.

◆ **Underground Facilities.**

- ◆ *Application:* The construction of underground facilities ensures the survivability of the government and military. This requires a priority to ensure missile and strategic early warning and communication networks can operate in any contested environment.
- ◆ *Challenge:* The construction of underground facilities is difficult to disguise, and Chinese strategists realize that any underground facilities within China and abroad are targets.

The Next 30 Years

Over the next 30 years, the overall measure of the Central Military Commission's success is the ability to increase readiness within the theater command structure, established in 2016 and divided into the Eastern, Southern, Western, Northern, and Central Theater Commands. Each theater has specific missions directed toward immediate regional security matters, with the exception of the Central Theater Command (headquartered in Beijing), which has the mission of capital security and the ability to support other theaters' response to non-war military activity.

The PLA is increasing the combined arms approach to operations. The Central Military Commission's Joint Operations Command Center is central to coordinating contingencies between the five theater commands. Over the next 30 years, the realism and size of these exercises will



The five theater commands of the People's Liberation Army

grow. The 83rd Group Army's airfield seizure exercise is an example of combined training, with a growing complexity that will result in the demonstration of joint warfare capabilities. The 83rd Special Operations Brigade, 83rd Group Army, conducted a force-on-force exercise simulating a mission to seize an airfield in November 2020. Training consisted of reconnaissance, wet obstacle crossing, resupply of scouts by small unmanned aircraft systems (identified as hexacopter), and offensive phase, including heliborne insertion from the 161st Air Assault Brigade (not organic to the 83rd Group Army).⁷

People's Liberation Army Army (PLAA)

In the late 1990s, evidence of an Army reorganization revealed a restructuring from divisions and regiments to an operationally flexible force, including an emphasis on a brigade formation executing complex combined-arms and joint operations.

The PLAA restructured five "theater army commands" that comprised 13 group armies with a total of 78 combined-arms maneuver brigades—heavy, medium, and light—along with six additional brigades for artillery, air defense, aviation, SOF, engineer and chemical defense, and sustainment. There remain nonstandard independent divisions and brigades outside of the group armies with specific strategic missions in contested regions and Beijing proper.

The PLAA brigade transformation comprises heavy, medium, and light, along with mountain missions. Additionally,

the airborne (7), marine (8), and re-structured SOF (15) brigades will be operational by 2049. The transition to a brigade of approximately 5,000 personnel and associated equipment ensures the PLAA can task organize forces to meet specific non-war military activities operations, or eventually to operate within a multi-domain contested action. New deployment concepts for the smaller, more adaptable brigades will improve the PLAA's ability to deploy, seize, and maintain areas abroad.

The modernization effort will replace existing armor (tanks and other combat vehicles), artillery, air defense, and aircraft in formations. The PLAA will field new advanced combat vehicles, armaments, munitions, and advanced communication devices based on

technology gained, and the development of new materials. Highlights of PLA force modernization initiatives include—

- ◆ **Autonomous Sentry Tanks.** The artificial intelligence modification to older equipment will enable the PLAA to employ an unmanned, likely autonomous security or defensive perimeter system. In November 2018, the Chinese already began testing artificial intelligence possibilities with the Type 59 tanks.⁸



Video footage showing a Type 59 medium tank with a PLA soldier possibly controlling via a remote computer terminal.

- ◆ **Autonomous Fires.** The integration of artificial intelligence into computing detection-to-fires will transform PLAA battlefield capabilities. Munition distance and accuracy will run parallel to experimentation in the detection of targets with the ability to assign fires autonomously while emphasizing speed and deception in order to increase system survivability.

- ◆ **Airborne and Marine Troops.** The PLA will emphasize combined arms training and mobility of the airborne and naval marine brigades. The priority through 2035 is an increase in aerial and amphibious lift capacity at greater distances than currently exist in the PLA.
- ◆ **SOF Capabilities.** Scalable, lighter, and advanced weapons tactics for initial entry to secure ports and critical infrastructure will be essential.

PLA Air Force and PLA Navy Aviation

The PLA Air Force and PLA Navy Aviation is the third largest global aviation combat force but will continue to increase in numbers and advanced avionics. Future emphasis is on airborne command and control, logistics and in-flight refueling, strategic reconnaissance, and paratroop operations.

Unmanned Aerial Vehicle. Future development of the unmanned aerial vehicle by the Chinese civilian and military employment strategies will enable new tactics and doctrine in PLA warfare. Stealth and miniaturization with advanced avionics, engines, and lift capacities will further a wide range of unmanned aerial vehicle technology. Swarming drones tied into autonomous guidance, target acquisition, and attack execution will accompany the growth in artificial intelligence-enabled autonomous unmanned technologies.

Integrated Air Defense System. The integrated air defense system is a significant antiaccess and area denial challenge for United States forces in the regional limits of China. Artificial intelligence will again improve autonomous operations to include kinetic-kill vehicle technology of a mid-course interceptor at the upper layer of the PLA's multi-tiered missile defense system.⁹

PLA Rocket Force

The PLA will continue to focus on a capable and robust ballistic missile global force. The focus for the PLA Rocket Force is "enhancing its credible and reliable capabilities of nuclear deterrence and counterattack, strengthening intermediate and long-range precision strike forces, and enhancing stra-

tegic counter-balance capability, so as to build a strong and modernized rocket force."¹⁰

Conclusion

By 2035, the PLA will have transformed from an army capable of defending China's internal and immediate regional security concerns to a "world class" military that is extremely visible on the global security stage. Global powers will recognize the PLA's transformation into small, multi-role, scalable brigades and SOF capable of responding to multi-domain contingencies. This transformation includes cyberspace operations, a physical presence in space (likely the Moon), and a global response beyond humanitarian and disaster relief events. 🌸

Endnotes

1. Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company, 2015).
2. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2020* (21 August 2020), 175.
3. Phillip C. Sanders, "Beyond Borders: PLA Command and Control of Overseas Operations," *Strategic Forum* no. 306 (July 2020), <https://ndupress.ndu.edu/Portals/68/Documents/stratforum/SF-306.pdf>.
4. Office of the Secretary of Defense, *Annual Report to Congress*, 148.
5. Elsa B. Kania, "'AI Weapons' in China's Military Innovation," *Global China* (April 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf.
6. Elsa B. Kania, "Chinese Military Innovation in the AI Revolution," *RUSI Journal* 164, no. 5–6 (29 November 2019): 26–34.
7. Department of the Army, *U.S. Army Asia Studies Detachment Report ASD21C03023* (November 4, 2020); and Department of the Army, *U.S. Army Asia Studies Detachment Report ASD21C03025* (November 6, 2020).
8. Office of the Secretary of Defense, *Annual Report to Congress*, 144.
9. Ibid., 52.
10. Ibid., 55.



Moments in MI History

How Did We Get Here?

The U.S. Army Intelligence School Moves to Fort Huachuca (Part 2 of 4)

by Lori Stewart, USAICoE Command Historian

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

January–March 2021 issue

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

April–June 2021 issue

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

July–September 2021 issue

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

MIPB Online FY 2022

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

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

Introduction

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



MG William H. Blakefield, Commander, Army Intelligence Command, 1965 to 1967.

ing efforts into one entity now known as the U.S. Army Intelligence Center of Excellence.

Blakefield Report Recommends Fort Huachuca

In 1969, MG Joseph McChristian, the Department of the Army's Assistant Chief of Staff for Intelligence, envisioned creating a "home" for intelligence, like the artillery center at Fort Sill, Oklahoma. Taking a list of nearly 30 possible sites, MG McChristian visited the most reasonable selections and narrowed his candidates to two: Fort Riley, Kansas, and Fort Huachuca. At the same time, the Army initiated a Long-Range Stationing Study Group (LRSSG),

chaired by MG Linton S. Boatwright, Deputy Chief of Staff for Personnel's Director of Individual Training, which included finding a suitable location for a new Intelligence Center. On 24 January 1970, Vice Chief of Staff of the Army (VCSA) GEN Bruce Palmer Jr. turned the LRSSG's and MG McChristian's recommendations over to MG William H. Blakefield, who was then commander of the Army Intelligence Command, which oversaw all Army counterintelligence within the continental United States.

MG Blakefield was directed to conduct reconnaissance visits to Fort Riley and Fort Huachuca to determine their feasibility for the Intelligence Center. Just 3 weeks later, on 10 February, the Chief of Staff of the Army finalized and approved the Blakefield Report. Given only two locations for consideration, MG Blakefield eliminated Fort Riley because of the extensive new construction and renovations needed to accommodate the center. On the other hand, he believed Fort Huachuca offered many advantages, not the least of which was minimal air traffic and moderate weather that allowed for year-round flights and field training. Furthermore, the uncluttered electromagnetic environment would facil-

itate the development and training of sophisticated intelligence equipment. Fort Huachuca was also located in a minimally populated area with plenty of surrounding federal and state lands into which it could expand, if necessary.

Crucial to an acceptable location was the ability to integrate intelligence training, concepts, doctrine, and materiel: "The Army needed to locate the school at a facility where the capability existed to conduct realistic combat intelligence field training which is dependent on the effective and coordinated use of aviation, avionics, electronics, target acquisition devices, automatic data processing equipment, and tactical units."¹ With the already established presence of the Combat Surveillance and Electronic Warfare School, the U.S. Army Electronic Proving Ground, the Army Security Agency Test and Evaluation Center, and Libby Army Airfield at Fort Huachuca, Army intelligence could achieve that desired integration while saving the Army manpower and money.

The fact that Fort Huachuca was immediately available also figured into MG Blakefield's recommendation. His report endorsed the movement of the U.S. Army Intelligence School (USAINTS) and the Combat Developments Command Intelligence Agency to Fort Huachuca, but the proposed combat arms brigade was cut, as were all of the operational intelligence activities, which were recommended for retention within the Washington, DC, area for administrative purposes.² These reductions were necessary because of serious concerns about water and housing availability at Fort Huachuca that caused MG Blakefield to cap the move to only 2,100 permanent-party personnel. That number would not overtax the water situation because the arriving personnel would essentially replace those of a combat support training brigade scheduled for inactivation.³ One downside was an estimated deficit of more than 200 on-post housing units for eligible families, but this would soon be alleviated by upcoming construction projects at the post. Approved fiscal year (FY) 1970 and FY 1971 budgets already accounted for the construction of 200 family units. Furthermore, construction of a 1,200-man barracks was scheduled to begin in September 1970, and a 180-man Bachelor Officer Quarters was in the FY 1972 budget. Additionally, the Army fully expected the civilian community to begin the construction of suitable residences once the move decision was finalized. MG Blakefield did not provide cost estimates for future construction but estimated "move-in" costs at \$13.8 million.⁴

On 4 March 1970, less than a month after MG Blakefield presented his recommendations, the Office of the Secretary of the Army informed Congress that Fort Holabird would be closed as part of a host of other consolidations,



U.S. Army photo

Aerial view of Fort Huachuca in the early 1970s, looking southeast, with Libby Army Airfield shown in the lower left. The uppermost grouping of buildings would become the original U.S. Army Intelligence Center and School academic complex.

reductions, and realignments. Two days later, the Army publicly announced the closure of Fort Holabird and transfer of USAINTS to Fort Huachuca. The move would begin on 31 December 1970 with Holabird to close permanently 2 years later.

Not unexpectedly, the public announcement drew immediate criticism. Maryland Congressman Clarence Long demanded the Army reexamine the issue and called a session of the Military Construction Appropriations Subcommittee to evaluate the decision and the proposed expenditures for the move. Calling Fort Huachuca “austere” and “a nice place to visit but not to live,” he declared, “I am more certain than ever that this move will be an injustice to the taxpayers and to the Holabird personnel who are being asked to transfer.”⁵

Further caution came from the Army Corps of Engineers, which warned about the lack of water, stating, “We are not yet sure that we have sufficient water for the current strength let alone any increased strength.”⁶ A flurry of negative articles was published in national and local newspapers, primarily fueled by Congressman Long’s outrage.

At this point, MG McChristian was told to take his extensive Intelligence Center Concept and apply it to Fort Huachuca. Although he had initially favored Fort Huachuca if the entire post was turned over to intelligence activities, upon further study, he was reluctant to accept Fort Huachuca as the final answer. MG Blakefield’s recommended “reduced” center curtailed MG McChristian’s 21,000-person intelligence center to the bare minimum, leaving it little more than the USAINTS that already existed at Fort Holabird. Recognizing that his original vision was unfeasible in a shrinking Army, on 4 May 1970, he published his Assistant Chief of Staff for Intelligence Study. In the study, he revised his Intelligence

Center Concept down to a 9,700-personnel facility that included the school and the Intelligence Command, along with the 184th MI Company (Aerial Surveillance) and 14th MI Battalion to support training. Armed with MG Blakefield’s data stating that even that size center could not be supported at Fort Huachuca, MG McChristian recommended Fort Lewis, Washington, as an alternative.

Could Fort Lewis Be a Better Answer?

By June, because of political opposition, the movement of USAINTS to Fort Huachuca was essentially stalled as the Army considered other options, particularly Fort Lewis. In preparation for a final decision brief for the Army Chief of Staff, MG Boatwright travelled to Fort Huachuca to determine which of the post’s current activities did not “enhance operation of the Intelligence Center.”⁷ He was to consider whether these could be relocated elsewhere to allow more of the Army’s intelligence activities to move to Arizona but still keep the total population supportable by the available water supply.

While MG Boatwright headed to Fort Huachuca, MG McChristian went to Fort Lewis to determine its feasibility for his revised intelligence center. The Washington post had not been considered in any of the earlier studies because the Army had planned to move an entire infantry division there as activities in Vietnam wound down. By 1970, however, rumors surfaced that the division would not be moved to Fort Lewis after all, driving MG McChristian’s request that it be considered as an alternative to Fort Huachuca.

In its favor, Fort Lewis offered realistic training opportunities because of varied terrain and weather. However, the electromagnetic spectrum was cluttered, the air space was crowded, and the weather limited the number of training and flying days. Also, despite rumors to the contrary, the Army had not completely eliminated plans for stationing a division, or at least a brigade, at the Washington post.

Returning to Washington, DC, MG McChristian made his pitch for Fort Lewis to the VCSA on 14 August 1970. Foremost, he argued that Fort Lewis had none of the water and housing shortages that plagued Fort Huachuca and that his concept of an intelligence center could be established at Fort Lewis whether an infantry division was located there or not. He contended that the “reduced” center at Fort Huachuca recommended by MG Blakefield would cost approximately the same as his “revised” center at Fort Lewis. According to his calculations, “an operational intelligence center, less a brigade, could be established at Fort Huachuca in mostly temporary facilities with minimum family housing in about five to six years for



U.S. Army photo

Maryland Congressman Clarence Long visits Fort Huachuca on 10 May 1970.

a cost of \$19M. Long range replacement of temporary facilities would cost an additional \$57.7M for a total cost of \$76.7M.” On the other hand, Fort Lewis provided an opportunity for “a complete and fully operational intelligence center,” essentially his 9,700-man concept, within 3 to 4 years for about the same cost: \$14 to \$15 million move-in plus \$54 to \$59 million long-range construction (total \$68 to \$74 million). He concluded, “A better Army Intelligence Center can be established sooner, at less cost, and with more favorable political impact under the [Assistant Chief of Staff for Intelligence] ACSI Plan at Fort Lewis.”⁸ VCSA GEN Palmer reportedly replied, “Well and good, we have heard you, but I still think the Center should go to Fort Huachuca.”⁹ To placate MG McChristian, GEN Palmer granted his request to brief GEN William C. Westmoreland, now the Army Chief of Staff, who deferred the decision pending yet another study, the sixth in 3 years. ✱



GEN William C. Westmoreland, Chief of Staff of the Army, July 1968 to June 1972.

Endnotes

1. MAJ Kilday, *Information Brief: Advantages of Locating the Intelligence Center at Fort Huachuca*, n.d.
2. These included the majority of the Intelligence Command, as well as the Defense Central Index of Investigation, Department of Defense National Agency Check Center, the Data Handling Center, and the U.S. Army Personnel Security Group.
3. This refers to the “equivalent” population or the sum of the population resident on post 24 hours per day and one-third of the nonresident population who worked on post. For planning purposes, the study used 7,000 military personnel (permanent strength) and 6,500 civilian employees and dependents.
4. This figure included \$7.7 million relocation costs plus \$6.2 million for initial modifications and construction.
5. “Fighting Chance to Keep Holabird Here: Long,” source unknown, 21 May 1970; and “Long Fights Holabird Transfer,” *Baltimore Sun*, 14 May 1970.
6. Larry Phillips, “Huachuca Bombed as MI Site,” *Army Times*, 2 August 1972.
7. LTG W.E. DePuy, Assistant Vice Chief of Staff of the Army, to MG McChristian and MG Boatwright, “Location of U.S. Army Intelligence Center,” memorandum, n.d.
8. MG McChristian, “U.S. Army Intelligence Center,” briefing, 14 August 1970.
9. *Testimony before the Armed Services Subcomm. of the Comm. on Armed Services, House of Representatives, on Relocation of the U.S. Army Intelligence School from Fort Holabird to Fort Huachuca*, 92nd Cong., 2nd Sess. 21-22 (10 May 1972) (statement of MG Joseph McChristian, U.S. Army, Retired).

Next time in this series:

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



Contact and Article Submission Information



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

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

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

When submitting articles to MIPB, please consider the following:

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

What we need from you:

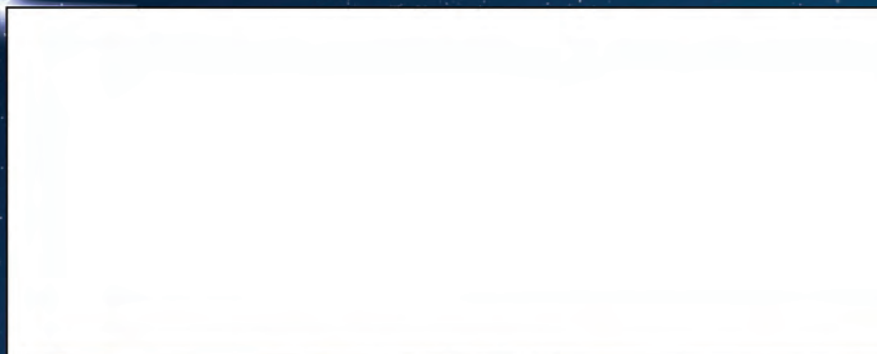
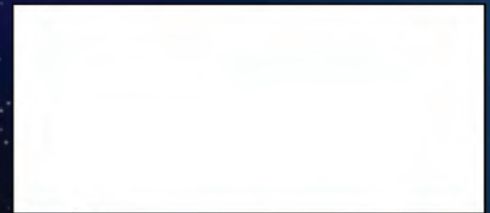
- ◆ Compliance with all of your unit/organization/agency and/or installation requirements regarding release of articles for professional journals. For example, many units/agencies require a release from the Public Affairs Office.

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

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

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

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



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

PIN:210617-000