REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 15-04-2021	**2. REPORT TYPE** Master of Military Studies (MMS) thesis	**3. DATES COVERED** *(From - To)* AY 2020-2021

4. TITLE AND SUBTITLE Keeping Army Intelligence Training Relevant in a Rapidly Evolving World	**5a. CONTRACT NUMBER** N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A
6. AUTHOR(S) Schloemann, Elizabeth K. (Major)	**5d. PROJECT NUMBER** N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068	**8. PERFORMING ORGANIZATION REPORT NUMBER** N/A
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

To attain a competitive edge in deterring or fighting a peer threat, training is the most critical factor in generating a force capable of dominating the systems-saturated environment of a future fight. The Army must learn lessons from past evolutions and become less resistant to change. A reform program that emphasizes training, specifically with emerging technologies and a heavy focus on joint and combined high intensity conflict that also maximizes the capabilities of all three Army components, can reverse the erosion in intelligence readiness – a high-intensity conventional war will not forgive a force that achieves intelligence proficiency only once it is immersed in a fight.

15. SUBJECT TERMS

Army Intelligence; Great Power Competition; Modernization; Army Training

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			USMC Command and Staff College
					19b. TELEPHONE NUMBER *(Include area code)*
Unclass	Unclass	Unclass	UU		(703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Keeping Army Intelligence Training Relevant in a Rapidly Evolving World

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Elizabeth K. Schloemann

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:
Dr. Richard Hegmann
Approved: Richard Hegmann
Date: 15 APRIL 2021

MMS Mentor Team and Oral Defense Committee Member:
Lt.Col. John Nash
Approved: John Nash
Date: 15 APRIL 2021

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Keeping Army Intelligence Training Relevant in a Rapidly Evolving World

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Elizabeth K. Schloemann

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:
Dr. Richard Hegmann
Approved: ____
Date: ____

MMS Mentor Team and Oral Defense Committee Member:
Lt.Col. John Nash
Approved: ____
Date: ____

Executive Summary

Title: Keeping Army Intelligence Training Relevant in a Rapidly Evolving World

Author: Major Elizabeth Schloemann, United States Army

Thesis: A transformation in the Army intelligence corps' approach to training will help it achieve proficiency in preparation for high-intensity conventional combat against a great power through emerging technologies courses, expanded continental intelligence architecture, refined capabilities requirements for more intuitive systems, emphasized garrison training time, joint and combined exercises at all echelons, and an innovative application of the total Army force.

Discussion: Informed by two interviews with senior Army intelligence experts, as well as historical and future doctrinal concepts, this paper assesses gaps and successes in Army intelligence training. While history provides many lessons on the evolution of intelligence support to warfare, the current strategic environment is evolving at such a rapid pace that intelligence training must keep stride in order to ensure analysts and collectors can proficiently meet the needs of a future fight. From the onset of the post-9/11 Long War in Iraq and Afghanistan, the Army's intelligence architecture underwent a rapid evolution that included massive innovation in systems, and eventually a revision of cognitive competencies. While the Army worked towards providing adequate training opportunities to meet the demanding needs of the intelligence corps, the rising counterinsurgency threat quickly overwhelmed its intelligence capacity as a whole. This led to another round of introspection and innovation, driving changes to the intelligence architecture and training requirements to complement the new Regionally Aligned Forces concept. However, despite the transformations of the past twenty years, the intelligence corps faces a similar need for reform to meet the threat of a potential Great Power conflict – its design, systems, and training are not adequate to meet the threat without another rapid evolution. Key intelligence leaders are driving the requirements for new force design concepts and new intelligence systems, to include upgrades, which give the Army overmatch against a peer threat, as well as taking a hard look at what proficiency really looks like. This paper will explore the history behind the current intelligence training architecture, depict the successes and failures that led to the most recent changes, look at the implications of future intelligence concepts and platforms on the training architecture, and make recommendations to improve overall Military Intelligence (MI) readiness through structure and training improvements.

Conclusion: To attain a competitive edge in deterring or fighting a peer threat, training is the most critical factor in generating a force capable of dominating the systems-saturated environment of a future fight. The Army must learn lessons from past evolutions and become less resistant to change. A reform program that emphasizes training, specifically with emerging technologies and a heavy focus on joint and combined high intensity conflict that also maximizes the capabilities of all three Army components, can reverse the erosion in intelligence readiness – a high-intensity conventional war will not forgive a force that achieves intelligence proficiency only once it is immersed in a fight.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Illustrations

Page

Table of Contents

Page

Preface

Throughout my time in the Army, the various leadership positions I served in from my very first assignment on all required me to be responsible for intelligence training in one fashion or another. The constant roadblocks to proper intelligence training were incredibly frustrating, causing me to question why the process was so difficult, especially since training (as a component of readiness) is the Army's top priority. My time as the S2 in 5th Armored Brigade, a Mobilization Force Generation Installation (MFGI) platform, was very eye-opening as I discovered just how different the National Guard force is from the Active-Duty force – not better or worse, but vastly different.

With the first decade of my career totaling nearly six years of S2 time, intelligence training is near and dear to my heart. From Foundry to platforms, I got to experience every aspect of training before I even became a major. While I will not claim to be an expert by any means, my unique experiences gave me a perspective very few intelligence officers get. My friend and fellow officer, MAJ Nicole Hash has been asking me to write about intelligence training based on these experiences, so it is with gratitude for her friendship and the many discussions we had in developing intelligence training that I thank her for encouraging me to write this.

I would be remiss if I did not also thank my dear friend, LTC (R) Scott Glenn, who has been a reliable sounding board for me throughout this process, particularly regarding Army policy, training practices, all things National Guard, and mission command systems. His willingness to provide unique perspectives to some of the problem areas identified in this paper was very much appreciated, along with his subject matter expertise in systems architecture.

Of course, I would not have been prepared to take on the role of brigade S2 at 5th Armored Brigade if it had not been for my old boss and mentor, COL James Welch, who also agreed to conduct an interview for my paper. I would like to give a special thanks to COL Welch for the time he has spent mentoring me over the years, and for showing me what senior intelligence officers should do to train and prepare their formations.

I would also like to say thank you to my thesis advisor, Dr. Richard Hegmann, who helped guide me in the right direction, ensuring that the important things I had to say were articulated in my paper. The countless hours and last-minute meetings were crucial in keeping me on track and on time. And, finally, thank you to Lt. Col. John Nash for agreeing to be part of my advisory team and giving me the military intelligence perspective that my paper requires.

Introduction

In the current global Great Power Competition environment, which comes with an increasingly dangerous anti-access/area denial (A2/AD) threat, the U.S. Army can no longer see as far as it can shoot. This expanding A2/AD threat posed mostly by China and Russia, respectively, prompted the U.S. Secretary of Defense to write a new National Defense Strategy (NDS) in 2018, which included a complete overhaul of the military's focus and force structure, turning away from its counterinsurgency (COIN) focus for the first time in decades, and focusing on the possibility of a high-intensity conflict. With the Army's new focus on the Indo-Pacific theater and a potential peer threat, it has re-evaluated its intelligence systems and architecture, prompting the development of faster, smarter, and more portable equipment and software. With the promise of new technology, and a shifting focus to corps and theater level intelligence from the previous COIN focus on division and brigade level collection and analysis, the Army will need to place new emphasis on modernizing its training architecture in support of these new developments.

While significant efforts have been made to improve Army intelligence in the last decade, both in the area of intelligence collection and production as well as the existing training architecture, some areas remain fundamentally flawed, creating instability and unpredictability when it comes to training a proficient force. The most vulnerable areas as the Army moves into the future are its dependence on low density contractor support, risk aversion in a training environment, complacency stemming from a generation of COIN, component inequities, and the ability for the training architecture to keep pace with emerging technologies. This paper will explore the history behind the current intelligence training architecture, depict the successes and failures that led to the most recent changes, look at the implications of future intelligence concepts and platforms on the training architecture, and make recommendations to improve overall Military Intelligence (MI) readiness through structure and training improvements.

This paper's premise is that Army intelligence training is based on two fundamental areas – cognitive skills and technical skills. An analyst can be a master in one of these fundamental areas and still not be a proficient analyst. Analysts must achieve proficiency in both areas to be considered fully proficient. For example, an analyst who figures out the precise location of an attack, but cannot explain how he came to this conclusion is ineffective because the commander will not act on the information, considering it to lack reliability. Likewise, an analyst who spends months learning how to operate a system, but does not understand how to use the data it produces will not be able to provide any useful information to the commander. The Army's efforts to bridge the gaps in training between these two fundamental areas has made considerable progress but still falls short in meeting the demanding needs of a future fight.

Another important distinction to make is which training "domain" this paper focuses on. The Army defines the operational, institutional, and self-development domains as the three areas in which training can occur for the professional development of competent, capable military leaders (see Figure 1 on the following page). The issues that will be discussed in this paper focus solely on training in the operational domain, with the recognition that institutional training does have a significant impact on training in the operational domain. Therefore, while the United States Army Intelligence Center of Excellence (USAICoE) plays a vital role in Army intelligence training, its effectiveness is not being assessed in this paper. Self-development in terms of training to prepare for a future war should be encouraged at the unit level, but will be absorbed into the recommendations proposed for improving operational training.

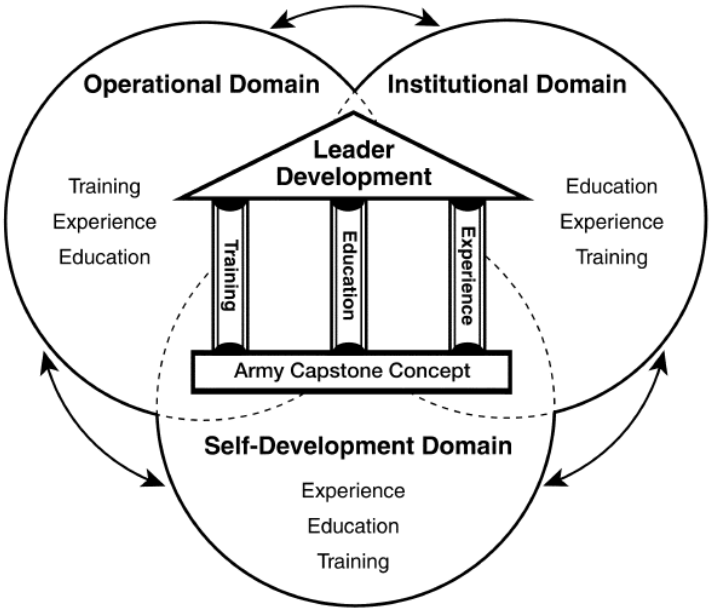


Figure 1. Army's Leader Development Model
Source: DA Pam 350-58, 2.

Intelligence Training from the Iraq War Until Now

The Rise of Automated Systems

The lessons of past wars illustrate the importance of innovation in warfighting, especially when it comes to gaining overmatch. Historically, winning armies were the ones who developed new, more effective tactics, weaponry, transportation, or logistics capabilities. This innovation ventured into the realm of computers and automated systems around the second world war, while throughout the Cold War, America's competition against the Soviet Union and communism globally drove the invention of the technologies still used by the military entering the 21st century. But America had not fought a COIN fight since Vietnam, and the failures of that war loomed large over the Army entering the Iraq War, an Army organized and equipped for a conventional fight. The Army quickly realized its intelligence systems and training were inadequate to defeat its new enemy – one not fazed by America's superpower status and its nuclear dominance. It had to adapt to compete in the unfamiliar environment, seeking overmatch through a wave of new automated intelligence systems.

When the Iraq War began, the Army grew rapidly to meet the needs of the fight. Along with a growth in numbers, the Army ushered in a new era of battlefield systems architecture, to include DCGS-A, Command Post of the Future (CPOF), and Blue Force Tracker (BFT). This modern digital architecture gave intelligence analysts a wealth of information at their fingertips, which streamlined analytical processes and gave commanders significantly better situational awareness of the battlefield, beyond even Operation Desert Storm a decade prior.[1] However, several years into the Iraq war, development of analysts' reasoning skills began to fall behind the progression curve of digital systems.[2] The Army developed a capability gap in analytical reasoning as analysts, who were trained to fight conventional battles, were suddenly faced with a completely different doctrinal concept – COIN – and an ambiguous, complex enemy and environment. Despite having systems that provided data and helped develop products, analysts lacked intelligence training in key areas, such as reasoning and critical thinking.

While systems give analysts an advantage in data management, data has no meaning until it has been processed into information. Likewise, information can overwhelm a commander until analysts turn it into actionable intelligence – a skill that requires well-developed critical thinking and reasoning skills. The principle applies from the tactical to the national levels. In fact, during Colin Powell's time as Secretary of State, he said in his opening remarks before the Senate Governmental Affairs Committee, "the Intelligence Community must provide insights and value added to the information that we already collect through diplomatic channels. When the

[1] MAJ George E. Lewis III, 2005. *Army Intelligence Analysis, Transforming Army Intelligence Analysis Training and Doctrine to Serve the Reasonable Expectations*. Monograph, Fort Leavenworth, KS: School of Advance Military Studies, 3.
[2] Lewis III, *Army Intelligence Analysis,* iii.

intelligence community weighs in with less than this level of expertise, it is a distraction rather than an asset."[3] He considered the analysis piece so important, he went on to state, "to do my job, I need both tailored intelligence support responsive to, indeed, able to anticipate my needs, and I need informed, competitive analysis."[4]

However, a decade into the Global War on Terror (GWOT), the Army continued to outpace analytical acumen with new systems designed to improve intelligence collection. In 2012, LTG Mary Legere, then Army Deputy Chief of Staff for Intelligence (G-2), took a hard first look at the strategic landscape the U.S. was facing outside of the wars in Iraq and Afghanistan, recognizing that the Army had not been preparing its analysts to address growing threats on the horizon, such as North Korea and Iran.[5] The implications of the changing operational environment triggered the fielding of more capabilities to add to the Intelligence, Surveillance, and Reconnaissance (ISR) toolkit, as well as advancements in cyber and DCGS-A. Training became a logistical feat too great to maintain at the BCT level and below, which meant the majority of these systems were relegated to the new (in 2012) Expeditionary-Military Intelligence Brigade (E-MIB).[6]

The E-MIBs had the personnel to train and use these systems routinely, and LTG Legere's idea was that the E-MIBs would serve as enablers for their aligned divisions and brigades in a deployed environment. While Full Motion Video (FMV), biometrics systems, and other critical capabilities greatly enhanced situational awareness of the battlespace, analysts typically only achieved MOS proficiency in theater as a result of the demands during

[3] Colin L. Powell, Opening Remarks by Secretary of State Colin L. Powell Before the Senate Governmental Affairs Committee, U.S. Department of State, Office of the Spokesman, Washington, D.C., 13 September 2004.

[4] Powell, Opening Remarks.

[5] Mary, A. Legere. "Army Intelligence 2020: Enabling Decisive Operations while Transforming in the Breach." *Army Magazine* 62, no. 10 (2012): 165-169.

[6] Legere, Army Intelligence 2020.

deployments, with the exception of those assigned to an E-MIB or a Military Intelligence Brigade – Theater (MIB-T).[7]

In MAJ George Lewis' analysis of Army Intelligence training at the time, he compared the role of an analyst to a chess grand master, forecasting an opponent's next moves based on skill and intuition, recognizing patterns that years of experience have trained their brains to seek out.[8] However, when his monograph was published in 2005, critical thinking was one of the least trained skills for Army intelligence analysts, even though agencies within the IC had recently adopted it as a core competency. For the Army, however, analysts were still lacking analytical proficiency during deployments throughout the following decade.[9] In fact, it was seven years after Lewis' diagnosis when the Army had finally embraced critical thinking and reasoning skills by publishing its core competencies: *intelligence synchronization*, *intelligence operations*, and *intelligence analysis*.[10] Within the core competency of *intelligence analysis,* critical thinking would finally be included as one of three critical components:

1) *"Critical thinking*. Critical thinking is essential to analysis. Using critical thinking, which is disciplined and self-reflective, provides more holistic, logical, and unbiased analysis and conclusions. Applying critical thinking ensures analysts fully account for the elements of thought, the standards of thought, and the traits of a critical thinker.
2) *Embracing ambiguity*. Well-trained analysts are critical due to the nature of changing threats and operational environments. They must embrace ambiguity and recognize and

[7] Maria C. Lytell, Susan G. Straus, Chad C. Serena, Geoffrey E. Grimm, James L. Doty III, Jennie W. Wenger, Andrea M. Abler, 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.
[8] Lewis III, *Army Intelligence Analysis*, 24-25.
[9] Lewis III, *Army Intelligence Analysis.*
[10] Department of the Army, *Intelligence,* ADP 2-0 (Washington, DC: Department of the Army, 2012), 6.

mitigate their own or others' biases, challenge their assumptions, and continually learn during analysis.

3) *Collaboration*. Commanders, intelligence and other staffs, and intelligence analysts collaborate. They actively share and question information, perceptions, and ideas to better understand situations and produce intelligence. Collaboration is essential to analysis; it ensures analysts work together to effectively and efficiently achieve a common goal. Often analytical collaboration is enabled by the intelligence enterprise."[11]

Foundry Program

With new systems and a complex unconventional fight driving the Army's demand for intellectual dominance, it had to find a way to train its analysts properly – efficiently, expertly, and *en masse*. The Army began its Foundry Pilot in 2006, realizing it needed trained instructors outside of the traditional schoolhouse setting, ready to train the operational force on the most up to date tactics and systems at the speed in which they were deploying. [12] As written in Army Regulation 350-32, *Army Foundry Intelligence Training Program*, "The Foundry Program provides training electives that sustain and improve the technical intelligence skills of military and civilian Army personnel, who conduct, supervise, or support authorized Army intelligence activities."[13] The Army integrated its Foundry instructors into the Operation Inherent Resolve (OIR) and Operation Enduring Freedom (OEF) theaters, in order to provide current, relevant intelligence training through a rich offering of courses that covered the full spectrum of intelligence operations.

[11] ADP 2-0, 2012, 7.

[12] Department of the Army, Army Foundry Intelligence Training Program, AR 350-32 (Washington, DC: Department of the Army, 2010).

[13] Department of the Army, Army Foundry Intelligence Training Program, AR 350-32 (Washington, DC: Department of the Army, 2015), 10.

Through Foundry, the Army did more than temporarily patch a gap in intelligence proficiency – it created a force multiplier that has persisted for nearly two decades and continues to improve cognitive and system proficiency within the intelligence corps, keeping pace with emerging technologies and tactics in the operational training setting. Intelligence officers could now train their analysts through a number of courses in the Foundry catalog, including special certifications and Live Environment Training (LET). Foundry also offered Mobile Training Teams (MTTs) that could facilitate onsite training for a unit, which meant more analysts could receive training at a significantly reduced cost.

The project was so successful that the Army permanently implemented the Foundry Program in 2008. By its third year, the number of Soldiers receiving Foundry training had multiplied by five.[14] Under the Foundry Program, intelligence training funds were apportioned under budgets separate from unit funds and managed all the way down at the brigade level, requested annually through the unit hierarchy. If a unit budgeted their Foundry funds properly, they could send their Soldiers to any number of intelligence training courses throughout the fiscal year, integrating classroom instruction and Live Environment Training into the unit's intelligence training plan.

Doctrinally, the Foundry Program's mission is to "provide timely and relevant advanced intelligence skills training in [Signals Intelligence] SIGINT; [Geospatial Intelligence] GEOINT; [Counterintelligence and Human Intelligence] CI/HUMINT; [Open Source Intelligence] OSINT; Analysis/Fusion, and Information Operations [IO] to Army MI Soldiers."[15] This mission encompasses the Army G2's goal of keeping all Army components actively engaged with "no

[14] United States Army Intelligence and Security Command, Foundry Briefing, August 12, 2009.

[15] "Foundry," Intellipedia, accessed March 29, 2021, https://intellipedia.intelink.gov/wiki/Foundry.

MI Soldier at rest, no cold starts."[16] At a time when deployments were cycling rapidly through the Active-Duty, National Guard, and Reserve forces combined, ensuring that all MI Soldiers had available training opportunities was critical to force readiness requirements.

Through Foundry, the Army addressed the concern of providing intelligence training across the components, incorporating National Guard and Reserve MI training under the Military Intelligence Reserve Command (MIRC). All three components now had equal access to intelligence training funds and courses. In the MIRC's early integration of Foundry, the scope was limited either by a misunderstanding of the true intentions of the program or a lack of available resources, which can be seen in the MIRC's 2020 Vision and Strategy:

> "The program serves as an MI skills advance course to prepare Army MI Soldiers for deployment. It has served to get Soldiers not only to refine and improve their technical skills, but to provide an unprecedented degree of access and focus on the threat that supported units will confront on deployment."[17]

While the Foundry Program was designed to ensure "no MI Soldier at rest," in support of Army Force Generation (ARFORGEN) cycle requirements, deployment training was not its sole purpose. The MIRC's understanding of what Foundry was designed for may have contributed to its unique investment in the Army Reserve Intelligence Support Centers (ARISCs), developing a vast intelligence training enterprise with National Intelligence Agency reach-back capability. Though ARISCs already existed in a lesser capacity, this initiative boosted the enterprise to manage the mounting requirements of deployments in multiple theaters of operation. The ARISCs, doubling as Intelligence Readiness Operations Centers (IROCs), let reserve MI

[16] Department of the Army, *Army Intelligence Training Strategy*, (Washington, DC: Department of the Army, 2013).
[17] Department of the Army, *MIRC 2020: Military Intelligence Readiness Command Vision and Strategy*, (Washington, DC, 2011), 11.

Soldiers "leverage and augment the organic processing capabilities of forward-deployed intelligence collection systems through continuous targeting over watch of networked threats."[18]

Unfortunately, the interpretation of ARISCs and Foundry as platforms for deployment training meant that intelligence training within the Army Reserves and National Guard was limited to pre-mobilization requirements in the Available year of the ARFORGEN cycle, as depicted in Figure 2. Year one was dedicated to resetting and refitting post-deployment, with years two and three focused on recruiting and retention, along with training basic warrior tasks and battle drills and one major training exercise per year during the annual training period.

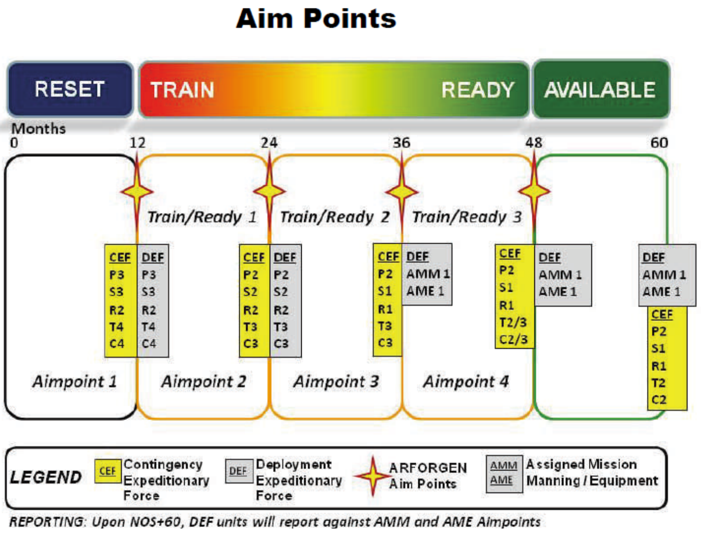


Figure 2. National Guard ARFORGEN Aim Points
Source: National Guard Bureau Implementing the Army Force Generation Model in the Army National Guard

The annual training exercise has historically been determined by the unit commander and aligned with the higher headquarters guidance, but rarely required non-MI units' intelligence enterprises to refresh their MOS-specific skills and proficiencies, which led to skill atrophy over a three-to-four-year period. While ARISCs and Foundry have been available for units to use throughout all phases of the ARFORGEN cycle, the use of these resources is driven by command requirements and higher headquarters' policy.

[18] Army, *MIRC 2020*, 16.

Within the Active force, on the other hand, the ARFORGEN cycle was only three years, theoretically giving analysts' skills less time to atrophy.[19] However, analysts in the active component were subject to Permanent Change of Station (PCS) moves that sometimes meant long periods without deployments. Additionally, with such a short ARFORGEN cycle, the focus of intelligence at a unit's home station was on resetting and refitting, which included many personnel moves. Scheduling Foundry training had to be deliberate and purposeful or it was overcome by more pressing and visible requirements.

Company Intelligence Support Teams (COISTs)

As the Army sought to build cognitive capacity within the MI Corps through the Foundry Program, it also realized that intelligence was a commodity in high demand during OEF and OIR. Within the size limits of its existing force structure, the Army sought creative ways to include additional intelligence capacity for lower echelons, which spawned the development of COISTs. Maneuver units on the ground were overwhelmed by unconventional attacks, to include improvised explosive devices (IEDs), suicide bombers, and vehicle-borne IEDs (VBIEDs). In fact, three out of five coalition force deaths in Iraq were caused by IEDs, as well as a quarter of the deaths in Afghanistan.[20] COISTs were implemented to add to the intelligence capacity of maneuver units in order to improve predictive analysis on the ground. The Army had the capacity to conduct intelligence training through Foundry, but lacked the capacity of intelligence Soldiers at the company level needed to plan safe routes.

The Army viewed COISTS as a way to increase intelligence proficiency at the tactical level. The COISTs provided a collection and processing, exploitation, and dissemination (PED)

[19] Andrew Feickert. "Army Drawdown and Restructuring: Background and Issues for Congress*." Current Politics and Economics of the United States, Canada and Mexico* 16, no. 4 (2014): 567–., 10

[20] Sheila M. Bird and Clive B. Fairweather. "Military Fatality Rates (by Cause) in Afghanistan and Iraq: A Measure of Hostilities." International Journal of Epidemiology 36, no. 4 (2007): 841-846. doi:10.1093/ije/dym103. https://doi.org/10.1093/ije/dym103.

element at the company level, while force structure still limited intelligence personnel to the battalion level and higher. The concept proposed that a maneuver battalion in a BCT would allocate two all-source analysts and one HUMINT collector from its own battalion headquarters' intelligence section down to each maneuver company, and that several Soldiers from the maneuver company would train and certify in Intelligence Preparation of the Battlefield (IPB), Pattern of Life, Link Analysis, and other key intelligence tasks.

COISTs, like many other good ideas, looked great on paper, but in practice the concept fell apart, according to many Center for Army Lessons Learned (CALL) accounts of units failing to implement COISTs during combined training exercises.[21] For one, the relationship between a battalion S2 and a maneuver company commander is not a command relationship. Unless directed by the battalion commander, a maneuver company commander had no requirement to actually send their Soldiers to intelligence training, even if the battalion S2 developed a COIST training plan for their Soldiers. On the other hand, the battalion S2 sections already suffered a lack of manpower to address all the requirements in their purview, so distributing their Soldiers down to the company level was viewed as a burden. Though the intent was that the COISTs would stand up during deployments, the training had to occur in a garrison environment pre-deployment, and the relationships were supposed to be cultivated during this period. In some cases, however, units only realized the value of COISTs after they had deployed, which led to dysfunctional teams being thrown together without proper training. In order for COISTs to be effective, they needed buy in from the commanders and the battalion S2 throughout the ARFORGEN cycle.

[21] Elizabeth A. Brunette, "Intelligence Support to Sustainment," *News from the CTC,* (Department of the Army, Center for Army Lessons Learned, 2017). Captain Brunette details intelligence inefficiencies during her experience from multiple Combined Training Center (CTC) rotations while serving as a battalion S-2, highlighting the need for COISTs in support of logistics on the battlefield. Her account comes eight years after the implementation of COISTs and underscores the continuing omission of COISTs in combat operations.

Distributed Common Ground System – Army (DCGS-A)

While Foundry and COIST provided additional training opportunities, DCGS-A provided analysts with a processing platform. Though considered the Army's staple intelligence production platform, DCGS-A has been the source of many grievances across the intelligence corps for the past two decades. To be sure, as a production platform, DCGS-A has a suite of applications that, when trained properly, increase a unit's analytical processing capabilities and speed immensely. However, the lack of training coupled with the time it takes to train, as well as unavailability of contractors to operate the system, have been its greatest failures as a platform.

In its prime (the early Iraq war), DCGS-A was heralded by the Army as a remarkable system that offered intelligence analysts a multitude of capabilities in one "portable" platform, as well as access to data stored on 1 of 13 standalone theater databases (unit servers had to be configured to connect to a specific theater database). The data that analysts entered into the system was meant to feed into these larger servers where it would be aggregated and synchronized for battlefield dissemination. As the battlefield changed over the years, the DCGS-A Program Executive Office (PEO) tried to keep up with the requirements analysts were facing down range, but the changes out-paced the rate of technological improvements.

The first major change occurred soon after the Iraq War began, when the PEO realized very quickly that intelligence staffs operating at the battalion level required a "smaller, lighter, more mobile (laptop-based) intelligence analysis automation system" as opposed to the earlier version of DCGS-A that was being used in Kosovo at static locations like Camp Bondsteel since the system was acquired in 2001.[22] This "smaller" laptop version of DCGS-A made it easier to move across the battlespace, but still came with 500 pounds of equipment and required a 35T

[22] Chet Brown. "Change Is Constant-Yet Some Things Never Change." *Military Intelligence Professional Bulletin* 46, no. 1 (2020): 75–78, 76.

(intelligence systems maintainer/integrator) or an FSR to operate the server stacks in order for analysts to use the laptops.[23] However, the system "largely built upon technology from the 1990s…was difficult to use, crashed easily, and could not quickly upload information from disparate databases," which led to analysts abandoning the system altogether. [24]

Around 2010, Palantir began to gain recognition on the battlefield as a more intuitive intelligence processing platform than DCGS-A, particularly in Special Operations Forces (SOF) units. Army analysts wanting to use Palantir for its ease of use were disappointed when the Army insisted that DCGS-A provided all the capabilities they needed, seemingly ignoring the fact that the system was too cumbersome to use. They would spend the next decade fighting for a better system, while trying to figure out the best way to use the one they had.

The two largest issues that arose from DCGS-A as the Army's Program of Record for intelligence processing were that it was too complex to set up and operate, limiting its use in a garrison environment, and that its applications were not intuitive enough to learn in a condensed training timeline, as seen when Major General Michael Flynn (former intelligence officer to U.S. and NATO forces in Afghanistan) undertook the effort to transition the force to Palantir.[25] These would remain issues that made intelligence training a significant hurdle in garrison.

Aside from requiring an FSR or 35T to set up and operate the DCGS-A servers, the basic level operator block of instruction was an 80-hour course. Any system that requires 80 hours of training to reach a baseline level of proficiency is not intuitive enough to support a rapid deployment to a high-intensity conflict in a "fight tonight" scenario. This level of proficiency would need to be maintained throughout the year, but lacking FSRs and trained 35Ts, the total

[23] John R. Hoehn, Nishawn S. Smagh. Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition, CRS Report No. R46389 (Washington, DC: Congressional Research Service, 2020), 24.

[24] David W. Barno, and Nora Bensahel. *Adaptation Under Fire: How Militaries Change in Wartime.* New York, NY: Oxford University Press, 2020, 168.

[25] Barno, Adaptation Under Fire, 168.

Army force is not designed to sustain this level of training at the unit level. Foundry offers a solution to this dilemma, maintaining fully functional DCGS-A systems, while also maintaining the newest fielding intelligence systems for training purposes, but this is less than ideal, since units would not be training on their own systems and building maps or products for future use.

New Equipment Training/New Equipment Fielding (NET/NEF)

The Army's current method for training and fielding new Intelligence systems has been used for several decades: New Equipment Training and Fielding. For brand new systems, this gives analysts a baseline knowledge of what the system can do, how to set it up, and how to use it. Unless a unit develops training plans to incorporate these systems, the NET/NEF tends to be the only time a unit conducts training until they conduct a field exercise or collective training event. Unfortunately, NET/NEF training is very basic and often does not replicate the environment in which the systems will be used. If units rely on NET/NEF as their only source of training, they will not reach proficiency on their intelligence systems until they deploy – a collective training event, while useful, is not long enough to develop proficient skills on a complex system.

DCGS-A is one of the Army's intelligence systems that is constantly upgraded through NET/NEF, which also poses planning and logistics problems. One such challenge is that unit senior intelligence officers are responsible for validating equipment versions, scheduling fielding cycles, and ensuring their property books are updated properly. For a variety of reasons, this process is laden with roadblocks, especially when there is a high rate of turnover in a unit. However, once complete, a unit will receive an additional two-week block of instruction on the new DCGS-A version they received. This is one of the two levels of training that occur – systems maintainer and end user. The end user training gives analysts a baseline of training that, at a minimum, should give them enough expertise to be able to operate the system on their own, provided they have the instruction manual available for reference.

However, new equipment training is not equivalent to field training. For example, during NET/NEF for the One System Remote Video Terminal (OSRVT), training occurred indoors. Realistic application of the system requires outdoor setup to ensure line of sight communication with Unmanned Aerial Systems (UAS), but that was not included in the training. Analysts would have had to conduct an additional level of training by taking their systems out to a field training environment at least semi-annually to ensure they maintained proficiency. Nevertheless, time and resources are rarely devoted to this level of training due to garrison requirements that often eclipsed realistic military training.

Gaps in between training periods are particularly concerning when taking into account the "forgetting curve," or the rate at which information is forgotten from the time learners consume it.[26] In an article examining the importance of the skills gap in developing training programs, author Megan Davidson describes how the "forgetting curve" impacts learners over time:

> "Studies…have found that within a single hour of instruction, most trainees will have forgotten about 50% of what was presented. This purging of information continues over the course of the day, as 70% of new information has been forgotten within the first 24 hours. After a week, an average of 90% of what trainees learned in their training session is gone."[27]

With this in mind, intelligence officers and instructors must understand the impacts of the forgetting curve on training events, finding ways to reinforce learning continuously. For systems

[26] Megan Davidson. "Avoiding the Forgetting Curve." *Foundry Management & Technology 144, no. 9* (2016): 120.
[27] Davidson, "Forgetting Curve," 120.

learning, this means that intelligence leaders will need to ensure their analysts have a way to get time training on intelligence systems throughout the year and not just during classroom instruction and collective training events. While there are a variety of ways to incorporate training into an already overloaded unit schedule, intelligence officers must get creative in seeking out solutions that enable their analysts to maintain skills proficiency.

Realistic Military Training

The high-intensity and lethal environment of a great power conventional war places a premium on training in a challenging environment. Training in controlled environments, such as a classroom or a range, gives analysts repetitions and sets in their individual and collective tasks that build on their proficiency levels. But realistic military training replicates the battle space analysts will be operating in, raising their proficiency to meet the metric of "trained" more adequately. Semi-permissive environments add complexity and unknowns to training, forcing analysts to adapt and overcome obstacles that are missing from controlled training environments. One aspect that remains ever-present in a semi-permissive environment is a heightened level of anxiety and alertness, due to the inherent risks involved in operating outside the constraints of a military installation. Many commanders see these risks as a cause for concern, but the risks are minimal compared to the risks of deploying to a hostile environment unprepared. With a proper understanding of how to run realistic military training, most risks can be mitigated through planning, coordination, and classroom instruction.

The Kosovo Case Study found later in this paper explores a real training scenario that incorporated realistic military training into a collective training event successfully. An area of stagnation in intelligence training is in making the training realistic. One barrier to this is risk aversion. Commanders, with good reason, are very aware of the risks that come with intelligence training, specifically under Intelligence Oversight, which controls intelligence collection on US Persons and is regulated under Executive Order 12333 and Army Regulation 381-10, U.S. Army Intelligence Activities. These risks have always existed under the surface of every intelligence training plan, but in 2015, the Army's Jade Helm exercise brought the true risks of conducting realistic intelligence training to the forefront.

Jade Helm 15 caused widespread panic across the southwest U.S. as a steady flow of press releases began to mount contradictions as to the true nature of the exercise.[28] One press release even mentioned that the Army Special Operation Forces (ARSOF) running Jade Helm would be conducting HUMINT collection on civilian populations.[29] To further ignite the fears that ARSOF was conducting HUMINT collection on civilians during Jade Helm, the logo designed for the exercise explicitly stated, "Master the Human Domain" (see Figure 3).[30]

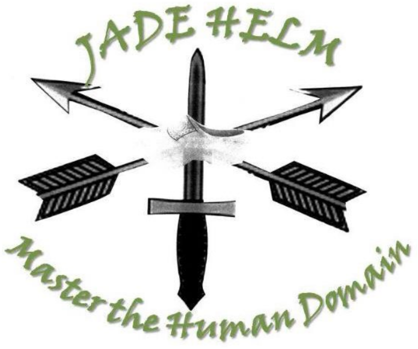


Figure 3. Jade Helm Logo
Source: Haley Jordan Richey. Operation Jade Helm: A Cultural Analysis of Public Opinion. Undergraduate Research Scholars Program. 2017, 27.

[28] Haley Jordan Richey. *Operation Jade Helm: A Cultural Analysis of Public Opinion*. Undergraduate Research Scholars Program. 2017, 5. According to Richey, "this is apparent when Lieutenant Colonel Mark Lastoria was sent by [the Pentagon in response to] Operation Jade Helm to ease tensions and fears of conspiracy surrounding Operation Jade Helm. *Yahoo News* wrote that when this meeting was being held with the intention of Lastoria reassuring citizens, they 'erupted in applause when he was called a liar,' suggesting that there is a deep mistrust within the system and its experts," (Richey, 17). She also notes that, "Despite high-ranking officials confidently and consistently reassuring the public that there is no reason to fear Operation Jade Helm, the public still feared, and some even retaliated. In fact, Texas's Governor, Greg Abbot, supported and encouraged citizens to sign up for the State 39 Guard in case there was an ulterior motive behind the military operation,"(Richey, 38).

[29] Richey, Operation Jade Helm, 5.

[30] Richey, Operation Jade Helm, 27.

Now, commanders had good reason to be wary of conducting any intelligence training exercises outside of military installations. No commanders wanted their training to become the next Jade Helm. But as disreputable as Jade Helm became, another annual off-installation intelligence training exercise has quietly persisted through the fear and hesitation, gaining recognition as one of the best intelligence exercises in the Army – "Panther Strike."

In 2019, Panther Strike had over 800 U.S. participants and an additional 110 five eye partner participants, conducting training in counterintelligence, human intelligence, geospatial, all-source and signal intelligence at Camp Williams, UT.[31] The exercise is designed as a "multi-echelon, brigade-level intelligence exercise that comes with external validation."[32] Since Panther Strike is the largest Army intelligence exercise, it must ensure that it remains relevant for the warfighters. In 2019, the exercise finally transitioned from its COIN scenario to focus on training against "an enemy with similar capabilities to the U.S. military known as a peer-to-peer foe."[33] These types of exercises will be even more critical as the Army transitions along with the rest of the service components to a joint and combined force. As intelligence platforms cross services via interoperability and sensor to shooter capabilities, the Army should look at expanding Panther Strike or creating a larger, broader exercise emulated on its design. Again, the Kosovo case study below also aims to build confidence that the benefit of challenging training is worth the risks.

[31] "341st Military Intelligence takes part in Panther Strike '19," Joint Forces Headquarters, Washington National Guard Washington National Guard, accessed on March 14, 2021, https://www.army.mil/article/223967/341st_military_intelligence_takes_part_in_panther_strike_19.
[32] Sgt. 1st Class John Etheridge, "Panther Strike 2019," accessed March 16, 2021, https://ut.ng.mil/Site-Management/News-Article-View/Article/1879562/panther-strike-2019/.
[33] Etheridge, "Panther Strike," https://ut.ng.mil/Site-Management/News-Article-View/Article/1879562/panther-strike-2019/

Intelligence Electronic Warfare Tactical Proficiency Trainer (IEWTPT)

Though realistic military training in a semi-permissive environment is optimal for training, there are instances when it is not feasible, suitable, or acceptable. For intelligence training, USAICoE designed IEWTPT to simulate the training events that cannot be conducted in a real training environment due to constraints. For example, SIGINT analysts need to train on low level voice intercept (LLVI) to maintain individual task proficiency, but such training can be difficult to schedule, plan, and conduct properly due to the space required and the risk of Intelligence Oversight violations. IEWTPT offers a simulated training environment that enables analysts to learn skill proficiency in these types of tasks, while eliminating the inherent risk of conducting live training. In some instances, units may choose to use IEWTPT to get training repetitions prior to conducting a live training event, due to the difficulty in planning and running live events. While IEWTPT was designed to remove barriers to intelligence training, it comes with its own set of problems that the Army will need to address in the coming years.

One of the benefits IEWTPT brings to the Army is that it incorporates analysts' skills into unit or joint intelligence exercises, versus exclusively intelligence exercises. While exercises conducted independently of the other warfighting functions have shown proven success in developing analyst and collector skill proficiency on a deeper level than unit training, the intelligence function must be integrated into the larger staff. IEWTPT was implemented in 2008 as a tool to provide "mission-essential skills based training to intelligence collectors and analysts" through an intelligence-driven simulation that uses both real world and simulated data.[34] As an example, training HUMINT collectors in live scenarios using U.S. Persons carries ramifications that are not easily mitigated, while training through an IEWTPT simulation would

[34] "IEWTPT Mission & Description," Program Executive Officer for Simulation, Training and Instrumentation (PEO STRI), accessed February 21, 2021, https://www.peostri.army.mil/intelligence-electronic-warfare-tactical-proficiency-trainer-iewtpt

minimize the risk of Intelligence Oversight violations, as well as minimize training time and planning factors.

While IEWTPT provides the Army a cost-effective training simulation platform, in fact the only intelligence simulation platform, it also has its shortcomings.[35] As seen previously with DCGS-A, IEWTPT relies on a very specialized group of operators to run its complex architecture. One part of the system is "the Intelligence Low Overhead Driver (iLOD), [which] interfaces with the Distributed Common Ground System-Army through the Intelligence Fusion Server stack to populate the graphics and reporting." Each of these have to be connected and operational or the entire system will be unable to function correctly. Likewise, hardware and software versions need to be compatible or they will not be able to interface.

Integrating IEWTPT into exercise development requires intelligence planners to build a scenario or provide their unit's exercise scenario to the IEWTPT contractors months in advance, which is not all that uncommon. Regular meetings would validate that IEWTPT's simulation is congruent with the overall exercise design. Part of this planning process includes incorporating individual tasks and training objectives that would need to be captured in the scenario.

For all the work that goes into developing these exercises, the actual running of each exercise should only be a matter of supervising the simulation and adjusting portions as it plays out. There are two historic problems with this. One, not all operators can operate the platforms at the same level of expertise. What a unit gets out of IEWTPT depends a great deal on the person who designs and runs the simulation. An operator with a high experience level will provide a rigorous training experience for a unit's intelligence analysts and collectors. On the other hand,

[35] "Training and Simulation: IEWTPT," General Dynamics Mission Systems, accessed on February 21, 2021, https://gdmissionsystems.com/services/training-and-simulation

an operator with a relatively low level of experience may only provide a margin of that added value.

The second problem is that this system relies on good contracting support. Poorly managed contracts had such tremendous impacts in the past as to shut down IEWTPT support for at least one entire installation, relying on contractors from other installations to travel in support of previously scheduled exercises (assuming they were not already assigned to their own exercises). Even though IEWTPT support is regionally managed, and operators, in theory, are interchangeable, there are challenges in introducing an operator to an exercise within days of the communications exercise (COMEX). This, unfortunately, happens frequently enough to be a persistent problem. A trip report from a 2016 Panther Strike exercise stated, "Unfortunately we were not able to use all GEOINT capabilities (FMV and GMTI) due to the IEWTPT Contractors already being tasked for another exercise."[36] With Panther Strike, one of the Army's largest intelligence exercises, unable to obtain adequate support, use of the platform could pose a risky gamble to units trying to incorporate it into their own exercises.

Despite these problems, IEWTPT still adds a deeper level of skill training to the Army's intelligence enterprise, giving units and Soldiers an alternative path to skill development and training repetitions to achieve greater levels of proficiency. Future development of this training platform will need to be paired with a hard look at how the support is contracted, whether the support is appropriately aligned, and how well the contractors are trained to operate the systems and adjudicate Mission Essential Task List (METL) proficiencies.

__Regionally Aligned Forces (RAF)__

As seen with the COISTs previously, the Army also made another attempt to make the most of its limited manpower by regionally aligning its forces to maximize global

[36] 300th Military Intelligence Brigade, GEOINT Trip Report for Panther Strike Exercise 02-17 June 2016.

responsiveness. With forces dedicated to aligned mission sets, they could be more exclusive with their training, focused specifically on what their region might require them to do. Overall, this helped reduce excess intelligence training that had no application within the unit's immediate purview, allowing analysts and collectors to dive deeper into training that was critical to their mission sets. However, this created a rift between units with strong intelligence officers and those without, since RAF alignment lacked prescriptive training guidance for each theater, thus creating entirely new problems that persisted for years that could have been mitigated from the onset.

In 2013, the Army made the switch from its previous active force ARFORGEN cycle to its Regionally Aligned Forces ARFORGEN cycle. The move gave the Army greater flexibility to respond to emerging threats worldwide with a dedicated and ready force. The ARFORGEN cycle shortened from three years to two years.[37] Aligning brigades to missions meant that even in garrison, intelligence analysts were working within their expertise. In an interview for this paper conducted on February 20, 2021, U.S. Army COL James Welch, who served as a Brigade S2 in 3rd Brigade, 3rd Infantry Division during its first RAF mission under NORTHCOM, said of his experience, "our intelligence Soldiers had a variety of opportunities to support daily operations for ARNORTH. These opportunities not only enabled our Soldiers to hone their skills, they became very familiar with the threats our unit might face in support of the RAF mission."

In garrison operations, the RAF missions kept analysts busy maintaining proficiencies, but other skills deteriorated as a result. Intelligence training comes with its share of risks, especially inadvertent collection on U.S. persons, which is regulated under Intelligence Oversight policies and regulations, as well as Executive Order 12333. Certain intelligence activities are limited in training environments, and RAF missions that concluded without

[37] Feickert, "Army Drawdown," 8.

deployments lacked the proper environment for certain skill training. Another area that suffered under garrison intelligence activities was systems training, particularly systems that required FSRs to even have them turned on, like the DCGS-A.

However, special skills and systems proficiency loss were not the only casualty of the transition to RAF missions. A DOD Inspector General audit of USAFRICOM RAF training exposed some serious failures that compromised the USAFRICOM mission:

> "RAF personnel supporting USAFRICOM did not receive adequate regionally aligned training to meet mission requirements in the USAFRICOM area of responsibly. Specifically, 7 of the 14 personnel from the RAF or country teams and the USAFRICOM branch chief expressed concern that RAF personnel did not always receive the necessary regionally aligned training to meet the USAFRICOM mission requirements."[38]

This problem persisted not only in USAFRICOM, and not only within the Active-Duty forces. RAF training requirements for FORSCOM were very generic, covering basic deployment requirements like SHARP and EO training, counter-IED training, and basic warrior tasks and battle drills, but FORSCOM expected the theaters to develop more detailed requirements. For example, the Foundry Intelligence Training Program is listed under FORSCOM's general RAF training guidance, but only to say that units should utilize Foundry intelligence training.[39]

The quagmire that this creates is compounded by the fact that RAF training requirements can only be generated by a given theater after its units have deployed long enough to determine if the pre-deployment training they conducted had properly prepared them to meet the mission

[38] Department of Defense, *Audit of the Training of the Army's Regionally Aligned Forces in the U.S. Africa Command*, DODIG-2019-096 (Washington, DC: Office of the Inspector General, 2019), 13.
[39] Department of the Army, Annex A to U.S. Army Forces Command (Forscom) Regionally Aligned Forces (RAF) Training Requirements 2019 (General), 2019.

requirements.[40] If done properly, a unit will reassess the pre-deployment training they conducted when they are well into their mission or when they return from a deployment and are really only focused on reset and refit requirements. This process relies on units to make a deliberate, unrequired assessment to submit to their Geographic Combatant Command (GCC), with no clear understanding of what that process looks like.

Figure 4 below demonstrates the impacts of just one unit or theater neglecting to provide updates to FORSCOM on changing mission requirements in a nine-month cycle. If the problem persists over more than one deployment, the number of units that deploy without appropriate training continues to expand for each rotation that updates are not submitted for publication through FORSCOM.

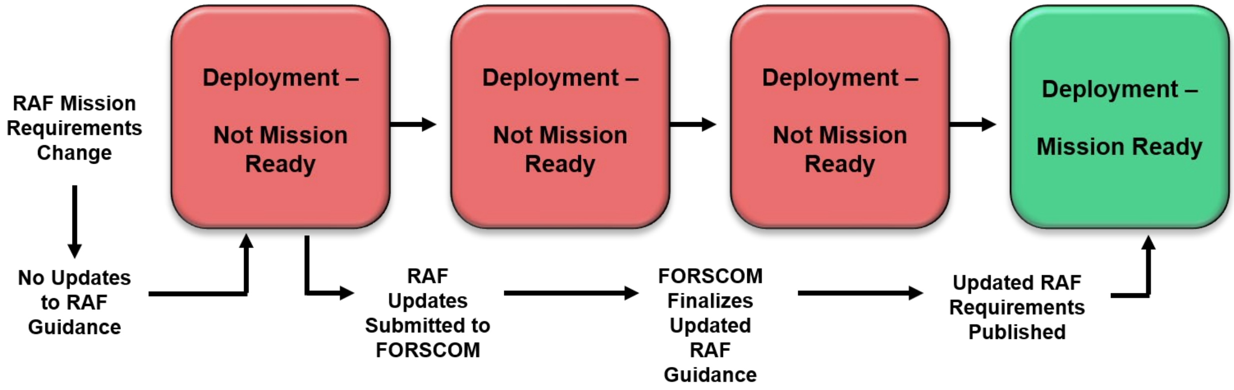

RAF Mission Requirements Change
No Updates to RAF Guidance
Deployment – Not Mission Ready
Deployment – Not Mission Ready
Deployment – Not Mission Ready
Deployment – Mission Ready
RAF Updates Submitted to FORSCOM
FORSCOM Finalizes Updated RAF Guidance
Updated RAF Requirements Published

Figure 4. Army RAF Requirements Update Cycle Impacts

This is seen in many instances, even apart from the Inspector General audit of USAFRICOM's RAF training shortcomings. There are many units impacted each year, highlighting areas in which RAF training is insufficient across multiple theaters, either due to changing mission requirements that are not adequately captured or due to vague training guidance that fails to capture the actual training that is needed.

[40] Department of Defense, *Pre-Deployment Training and Theater Entry Requirements*, DOD Instruction 1322.32 (Washington, DC: Department of Defense, 2020) 7.

One mission in particular that is worth a closer look is the Kosovo Forces (KFOR) mission, in which the intelligence element consists of both a Brigade S2 and a Division Analysis and Control Element (ACE). The theater-specific RAF training guidance for KFOR home station training vaguely listed required intelligence training tasks that leave room for interpretation and lack robustness. The following Kosovo case study provides a comprehensive look into RAF training guidance issues, including specific examples of most of the previously listed intelligence training problems, how the issues were managed, and what approaches were used to prevent problems from repeating.

Kosovo Forces Case Study (KFOR 21 – KFOR 25)

To understand the limitations imposed by each of the previously described intelligence training concerns, the evolution of intelligence training in regard to the Kosovo Forces mission highlights the culmination of each of these issues in one scenario. The changes from 2015 to 2018 were the result of meticulous planning and constant revision, addressing training requirements, as well as finding inventive ways to train individual and collective tasks prior to the implementation of current intelligence training concepts that will be described in the next section. Even though these changes made the training much more effective, challenges like risk aversion and FSR support still persisted by KFOR 25, reducing the effectiveness of training, despite the efforts to overcome them. This case illuminates the need for a wholistic approach in improving training to meet proficiency demands, as well as ensuring the training and revision process is continuously evaluated and modified for effectiveness.

KFOR Mission

The KFOR mission is assigned to the Army National Guard, which, during the period of this case study (2015 – 2018), maintained a rotational command of the Multi-National Battle Group – East (MNBG-E). The National Guard has established nine-month rotations to the region and each rotation contains an intelligence manning requirement of over 50 personnel, consisting of All Source (35F), HUMINT (35M), CI (35L), and GEOINT (35G) analysts, as well as an intelligence systems maintainer/integrator (35T). Each KFOR rotation is given a numerical designator, identifying which rotation it is (e.g., KFOR 21 is the 21st rotation of the mission).

The KFOR mission consists of three main tasks: 1) Maintain a safe and secure environment (SASE), 2) Ensure freedom of movement (FOM), and 3) Enforce the military technical agreement (MTA). These tasks specifically support the North Atlantic Treaty Organization (NATO) peacekeeping operation, which focuses on building stability in the region.

Training Guidance

RAF training guidance for Kosovo is outlined in FORSCOM's training requirements, which consists of FORSCOM overall requirements (Annex A and B), EUCOM theater-specific requirements (Annex E), and KFOR-specific requirements (Appendix 1 to Annex E). The KFOR-specific requirements are further separated by the training and validation location, requiring some training to be completed at home station or mobilization platform, with the remainder of the training conducted at the Joint Multinational Readiness Center (JMRC).

The JMRC portion of intelligence training for KFOR focused specifically on a Balkan overview and coordination with regional authorities. The continental U.S. (CONUS) – also known as home station – portion of the training requirements included prerequisites for all HUMINT and CI Soldiers to be military occupation specialty qualified (MOSQ). There was also a requirement for at least two of these Soldiers to have completed the Source Operations Course (SOC), a seven-week period of training at USAICoE in Fort Huachuca, AZ. If the unit did not have SOC-certified or CI-equivalent operators, the unit was required to source them from another unit. Since all SOC admission requests are personally vetted by the Army G-2, selection into the course is limited across the Army.

In the period of this case study, KFOR rotations typically consisted of many young, new collectors who had not received much, if any, MOS-specific training outside of their Advanced Individual Training (AIT) courses. In most cases, the Soldiers had graduated AIT several years prior and the skills learned there had atrophied with no further opportunities for application. Except for a few seasoned senior Non-Commissioned Officers (NCOs), the intelligence enterprise lacked experienced collectors, though the units varied in overall MI readiness.

The collectors were not alone in this conundrum, though. The 35T included on the manning document had to be trained to operate and troubleshoot all intelligence systems within the KFOR mission, since FSR support would not be available. The Army in general has had difficulty in retaining Soldiers in this low-density MOS, since they are typically offered much more lucrative opportunities as contractors, having received training in a very specialized skillset. As a result, the 35Ts that were identified to assume the KFOR mission were typically young and rarely trained on all the systems required for the theater they were deploying to. One proposed solution to remediate this was to have the 35Ts deploy into Kosovo several weeks early and receive on-the-job training (OJT). This solution should only have been considered as a worst-case scenario if everything else had been attempted first, but was proposed before even trying to schedule the requisite 35T maintainer courses.

Ultimately, by the KFOR 24 rotation, these courses were scheduled properly and the 35T received training on all three platforms she would be responsible for in theater. Even so, the task was not as simple as requesting training. Given that the unit was National Guard, they needed to put the Soldier on orders in order to send her to training, but the time period of the training crossed both the pre-mobilization and post-mobilization periods. This created an incongruency with orders and funding, since pre-mobilization training was funded by a mixture of state and Title 32 funds and post-mobilization training was funded exclusively by Title 10 funds. The unit created a work-around for the funding in order to send the Soldier to both courses, adjusting her temporary duty (TDY) to end after one course, and beginning her next course under new TDY orders with federal funding. This was a feasible course of action since the courses were located in two separate states.

KFOR GEOINT training was not covered under any level of RAF training guidance, which meant the post-mobilization GEOINT training was designed specifically based on KFOR pre-deployment site surveys (PDSSs) and after-action reviews (AARs). These proved invaluable in assessing the training required for mission success.

The RAF training guidance for all source analysts was not much better, listing the training task of "Conduct Intelligence Preparation of the Battlefield (IPB) in a SASO environment (FMI 2-01.301 (2009))."[41] Additionally, the guidance states, "As an essential mission command system all units will ensure they establish network connectivity at home station for the Distributed Common Ground Station-Army (DCGS-A) and have soldiers trained

[41] Department of the Army, Annex E to U.S. Army Forces Command (FORSCOM) Regionally Aligned Forces (RAF) Training Requirements 2019 – U.S. European Command (USEUCOM) Theater Specific Training Requirements ISO Deployments to USEUCOM Area of Responsibility, 2019.

on the system."[42] It further elaborates that units can request training on DCGS-A at home station through the Foundry Program. This raises several questions – 1) Does this imply that all units are expected to deploy with their own DCGS-A? and, 2) What level of proficiency is required?

Pre-Mobilization Training Requirements

This training guidance lacks the robustness that would assist the development of a proper training plan specifically designed to enable the intelligence enterprise within its theater of operation, as indicated previously in the USAFRICOM example. To exacerbate the problem, National Guard units vary in degrees of readiness. Some units have mastered collective training by the time they reach the post-mobilization platform, while other units are still identifying individual tasks that will need to be validated prior to deployment. With intentionally vague guidance on which training must be completed during the pre-mobilization period, if any, the intelligence training conducted by each unit at home station prior to arrival at the mobilization platform varied significantly.

With the requirement for all units to validate prior to deploying, some might consider this predicament to be of little concern, but without deep diving the problems inherent in the validation process itself, consider a maneuver company arriving at the post-mobilization platform without having completed an individual rifle qualification range. The scheduled bounding squad live fire range is no longer viable, forcing the validation authority to approve a unit to deploy having only completed a static individual live fire range. The disparity between a unit validating on a static individual live fire range, versus a unit that excels at bounding squad live fires depicts the massive skills gap between units arriving at varying degrees of readiness.

[42] Department of the Army, Annex B to U.S. Army Forces Command Regionally Aligned Forces (RAF) Training Requirements 2019 (Mission Specific), 2019, 22.

This is an artifact of the National Guard component that will be hard to overcome, but more prescriptive training requirements may alleviate some confusion.

As a result, pre-mobilization training (as opposed to post-mobilization training at Fort Bliss) for at least half of the KFOR rotations suffered a lack of robust intelligence training. With the DCGS-A basic course totaling 80 hours, Soldiers would have to spend their entire Annual Training period in DCGS-A training instead of training with their unit, or their unit would need to bring them on Title 32 orders for an additional 14 days at another point in the year, which could also become contentious as the civilian Soldiers of the National Guard had civilian jobs that competed with these requirements. While other intelligence training could be conducted in a shorter period of time, the requirements listed above may not be easily interpreted into an actual pre-deployment training schedule. The units which had managed their intelligence training well throughout their ARFORGEN cycle maintained proficiency and required less refresher training during their pre-deployment year, which allowed additional time for other skills training.

Apart from time and prescriptive requirements, one barrier to successful individual and collective intelligence training specific to the KFOR mission was that sourcing came from multiple units, nearly always from two different states. This meant the intelligence enterprise for KFOR had a Brigade S2 element from one state and a division ACE, or a MICO acting as a division ACE, from an entirely different state. The first time these units met was at the post-mobilization platform where they would plunge into a 33- to 45-day training schedule together.

Despite the lack of training guidance provided by the theater and FORSCOM, the post-mobilization platform at Fort Bliss, TX had its own means of assessing what training should be conducted at home station through the implementation of AARs and PDSS visits. For example, a PDSS site visit conducted in preparation for KFOR 22 noted that the CI/HUMINT training needed to be incorporated into the overall Mission Readiness Exercise (MRX), the collective training event. It was one thing to train them on their individual tasks, but the impacts of forcing them to learn how to communicate with the ACE and Brigade S2 were monumental when this consideration was implemented in the KFOR 23 and KFOR 24 post-mobilization exercises, and even more so when they reached Kosovo. Previous units had reported in their post-deployment AARs that they were never able to overcome this communication barrier, making it an essential aspect of post-mobilization training.

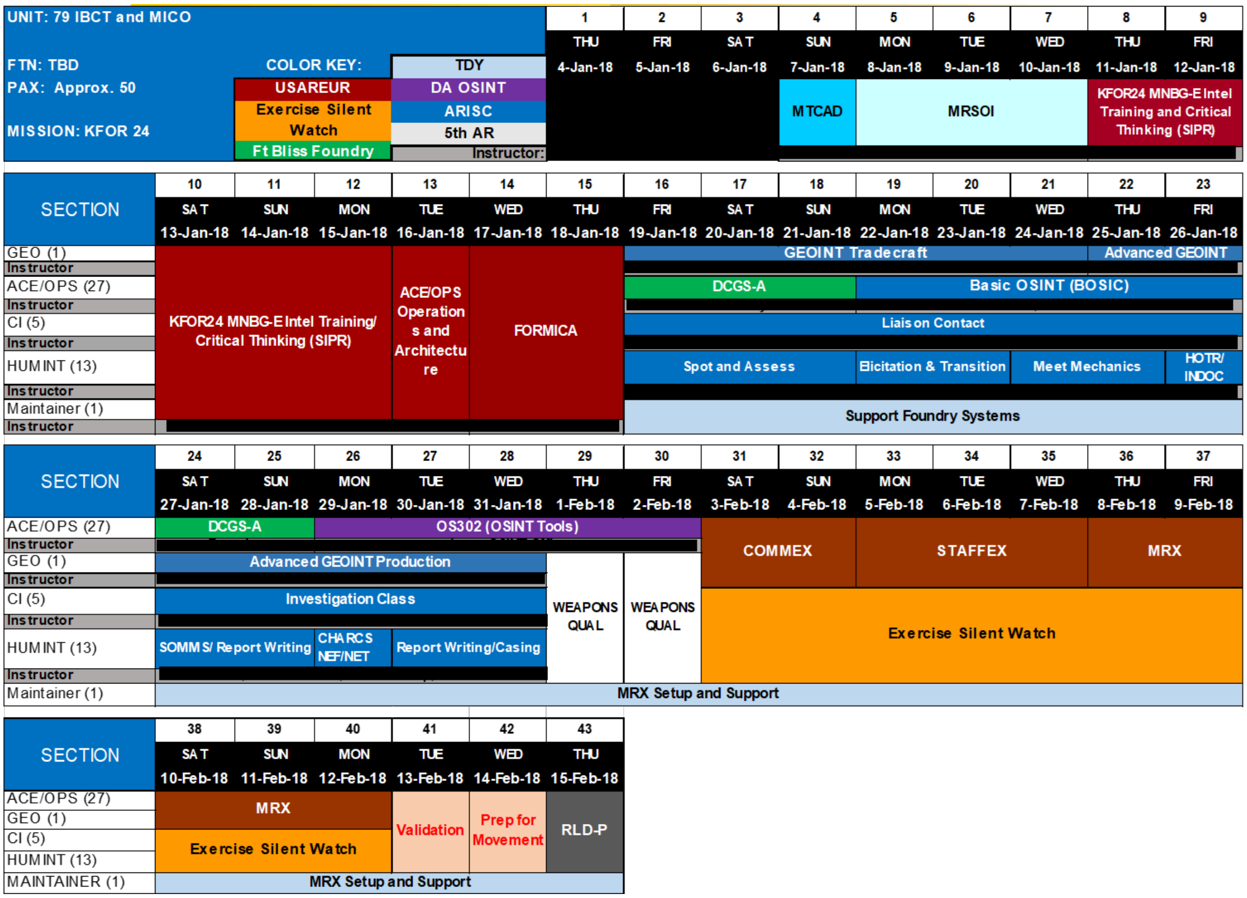
Before taking a closer look at the final training plan, it is important to note the issue of limited access to the Secure Internet Protocol Router Network (SIPRNet) within the National Guard. Just as units varied in skill level and levels of training, they also varied in levels of access to SIPRNet at home station. One unit's BDE S2 stated that he had to travel nearly 100 miles away from his headquarters to access SIPRNet, which was detrimental to the unit's ability to prepare for deployment. Of the many concerns this raises, it is particularly troubling in regard to training the KFOR intelligence mission, since CI regulations are classified. To have a basic understanding of what his CI Soldiers were required to do, he needed access to review these documents. It became incumbent on the post-mobilization platform to take on this role when he lacked the capacity, which meant he only gained a thorough understanding once in theater.

Developing the Post-Mobilization Training Plan

Despite these inherent shortcomings, each KFOR rotation executed an intelligence training plan developed by an intelligence planning team consisting of individuals from both sourced units, the post-mobilization platform intelligence team (from the training command and the Foundry site), ARISC instructors from each of the intelligence disciplines (minus SIGINT, which was not part of the KFOR mission), and the USAREUR G-2 trainer. This created a robust intellectual effort to define actual training requirements and build a plan to give the unit realistic, effective training that would help them deploy with proficient MOS skill levels.

The training plan depicted on the following page was the final training plan executed for KFOR 24 at Fort Bliss, TX in 2018. This was modified from previous iterations to include a shortened MRX at the request of the unit's Brigade commander in order to truncate the post-mobilization timeline. Truncating the post-mobilization training timelines is highly discouraged, but due to the nature of what Title 10 and Title 32 authorities allow for National Guard deployments, funding is typically the root cause of shortening training time, with the commander's desire for their unit to spend as little time as possible away from their families and jobs as a close second. Each line of training was curated to each intelligence discipline based on an assessment of the unit's current proficiencies. This unit only required a five-day course in DCGS-A to meet FORSCOM RAF requirements. Conversely, they spent ten days conducting open-source intelligence training, which directly supported the open-source mission that comprised the majority of ACE operations at the time.

Based on AAR feedback from previous KFOR rotations, the CI and HUMINT blocks of instruction were ran in parallel instead of together, as had been done in earlier iterations of post-mobilization training. This separation of skillsets mirrored the separation of missions in theater, though the two sections were brought together during the final MRX in Exercise Silent Watch – an off-post CI/HUMINT training event that enabled the Soldiers to learn in a semi-permissive environment under direct supervision of certified source operations instructors.



UNIT: 79 IBCT and MICO

FTN: TBD

PAX: Approx. 50

MISSION: KFOR 24

COLOR KEY:

	TDY
USAREUR	DA OSINT
Exercise Silent Watch	ARISC
	5th AR
Ft Bliss Foundry	Instructor:

1	2	3	4	5	6	7	8	9
THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI
4-Jan-18	5-Jan-18	6-Jan-18	7-Jan-18	8-Jan-18	9-Jan-18	10-Jan-18	11-Jan-18	12-Jan-18
			MTCAD	MRSOI			KFOR24 MNBG-E Intel Training and Critical Thinking (SIPR)	

SECTION	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI
	13-Jan-18	14-Jan-18	15-Jan-18	16-Jan-18	17-Jan-18	18-Jan-18	19-Jan-18	20-Jan-18	21-Jan-18	22-Jan-18	23-Jan-18	24-Jan-18	25-Jan-18	26-Jan-18
GEO (1)	KFOR24 MNBG-E Intel Training/ Critical Thinking (SIPR)			ACE/OPS Operations and Architecture	FORMICA		GEOINT Tradecraft						Advanced GEOINT	
Instructor														
ACE/OPS (27)							DCGS-A			Basic OSINT (BOSIC)				
Instructor														
CI (5)							Liaison Contact							
Instructor														
HUMINT (13)							Spot and Assess			Elicitation & Transition		Meet Mechanics		HOTR/ INDOC
Instructor														
Maintainer (1)							Support Foundry Systems							
Instructor														

SECTION	24	25	26	27	28	29	30	31	32	33	34	35	36	37
	SAT	SUN	MON	TUE	WED	THU	FRI	SAT	SUN	MON	TUE	WED	THU	FRI
	27-Jan-18	28-Jan-18	29-Jan-18	30-Jan-18	31-Jan-18	1-Feb-18	2-Feb-18	3-Feb-18	4-Feb-18	5-Feb-18	6-Feb-18	7-Feb-18	8-Feb-18	9-Feb-18
ACE/OPS (27)	DCGS-A		OS302 (OSINT Tools)					COMMEX		STAFFEX			MRX	
Instructor														
GEO (1)	Advanced GEOINT Production					WEAPONS QUAL	WEAPONS QUAL							
Instructor														
CI (5)	Investigation Class							Exercise Silent Watch						
Instructor														
HUMINT (13)	SOMMS/ Report Writing		CHARCS NEF/NET	Report Writing/Casing										
Instructor														
Maintainer (1)	MRX Setup and Support													

SECTION	38	39	40	41	42	43
	SAT	SUN	MON	TUE	WED	THU
	10-Feb-18	11-Feb-18	12-Feb-18	13-Feb-18	14-Feb-18	15-Feb-18
ACE/OPS (27)	MRX			Validation	Prep for Movement	RLD-P
GEO (1)						
CI (5)	Exercise Silent Watch					
HUMINT (13)						
MAINTAINER (1)	MRX Setup and Support					

Figure 5. KFOR 24 Post-Mobilization Intelligence Training Plan

The coordination that occurred prior to the execution of Exercise Silent Watch included many detailed control measures, such as coordination with local law enforcement, deliberate risk assessment worksheets, designated exercise control personnel, an established C2 plan, coordination with the 1st Armored Division Public Affairs office, rules of exercise conduct, and an authorization memo. Additionally, all students conducted rehearsals prior to any execution of training off-post, pending instructor approval, and the Commanding General of the installation was the final approval authority for the exercise.

Though planning Exercise Silent Watch alone took considerable effort and time, the training leading up to the exercise enabled the (mostly) smooth integration of CI and HUMINT operations into the Brigade MRX at the culmination of the post-mobilization training period – a measure that is usually forgone due to the amount of effort and approvals required. This was critical in ensuring that analysts and operators did not deploy for the first time without a moderate level of proficiency in their MOS. Conducting this level of training in a CONUS, semi-controlled environment afforded them firsthand interactions while under direct supervision of instructors who could make on the spot corrections and explain in detail any aspect of the training the Soldiers did not comprehend.

Conclusion

Had these Soldiers deployed without this level of training, they may have made it through their deployment to KFOR just fine, but at the likely cost of degradation to the mission, and specifically, degradation to the Army's intelligence enterprise. The skills these Soldiers learned by undergoing a rigorous training schedule prepared them for a very successful deployment in which they were able to expand the Balkan intelligence enterprise, ultimately meeting the U.S. strategic aim of fostering stability in the region. And now those same Soldiers, having completed their KFOR rotation and gaining a higher level of experience, will go back into the force pool sharing the knowledge and skills they learned, better prepared for their next mission.[43]

Future Implications for Army Intelligence Training

Training Requirements and Calculating Proficiency

Improving Army intelligence is also challenged by challenges in assessing and measuring analyst proficiency. The first aspect of this conundrum is identifying which combination of skills make analysts and collectors successful in their missions. The second aspect is measuring that

[43] Admittedly, the underlying difficulties in getting these units to a level of proficiency are severely understated in such a short case study. The planning team's efforts in pooling resources, scheduling, funding, coordination with civil authorities, and all other planning processes demonstrate a need for more prescriptive training requirements and a better understanding among the MI Corps of how to facilitate this level of intelligence training.

success through metrics. Though both the Army and USAICoE have spent decades analyzing these two aspects of proficiency, identifying critical skills and metrics of measurement remains more of an art than a science.

Vague training requirements and a deference to the commander as the single position of authority regarding training are barriers to effective intelligence training and measuring proficiency. While commanders are responsible for validating their unit's training, the subject matter experts (the "S" shops – S1, S2, S3, etc.) have a more detailed understanding of MOS-specific requirements for their own Soldiers, and this paper asserts they should have the primary responsibility for training and assessments. Understanding individual and collective tasks within the intelligence section is one of the primary functions of the Senior Intelligence Officer (S2/G2). Even though the commander validates total unit readiness (think collective task training), each section should be responsible for achieving individual task training readiness.

In an effort to better capture training readiness metrics, the Army recently transitioned its readiness model to Objective-Task, or Objective-T, in 2018 in order to provide a more accurate assessment of a unit's proficiency as applied to the full scale of military operations and not simply counterinsurgency tasks.[44] The methodology was designed so that "to achieve the highest proficiency ratings, Fully Trained (T) or Trained (T-), units need to have at least 80 percent of authorized unit personnel and 85 percent of leaders present at training (for a rating of T) or 75–84 percent of leaders present (for a rating of T-), as well as an external evaluation of the training exercise by the commander two levels above the unit."[45] One problem with using this evaluation metric is that it only accounts for Soldiers and leaders being *present* and not failing, which may

[44] Ellen M. Pint, Christopher M. Schnaubelt, Stephen Dalzell, Jaime L. Hastings, Penelope Speed, and Michael G. Shanley, *Review of Army Total Force Policy Implementation*, Santa Monica, CA: RAND Corporation, 2017, 53.
[45] Pint, Schnaubelt, Dalzell, Hastings, Speed, and Shanley, *Total Force Policy*, 53.

not be an accurate indicator of whether they have achieved *proficiency* in the tasks by the end of the training event.

This begs the question: how important is it that Soldiers are *good* or even *excellent* at their tasks? For example, applying this metric to a rifle qualification, given a hypothetical requisite that all Soldiers must at a minimum hit 50% of the targets, does a "T" rating accurately portray a unit that hits only 50% of the targets? How is this unit differentiated from a unit that hits 90% of their targets? Applied to intelligence training, a unit collective training event still meets the criteria for a "T" rating under Objective-T, whether the unit uses IEWTPT or not, even though IEWTPT is the intelligence simulation system recommended for use in this type of event. While Objective-T provides a more thorough assessment of unit training and readiness than its predecessor, it does not account for these nuances that can significantly impact a unit's actual readiness in terms of being able to transition smoothly to a real-world mission.

Recognizing that Objective-T did not resolve vague training requirements, USAICoE took proficiency assessment a step further, formalizing what was previously known as "MI Gunnery" into the Military Intelligence Training Strategy (MITS) "to develop a tiered certification plan that can provide an objective approach to measure intelligence readiness across the brigade combat team (BCT) intelligence structure."[46] MITS training circulars (TC 2-19.400 – 2.19-404) provide prescriptive training guides on individual and crew intelligence tasks, as well as MI platform certification. MITS was designed to offer commanders and trainers prescriptive training guidance and sample training schedules. By the end of 2019, MITS became more than

[46] Leah B Haller. "Military Intelligence Training Strategy Update." *Military Intelligence Professional Bulletin* 44, no. 4 (2018): 29–31, 1.

just a suggestion when FORSCOM published an order requiring units "to use MITS as a foundation for intelligence certification and…report MITS as part of unit readiness status."[47]

Since MITS is still in its infancy, its effectiveness is yet to be seen. However, some aspects appear promising. MITS aims to resolve the issue of vague RAF training guidance at the FORSCOM level (which still leaves theater level guidance unaddressed), as well as previously vague metrics for Objective-T and its predecessor. It further attempts to resolve the training relationship between the commander and the Senior Intelligence Officer by mandating prescriptive training guidance across FORSCOM, giving the S2/G2 authority to manage their training plans in accordance with MITS.

With a more prescriptive training strategy in place, Army intelligence analysts and collectors will be able to receive training proportionate to their non-MI peers, which was not historically the case – MI Gunnery was not previously mandated, so BCT analysts relied on a strong brigade S2 to enforce MI skills training. Still, time remains a limiting factor to MITS' effectiveness. Commanders must ensure time is allocated for intelligence training in order to meet MITS training objectives.

This author's interview with COL Welch offered insights on the importance of protecting training time, noting that, "While Soldiers typically receive baseline training and introductions to concepts, much of their MOS proficiency comes from experience gained at home station. Time must be carved out from day to day duties for specific MOS tasks. These are often perishable skills that must be trained and practiced on a regular basis." This is especially important for the National Guard and Reserve components, to which allocated training time is finite. Intelligence training must be planned, scheduled, and prioritized by the commander in order to be effective.

[47] Department of the Army, Military Intelligence Training Strategy, TC 2-19.400 (Washington DC: Department of the Army, 2019) 1-1.

Another consideration that MITS endeavors to address is analyst certification. In 2017, the Army G2's RAND study on assessing analyst competencies and proficiencies posed the question of whether analysts should be required to receive credentialing or certification. The Army intends for MITS to provide intelligence analyst certification, but the DOD also recently created an analyst certification program that the Army has yet to capitalize on – the Certified Defense All-Source Analysis (CDASA) professional certification program, which is an Under Secretary of Defense for Intelligence and Security (USD(I&S)) initiative[48]. CDASA-I, the basic level credential, is valid for five years. CDASA-II and -III are still in development. These certifications can help Army intelligence analysts achieve a greater level of analytical rigor and acumen than solely learning their tasks and systems. While MOS-specific tasks and systems should take priority, the Army should make a concerted effort to have their analysts CDASA certified to meet the competitive standards of analysts across the IC.

Time will prove whether MITS is effective at getting after intelligence proficiencies. It will be imperative for USAICoE and FORSCOM to evaluate its effectiveness, and if they have not already identified Measures of Performance (MOP) and Measures of Effectiveness (MOE) for this assessment, they should implement them now. The problem still remains that component inequities may ultimately drive validation of National Guard and Reserve units that have not successfully completed MITS, which is a problem that the Army will need to review.

The Multi-Domain Task Force

In a shift from past organizational structures, the Army has big plans on restructuring parts of the force to align with Multi-Domain Operations (MDO). As MDO implies, the new structure will place greater emphasis on domains the Army historically has not been designed to

[48] "DoD Intelligence and Security Professional Certification: All Source Analysis Overview," Department of Defense, accessed on March 23, 2021, https://dodcertpmo.defense.gov/CDASA/.

fight in during large scale operations – specifically, cyber, electronic warfare, information, space, and even intelligence (which, in the proper order, the Army has dubbed I2CEWS). The Army designed the new Multi-Domain Task Force (MDTF) to employ MDO, standing up a conceptual I2CEWS battalion to manage the challenges of the future battlespace.

This new concept incorporates intelligence into all domains of the fight, not just in theory, but by design, breaking the barriers faced by the E-MIB and MIB-T, which fall under separate command hierarchies. With MDTF doctrine near publication, METL tasks will soon follow, as well as training requirements. Done right, the requirements would tie intelligence tasks to multi-domain operations (MDO), meaning the only way for the MDTF's military intelligence company (MICO) to train collective tasks would be in an MDO environment (real or simulated), which would present an ideal opportunity for units like the E-MIB and MIB-T to participate in a collective intelligence training event with them.

The Army is currently nearing the end of its MDTF pilot program with plans to stand up three MDTFs in the coming years (two will be located in the Pacific Theater).[49] The proposed MDTF doctrine includes entirely new concepts, such as a space control company, a cyber-electromagnetic activities (CEMA) section, an information defense company, and an extended range sensing and effects (ERSE) company.[50] Most of these will fall under the I2CEWS battalion, along with pre-existing organization types such as a MICO and a signal company. In addition to adding new organizational concepts to the MDTF to combat an evolving threat, the Army seeks to integrate other military branches, and even U.S. allied partners into the MDTF

[49] Sean Kimmons, "Army to Build three Multi-Domain Task Forces Using Lessons from Pilot," Army News Service, accessed on March 3, 2021, https://www.army.mil/article/228393/army_to_build_three_multi_domain_task_ forces_using_lessons_from_ pilot.

[50] Department of the Army, *Techniques for the Multi-Domain Task Force* (forthcoming), ATP 3-19.94, Washington DC: Department of the Army, 1-5 – 1-6.

architecture. In fact, "U.S. Indo-Pacific Command is making the Army's MDO efforts its foundational concept as it develops its own joint warfighting concept for the region."[51]

This organizational concept development aligns neatly with historical Army patterns, but poses the risk of repeating past mistakes. The Army has always organizationally restructured to meet emerging requirements, to adapt to restrictive defense budgets and manning cuts, and to maximize the effectiveness of new technologies and innovative weapon systems and vehicles. The MDTF, while an entirely new concept and design, falls within these natural historical tendencies. To avoid the mistakes of past organizational restructuring, the Army will need to address the issue of proper training and resist the urge to assemble its brightest intelligence analysts within the MDTFs, leaving the remaining conventional forces bereft and unable to fight effectively.

This was seen in the post-Korean War Army when the best and brightest leaders were sent to elite formations like airborne units and technical staff assignments, leaving less capable leaders throughout the remaining units.[52] While MDTFs will be an important formation in a Great Power conflict, they will not be fighting alone and will require support from the Army's conventional units. In addition to lessons from the past on managing training and personnel, the Army should also be prepared to properly field the task forces with requisite equipment on the same timeline as organizational restructuring – a lesson learned from the hasty construction of General Taylor's Pentomic Divisions of the post-Korean War period.[53] The design was less than optimal, but without the proper equipment, units were left completely stranded. In the MDTF, analysts trained to employ emerging technology like the Multi-Domain Sensor System (MDSS)

[51] Kimmons, "Multi-Domain Task Forces," https://www.army.mil/article/228393/army_to_build_three_multi_ domain_task_ forces_using_lessons_from_ pilot.

[52] Donald A. Carter, *The U.S. Army Before Vietnam, 1953-1965*, Washington, D.C: Center of Military History, United States Army, 2015, 16.

[53] Carter, US Army Before Vietnam, 27-31.

and Terrestrial Layer System (TLS) during field operations will be left scrambling if asked to fight without them.

E-MIB and MIB-T in Near Peer Conflicts

Though the Multi-Domain Task Force provides much more flexibility and interoperability in how the Army will employ intelligence in future environments, the Army will still rely heavily on the E-MIBs and MIB-Ts. The Army's new intelligence concept envisions the E-MIB as the lead intelligence element in a Great Power conflict against a peer threat. However, undermining the value that the MIB-T brings to the fight could drive resources away from what may be the Army's most critical intelligence node in the Pacific theater. In keeping with the Army's future concept, however, COL Blue Huber, commander of the 201st E-MIB, in a discussion with this paper's author, envisioned the E-MIB's role in a potential conflict in the Pacific as providing "C2 of ISR assigned to the Corps/[Joint Task Force, performing] as the Chief Integrator of all Theater/Joint ISR ground and air-based intelligence and EW platforms."

Yet another area of concern in the Army's vision of the E-MIB as the lead intelligence unit in a peer conflict is the dispersed battlefield of the Pacific theater. Without a clear vision for how the Army wants its brigade combat teams to employ their intelligence enterprises, the E-MIB could end up being piecemealed out contrary to its design. Taking these concerns into consideration, the Army will need to develop what its doctrine will look like in the Pacific and what role each formation is expected to have, so it can exercise the concepts before it has to fight a real fight it might not be ready for.

There may be a reversion back to a reliance on COISTs in a dispersed environment, especially considering the implications of Joint All Domain Command and Control (JADC2) connecting sensors to shooters in the future fight. This could significantly alter the current C2 construct, as well as the role of the battalion and brigade intelligence sections against a peer adversary in the Pacific theater. It will become increasingly important for maneuver battalions and brigades to understand their role in the future battle space, developing training for the employment of new systems, operations in a denied environment, as well as developing connective tissue with aligned E-MIBs and National Intelligence Agencies.

DCGS-A Capability Drops

As mentioned previously, DCGS-A's capacity as an intelligence production platform is quite significant. The platform, when used properly, enables analysts to leverage a suite of applications that aid the production and analysis of battlefield intelligence in order to give commanders a much better visualization of the battle space threats. For years, the Army struggled with this system's heavy components and disparate architecture, unable to overcome the cumbersome challenges these posed. Now, with a new focus on a peer threat, the Army is shedding the heavy weight and bridging the data gaps that have impeded its ability to maneuver on the battlefield and process data globally through cloud networks, finally gaining the speed and agility the intelligence corps has been seeking for at least a decade.

The complicated history of DCGS-A previously addressed in this paper demonstrates the fundamental challenges that analysts faced when operating this system in both training and operational environments. The battle between DCGS-A and Palantir illustrates the level of frustration even senior Army intelligence officers reached trying to find a practical solution for analysts that would eliminate the burden of complicated interfaces, heavy equipment, and complex architecture at echelons below division.

USAICoE's Lessons Learned Collections Team has been collecting valuable feedback from the operational force to implement changes to DCGS-A over the past two decades to keep pace with analysts' requirements and address the platform's shortcomings. This proved to be more difficult than it appeared at face value. Mr. Chet Brown, Chief of USAICoE's Lessons Learned Branch, wrote on DCGS-A in a recent article, "The quick and frequent changes in the operational environment present unexpected challenges in collecting and applying lessons learned to drive system improvements."[54]

Even so, the fight for a better system seems to have reached a culmination point with a series of planned capability drops in the imminent future that aim to address analysts' biggest grievances with the platform. With Capability Drop 1, the Army "will increase mobility by replacing roughly 500 pounds of equipment with three laptops, which act as servers connected to the intelligence architecture, to support analytic and intelligence planning functions."[55] This will not only make battalion intelligence sections more mobile and adaptable, but affords them the long-awaited freedom from reliance on FSR support to operate independently. Capability Drop 2 is planned to migrate from the current architecture of "13 disparate databases across multiple theaters…to consolidate data, using joint data standards, into three cloud ready nodes in the Pacific, Europe, and in the United States."[56]

These capability drops will drastically enhance analysts' experience with DCGS-A, providing more mobile, adaptable, and timely intelligence analysis and production in the battlespace. In a near peer conflict, these three factors will be irreplaceable and may help the Army gain the time overmatch it desperately seeks.

The Army will need to continue collecting lessons learned on the new capability drops to ensure they achieve the intended purpose and to adjust as necessary. However, the shift in focus to finally make the changes analysts have fought for holds promise for the future of intelligence

[54] Brown, "Change is Constant," 76.

[55] Hoehn, *ISR Design*, 24.

[56] Hoehn, *ISR Design*, 24.

systems innovation. The last remaining hurdle DCGS-A may face heading into a peer-to-peer conflict will be the unyielding timelines of the military's acquisitions process. If the Army can find a way to circumvent that hurdle for the sake of intelligence, future capability drops may not have to wait until FY2031 for fielding.

Emerging Technologies

DCGS-A is not the only systems upgrade coming to the intelligence corps. Emerging technologies such as smaller computer chips, faster processing speeds, free space optics, and artificial intelligence are taking systems innovation to a whole new level, enabling the evolution of intelligence collection platforms, which provides faster target processing and dissemination, as well as data management assistance. The Army is seeking to leverage artificial intelligence in data processing, helping analysts find data anomalies, which will speed up the targeting process. Intelligence support to force protection will also be greatly enhanced by these new technologies, ensuring that units on the ground are safe and secure while operating in a denied, degraded, and disrupted battlespace.

As the Army continues to look to the future, revolutionary military technology is an important driver to obtaining overmatch in Great Power Competition. Developments in deep sensing and the integration of AI into intelligence platforms are integral parts of the Army's 2028 intelligence strategy, but will require specialized recruiting and/or training.

While Artificial Intelligence (AI) is not necessarily a platform, the Army has begun incorporating AI into its intelligence systems to help analysts process data faster. The current Army G2, LTG Laura Potter, stressed the importance of identifying what work the intelligence enterprise can apportion to AI and machine learning (ML), and what portion needs to be retained in the human domain – "'If you think of the volumes of data that we have to analyze, the speed with which we will have to analyze it, and the way we have to synchronize for high-end conflict, we really need to look at what those analysts' skills look like,' and think about how to teach them to excel in areas of machine learning and artificial intelligence." [57] Identifying these skills early will help the intelligence corps make more targeted recruiting efforts, and will help USAICoE identify what needs to be added to MITS – as well as how soon those changes should take effect. Does the Army need to train analysts to implement AI and counter-AI measures prior to receiving platforms designed with these capabilities? The risk of waiting may be too great.

The Army currently has a number of legacy intelligence systems – DCGS-A for one – which reasonably met the requirements for its COIN fight of the last twenty years. Since the publication of the 2018 NDS, the Army has recognized the need for new intelligence platforms to compete in modern conventional war, specifically ones that can provide deep sensing in an A2/AD environment. To this point, LTG Potter is looking to modernize the Army by, "taking a multi-layered approach 'to make sure that the equipment that we're putting in the field can do the sophisticated intel it needs to do against a peer adversary.'"[58] The systems outlined below are integral to this strategy, and were identified by former Army G2, LTG Scott Berrier, as three of the four Army intelligence modernization priorities designed to "enable execution of joint all domain operations."[59] The fourth priority, space, is focused on the use of low earth orbit satellites to support Army intelligence operations.[60]

The Multi-Domain Sensor System (MDSS) "would employ various geospatial, full-motion video and technical intelligence sensors to identify targets and advanced signals deep in

[57] Mandy Mayfield, "JUST IN: Top Army Intelligence Official Lays Out Priorities," National Defense Magazine, accessed March 11, 2021, https://www.nationaldefensemagazine.org/articles/2021/3/10/just-in-top-army-intelligence-official-lays-out-office-priorities.

[58] Mayfield, "Intelligence Official Lays Out Priorities," https://www.nationaldefensemagazine.org/articles/2021/3/10/ just-in-top-army-intelligence-official-lays-out-office-priorities.

[59] Hoehn, *ISR Design*, 21.

[60] Hoehn, *ISR Design*, 22.

enemy territory and drive long-range precision targeting." MDSS is designed to meet the intent of JADC2 by creating a link between sensors and shooters that will close the kill chain. "A $52 million line item is budgeted for MDSS in FY2021 to launch sensor development and prototyping."[61] With the platform already in development and prototyping, the Army should already be looking to change its doctrine and training if it has not started. Linking sensors to shooters is a change in the long-standing dynamic between intelligence, operations, and troops on the ground. Command and control relationships may change, and the intelligence points of contact will likely need to be adjusted. As mentioned previously in the post-Korean War period, doctrine, organizational structure, and technology changes must occur on a simultaneous timeline to maximize effectiveness or the Army runs the risk of issuing technology that has no doctrinal foundations.

Another modernization effort, the Terrestrial Layer System (TLS), aims at converging "ground-based signals intelligence collection systems…with electronic warfare and cyber into a combined set of Information Warfare capabilities."[62] The TLS will act as more than just a sensor with its enhanced ability to "employ electronic attacks or cyber capability."[63] While the Army projects fielding the TLS to its BCTs, it will likely be a critical system within the MDTF's I2CEWS battalion. The combination of capabilities within one system makes it very adaptable, shortening the kill chain by limiting the connections and nodes from sensor to action. However, the Army will have to incorporate the system's training and manning requirements into its doctrine for this platform to realize its full potential. Within a BCT, an intelligence section issued a TLS will now not only be expected to collect intelligence with this system, but to understand

[61] Hoehn, *ISR Design*, 22.
[62] Hoehn, *ISR Design,* 23.
[63] Hoehn, *ISR Design,* 23.

EW and cyber enough to employ the attack functions appropriately, which will likely come with a set of restrictions and employment measures.

Perhaps the most revolutionary intelligence system the Army is pursuing is the Tactical Intelligence Targeting Access Node (TITAN), a ground-based intelligence system designed to rapidly process data and disseminate targetable intelligence directly to tactical weapon systems deployed across the battlefield, and generate situational awareness for battlefield commanders. This system employs AI/ML to deliver "deep sensing to Army long-range precision strike options to defeat A2/AD threats," ensuring calculated, critical targeting occurs at the speed of relevance. Fielding for this system is projected for FY2023 and FY2024.[64]

As with previous systems, training will be incredibly important when it comes to employing this system in the battlespace. As the Army begins to integrate AI/ML into its intelligence architecture, analysts need to be trained on not only the capabilities of the platforms, but the vulnerabilities inherent with AI/ML systems. For example, China's AI research currently outpaces that of the U.S., in which case the Army can assume they have identified ways to defeat AI systems. Understanding the vulnerabilities and risks of these types of platforms will ensure analysts make the best decisions in employing the systems appropriately.

With these three new systems in the acquisitions pipeline, now is the time for the Army to identify what the NET/NEF training will look like, what its MITS goals are for these systems, and how they will be incorporated into doctrine. Learning from the shortcomings of DCGS-A and OSRVT training, as well as other intelligence training, will be important as the Army moves to a more systems-saturated intelligence architecture. Multiple iterations of individual training on each system coupled with integrated collective training will need to be planned deliberately,

[64] Hoehn, *ISR Design,* 23.

which may require more autonomy for the senior intelligence officer to conduct training for their intelligence enterprise.

Remaining Barriers to Army Intelligence Training

Risk Aversion

As America's largest military body, the Army is designed to defeat enemies primarily in the land domain through deliberate application and escalation of force and violence. An organization whose primary mission is to defend friendly territory and take hostile territory by force must weigh the risks of entering a fight unprepared (risk of high casualties) with the risks of training in a friendly environment (risk of negative impacts to the civilian populace can erode trust in the Army and create additional barriers to future readiness, such as reduced funding and more restrictive policies). Too often, and perhaps understandably, the risks of a future war remain hypothetical, while the risks of a real-world training foul up "today" carries the risk of career damage to the unit commander. Commanders must not only understand the risks associated with intelligence training in a domestic environment, but must actively seek ways to mitigate those risks appropriately in order to maximize realistic training opportunities that will improve force readiness.

After its Jade Helm incident, the Army became even more risk averse when it came to intelligence training outside of military installations. Existing exercises like Panther Strike were largely unaffected because they had already been managing risk effectively for their given scenarios, but units venturing into the realm of realistic military training were faced with the dilemma of risk versus reward. Was the value gained from conducting realistic military training enough to outweigh the risk of something going wrong? What, exactly, could go wrong? How could every risk be managed? These are the questions commanders continue to face when deciding to pursue or forgo training outside their installations.

Why take the risk at all? As seen in the KFOR case study, a lengthy period of classroom instruction preceded the off-post training exercise, and many risk mitigation measures were in place to reduce the risk to an acceptable level. These foundations were integral in making the risk worth the reward. When calculating the reward in these types of situations, commanders and senior intelligence officers will need to evaluate not only the risk of public opinion, but the risk of sending Soldiers into hostile enemy territory with little more than AIT training, especially CI and HUMINT teams which often operate without the protection of their units. Risk acceptance will need to be commensurate with any increase in hostilities overseas.

FSR Dependence

As indicated in the DCGS-A and IEWTPT sections of this paper, FSR support is the Achilles heel of operational Army intelligence. By design, the Army contracts out FSR support for its mission command systems (DCGS-A), managed by the Program Executive Office Command Control Communications-Tactical (PEO C3T). The Army also contracts IEWTPT support through the Program Executive Office Simulation, Training and Instrumentation (PEO STRI). Future systems will be fielded with their own contracts, as well.

Within the existing programs, there are a finite number of FSRs on contract per each system. For DCGS-A, the number of contractors assigned to support each Army installation is usually around two. Given that a normal installation is home to one Army division (typically four to six brigades), plus a myriad of tenant units, each with their own systems requirements, the number of units with systems far outnumber the available contractors. If more than two units require support at any given time, the only option is for the third unit to request support from the regional manager, if there is anyone available. The Army's solution of having military intelligence systems maintainers/integrators (35T series) poses the exact same problem – 35Ts are a low-density MOS. As a result, even when filled to maximum end strength, the number of systems they are expected to maintain exceeds their workload capacity.

FORSCOM, recognizing this predicament, created the Digital Intelligence Systems Master Gunner (DISMG) Course in 2015. While the main function of the course is to train Soldiers (of any MOS) to plan and supervise "the integration of automated intelligence systems supporting intelligence operations, sharing best practices within their unit, and supervising DCGS-A systems architecture training," the course is also designed to give DISMGs "a limited capability to troubleshoot DCGS-A systems related issues, filling the current knowledge gap that exists between operator level and the MOS 35/353T MI System Maintainer/Integrator."[65]

Unfortunately, DISMGs cannot acquire administrative privileges for intelligence systems, meaning they will still rely on availability of 35Ts and/or FSRs. However, DISMGs do free up time for the 35Ts to perform administrative functions, allowing them to spread their time more appropriately among a unit's systems. The Army should consider a limited or deployed capacity for DISMGs to have administrative rights for DCGS-A, as well as new intelligence systems, in the future, in order to properly support a rapid deployment of forces against a peer adversary.

Component Inequities

The Army's three components make it an imposing force when deployed *en masse*. The threat of a peer-to-peer conflict makes it even more important that the National Guard and Reserve forces are just as ready to fight as the active component. However, the undeniable inequities between the components make the current structure less than ideal, especially in the

[65] Andrew Maykovich and Nick Rife. "Digital Intelligence Systems Master Gunner Course." *Military Intelligence Professional Bulletin 42, no. 4* (2016): 17.

intelligence capacity. Intelligence training requires more time than most National Guard and Reserve units have available, while also requiring resources they may not always have access to, like classified networks and satellite time. Structuring these units exactly the same as the Active-Duty force gives a false pretense that they can operate exactly the same way. This is not to say that these components cannot pack a punch in a peer-to-peer conflict, but that they should be structured in a way that better enables them to fight as part of the total force. A better force structure will lead to a smarter allocation of resources and a more deliberate deployment of forces in support of the overarching military strategy.

Rate of Emerging Technology

The Army has always managed to achieve overmatch through innovative doctrine and technology that adversaries have difficulty exploiting. Recently, the rapid evolution evoked by the 2018 NDS is going to put new systems in the hands of analysts and collectors in the next few years, giving them an edge on the competition. However, the concerns raised in this paper illustrate the importance of proper systems training that must be continuous to achieve success on the battlefield, while also aligning with doctrine in its distribution to the force and its employment in a fight. A rapid evolution in intelligence systems means a rapid succession of training must occur or units will not be able to use them properly when deployed.

Another concerning element of emerging technology is that the U.S. is no longer at the leading edge of military technology, especially when it comes to the grey zone. Analysts must not only learn to use the new systems in the Army's arsenal, but must understand the adversary's capabilities, which may be beyond their own in some areas. Training in COIN and conventional warfare must continue, but analysts will need to train to fight against weapons and sensors that integrate artificial intelligence on the battlefield. Analysts will need an understanding of how capabilities and limitations in this environment drastically differ from past battle spaces, while also actively identifying new technologies and changes to adversarial tactics of employment as they emerge.

A Culture of Complacency

The last two decades of war have led to a culture of complacency in intelligence. Often, training receives a hand wave as commanders are eager to get into theater, knowing they will have a thorough Relief in Place/Transfer of Authority (RIP/TOA) with the departing unit. The U.S. intelligence architecture already exists in Iraq and Afghanistan, meaning that in some cases units do not even bring all their own organic systems. The theater level assets have been operating in the region for over a decade, and Soldiers have become accustomed to multiple deployments, some to the same theater.

Over time, commanders and intelligence analysts have developed heuristics for operating in CENTCOM. Across the force, Soldiers say, “this is how we did it in Afghanistan/Iraq,” as an answer to why they chose to execute a certain action. These shortcuts seem harmless, and, in fact, may give the Army an advantage in the CENTCOM theater in some instances, but are extraordinarily dangerous when analysts stop critically thinking about why they are making decisions. Applied to a different theater, a different military with a different culture, these shortcuts may lead to very dangerous decisions, including neglecting intelligence or a failure to collect on the right targets.

Training will be critical in forcing analysts out of complacency. They will need to understand that fighting against new technology and peer adversaries will not resemble the wars in the CENTCOM AOR, and the things they learned in that theater may not apply in a new battle space. Exercises in a joint or combined environment will help strengthen the capacity for forward thinking, enabling analysts to think critically about how to employ their systems against a peer threat.

Recommendations to Improve Army Intelligence Training

With a full understanding of shortfalls in Army intelligence training and the risks these pose in the challenging environment of high-intensity great power war, what is to be done? This paper recommends six key areas that can better posture Army intelligence: adding AI; expanding the US-based intelligence architecture; refining requirements documents; preserving training time; conducting more joint regional exercises; and maximizing the total Army force. While these recommendations explore training solutions to some of the previously mentioned barriers, there are several areas in which solutions remain elusive, particularly with regards to an over-reliance on contractor support as the Army seeks to expand its intelligence systems architecture.

Adding Artificial Intelligence Courses

While most AI analytics will be conducted by CYBERCOM, Army intelligence analysts will need to learn how AI works in order to recommend ways to exploit it and also to recommend security measures to protect against enemy autonomous systems. New course offerings should be included in the Foundry Program and required for all 35 series analysts. Fighting an adversary without understanding how they can employ their technology is dangerous and leaves Army formations vulnerable. Likewise, fighting without understanding the limitations of Army systems can lead to poor decision making, putting Army systems in harm’s way, or leaving them susceptible to manipulation by the enemy. Analysts must be prepared to inform their commanders of these vulnerabilities and limitations in friendly and adversarial systems.

Expanding the Intelligence Architecture Within the U.S.

The Army should expand its intelligence architecture in the continental United States. Many intelligence tasks can be conducted remotely, and an expanded architecture would support additional training for active duty, National Guard, and Reserve intelligence analysts. Most Active Guard Reserve (AGR) intelligence analysts are already performing these tasks, which keeps their proficiency levels high. The ARISCs, which also serve as IROCs, are a fitting example of how successful this home station architecture is. Expanding the capability by creating additional ARISCs or building additional intelligence capacity at installations across the country will reinforce the architecture and reach back capability for forward deployed elements.

One option would be to build an arctic regional ARISC that could provide reach back capability in what could potentially be a future battle space. Establishing additional ARISCs in previously unconsidered regions will create more opportunities for LET events, as well as develop architecture in place before a conflict drives the need for it. While LETs are one of Foundry's most underused and undervalued offerings, creating additional opportunities may drive renewed interest in sending analysts to train. Even if analysts never deploy to the region where their LET is conducted, they develop an understanding of the capabilities offered by the IROCs and learn how to connect with National Intelligence Agencies.

Refining Capabilities Requirements Documents

Intuition and training time should be written into every intelligence system's capabilities requirements document. For example, a -10 level analyst should be able to achieve -10 level proficiency on a system within four training days, and a -20 level analyst should achieve -20 level proficiency within eight training days. The NET/NEF provided during equipment fielding should fit these requirements. Given the "forgetting curve," analysts need to be able to retain enough skills on any given system to be able to operate them at the basic level with minimal refresher training. In a rapid deployment scenario, the Army cannot afford to have complex systems that analysts will not be able to rapidly employ in their battle space without extensive training. While the goal should ultimately be to reinforce systems training throughout the year, in the event that does not occur, analysts cannot afford to deploy with systems they cannot operate with minimal training.

Create Space for Continuous Training

New Equipment Training is ineffective if a unit puts the system in a closet for six to twelve months once training is complete. Statistically, after six days of not applying a learned skill, analysts will forget about 90% of information learned in their training. This is because most of this training is stored in short-term memory and analysts make no attempt to retrieve the information after training to make it “stick” in their long-term memory. Units need to ensure that systems are properly integrated into regular training cycles and should pull the new systems back out within a month of initial training to conduct a second iteration of training on the system.

Joint and Combined Exercises

Units should consider conducting a minimum of one unit-level COMEX per year, while striving to participate in a larger joint or combined exercise annually, the outputs of which will drive future lower echelon training to build a cumulative progression of proficiencies and experience. The COMEX will ensure units are able to operate and integrate their systems properly, understanding how to rapidly employ them in an austere environment. COMEXs can be tiered or staggered within an installation or region leading into a regional collective exercise. The ultimate test in a training environment will be in having disparate units achieve connectivity and interoperability, validate their Standard Operating Procedures (SOPs), individual tasks, reporting procedures, and systems employment in achieving the desired exercise end state.

In addition to tying in the joint enterprise in collective training events, the Army should consider tying both the E-MIBs and MIB-Ts into regional training events in order to exercise C2 and information sharing across intelligence elements within the regional joint or combined force. Collective events at the brigade or even division level echelons will not be enough to prepare for a fight against a peer adversary. The Army must strive to tie its intelligence architecture into the joint fight, which must include training its new integrated doctrine and systems in a joint environment.

Maximizing the Total Army Force

The Army's "Total Force" concept implies that all like units are equal, when in reality, the disparity between an active duty BCT and a National Guard (NG) BCT is monumental. Accesses and opportunities are two of the largest gaps the National Guard is faced with, along with time and money. For example, an active duty BCT has access to JWICS and other intelligence networks, as well as appropriate facilities to train in, while a National Guard BCT may not even have access to SIPRNet within 100 miles.

The most difficult hurdles the National Guard faces with intelligence training, however, is time. With one weekend a month and two weeks of Annual Training per year, National Guard units are overwhelmed with requirements, and rarely will intelligence training make that cut. MI-specific guard units have more time allotted to intelligence training, but require money to pay for their analysts to receive additional training. Most states dislike paying Soldiers outside the training periods unless it meets a deployment requirement, but even then they have a hard time justifying it.

To fix this particular problem, this paper recommends a reorganization of National Guard BCTs into Single-Domain Enhanced Brigades. While the Army is writing its doctrine on Multi-Domain Operations, the National Guard could find a niche in providing the future force additional capabilities and highly trained Soldiers. The single domains include Electronic Warfare, Intelligence, Cyber, Space, and Information Operations.

In practice, an Information Operations Enhanced Brigade could "deploy" at home station in direct support of a mission or in support of an active duty unit in theater. An Intelligence Enhanced Brigade could specialize in artificial intelligence detection measures and operate a full-time operations center in support of National Agencies and Joint missions. The BCTs already operate as a division, so converting each BCT into a specific domain-enhanced brigade would make one division fully MDO capable. Additionally, the Army would build up the infrastructure to support these missions, which would provide additional continental United States capabilities that, in theory, are harder to target.

Many other opportunities would arise from this structure, including deployments of smaller teams in support of CONUS requirements. For example, space companies could "deploy" in shorter cycles in support of SPACECOM. This could potentially solve funding issues caused by Title 10 and Title 32 authorities, making it much more appealing than an OCONUS deployment. This construct, though requiring a significant organizational change, has the potential to alleviate a lot of issues facing the Total Army Force today, while preparing the Army to take on the demands of future fights.

Conclusion

While the Army is working to refine its intelligence training and training architecture, it needs to explore new options to ensure that new capabilities and emerging technologies are trained and retained properly to produce the best Army intelligence possible in a theater where the U.S. may not have systems overmatch. New doctrinal concepts, while giving the Army a strategic advantage against a peer adversary, will need deliberate and consistent training to be successful. Additionally, the Army's total force construct lends itself to impossible training objectives and timelines within the National Guard and Reserve components. An overhaul of the total force structure may be necessary to maximize the effectiveness of the Army as a whole, understanding the capabilities and limitations of each component and capitalizing on each of their strengths. The Army Intelligence Corps is finally overcoming some of the major challenges it faced in the past, but to reach its full potential, it needs to avoid making the same mistakes again.

GLOSSARY

A2/AD: Anti-Access/Area Denial

AAR: After Action Review

ACE: Analysis and Control Element

AI/ML: Artificial Intelligence/Machine Learning

AIT: Army Initial Training

AOR: Area of Responsibility

ARFORGEN: Army Forces Generation

ARISC: Army Reserve Intelligence Support Center

BCT: Brigade Combat Team

BFT: Blue Force Tracker

CDASA: Certified Defense All-Source Analysis

CEMA: Cyber Electro-Magnetic Activities

CI: Counterintelligence

COIN: Counterinsurgency

COISTs: Company Intelligence Support Teams

COMEX: Communications Exercise

CONUS: Continental United States

CPOF: Command Post of the Future

DCGS-A: Distributed Common Ground System – Army

DISMG: Digital Intelligence Systems Master Gunner

DOD: Department of Defense

E-MIB: Expeditionary Military Intelligence Brigade

EO: Equal Opportunity

ERSE: Extended Range Sensing and Effects

FMV: Full-Motion Video

FOM: Freedom of Movement

FSE: Field Service Engineer

FSR: Field Service Representative

GEOINT: Geospatial Intelligence

GMTI: Ground Moving Target Indicator

GWOT: Global War on Terror

HUMINT: Human Intelligence

I2CEWS: Intelligence, Information, Cyber, Electronic Warfare, and Space

IC: Intelligence Community

IED: Improvised Explosive Device

ILOD: Intelligence Low Overhead Driver

IO: Intelligence Oversight

IPB: Intelligence Preparation of the Battlefield

IROC: Intelligence Readiness Operations Center

ISR: Intelligence, Surveillance, and Reconnaissance

JADC2: Joint All-Domain Command and Control

JMRC: Joint Multinational Readiness Center

JWICS: Joint Worldwide Intelligence Communications System

KFOR: Kosovo Forces

LET: Live Environment Training

LLVI: Low Level Voice Intercept

MDO: Multi-Domain Operations

MDTF: Multi-Domain Task Force

MDSS: Multi-Domain Sensor System

METL: Mission Essential Task List

MFGI: Mobilization Force Generation Installation

MIB-T: Military Intelligence Brigade – Theater

MICO: Military Intelligence Company

MIRC: Military Intelligence Reserve Command

MITS: Military Intelligence Training Strategy

MNBG-E: Multi-National Battle Group – East

MOS: Military Occupational Specialty

MOSQ: Military Occupational Specialty Qualified

MRX: Mission Readiness Exercise

MTA: Military Technical Agreement

MTT: Mobile Training Team

NATO: North Atlantic Treaty Organization

NCO: Non-Commissioned Officer

NDS: National Defense Strategy

NEF: New Equipment Fielding

NET: New Equipment Training

OEF: Operation Enduring Freedom

OIR: Operation Inherent Resolve

OJT: On-the-Job Training

OSINT: Open-Source Intelligence

OSRVT: One System Remote Video Terminal

PCS: Permanent Change of Station

PDSS: Pre-Deployment Site Survey

PED: Processing, Exploitation, and Dissemination

PEO: Program Executive Office

RAF: Regionally Aligned Forces

RIP/TOA: Relief in Place/Transition of Authority

SASE: Safe and Secure Environment

SASO: Stability and Support Operations

SHARP: Sexual Harassment and Reporting Program

SIGINT: Signals Intelligence

SIPRNet: Secure Internet Protocol Router Network

SOC: Source Operations Course

SOF: Special Operations Forces

TC: Training Circular

TDY: Temporary Duty

TITAN: Tactical Intelligence Targeting Access Node

TLS: Terrestrial Layer System

UAS: Unmanned Aerial System

USAICoE: United States Army Intelligence Center of Excellence

USAFRICOM: United States Africa Command

USAREUR: United States Army Europe

USARNORTH: United States Army North

USARSOF: United States Army Special Operations Forces

USCENTCOM: United States Central Command

USD (I&S): Under Secretary for Defense, Intelligence and Security

USEUCOM: United States Europe Command

USFORSCOM: United States Forces Command

USNORTHCOM: United States Northern Command

VBIED: Vehicle-Borne Improvised Explosive Device

Bibliography

Barno, David W. and Nora Bensahel. Adaptation Under Fire: How Militaries Change in Wartime. New York, NY: Oxford University Press, 2020.

Berry, Todd A. and Lance C. Turner. “Expeditionary-Military Intelligence Brigade at War.” Military Intelligence Professional Bulletin 45.1. 2019. 23–26. Print.

Bird, Sheila M. and Clive B. Fairweather. "Military Fatality Rates (by Cause) in Afghanistan and Iraq: A Measure of Hostilities." International Journal of Epidemiology 36, no. 4. 2007. 841-846. doi:10.1093/ije/dym103. https://doi.org/10.1093/ije/dym103.

Brown, Chet. "Change is Constant-Yet some Things Never Change." Military Intelligence Professional Bulletin 46, no. 1. 2020. 75-78.

Carter, Donald A. The U.S. Army before Vietnam, 1953-1965, Washington, D.C: Center of Military History, United States Army, 2015.

Crawford, Bruce T. "Network Modernization: Innovation in a Time of Unprecedented Opportunity: The Army's Current Networks do Not Meet the Requirements of Operational Commanders, so the Army is Modernizing its Tactical, Enterprise, and Intelligence Networks to Increase its Warfighting Capabilities." Army Sustainment 50, no. 5. 2018. 20.

David, P. Elsen, Travis Tyler, J. Custodio R, and A. Glover Michael. "Military Intelligence Brigade-Theater Support to Multi-Domain Operations in the Indo-Pacific Strategic Environment." Military Intelligence Professional Bulletin 46, no. 1. 2020. 29-33.

Davidson, Megan. "Avoiding the Forgetting Curve." Foundry Management & Technology 144, no. 9. 2016. 120.

Department of the Army, Army Foundry Intelligence Training Program, AR 350-32, Washington, DC: Department of the Army. 2010.

Department of the Army, Army Foundry Intelligence Training Program, AR 350-32, Washington, DC: Department of the Army. 2015.

Department of the Army, Army Intelligence Training Strategy, Washington, DC: Department of the Army. 2013.

Department of the Army, Intelligence, ADP 2-0, Washington, DC: Department of the Army. 2012. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN18344_ADP%202-0%20FINAL%20WEB.pdf.

Department of the Army, MIRC 2020: Military Intelligence Readiness Command Vision and Strategy, Washington, DC: Department of the Army. 2011.

Department of the Army, Techniques for the Multi-Domain Task Force (forthcoming), ATP 3-19.94, Washington DC: Department of the Army.

Department of Defense, Audit of the Training of the Army's Regionally Aligned Forces in the U.S. Africa Command. DODIG-2019-096. Washington, DC: Office of the Inspector General, 2019.

Department of Defense. Pre-Deployment Training and Theater Entry Requirements. DOD Instruction 1322.32. Washington, DC: Department of Defense, 2020.

Feickert, Andrew. "Army Drawdown and Restructuring: Background and Issues for Congress." Current Politics and Economics of the United States, Canada and Mexico 16, no. 4. 2014. 567.

Haller, Leah B. "Military Intelligence Training Strategy Update." Military Intelligence Professional Bulletin 44, no. 4 (2018): 29-31.

Heller, Christian H. "Near-Term Applications of Artificial Intelligence: Implementation Opportunities from Modern Business Practices." Naval War College Review 72, no. 4. 2019. 73-100.

Hoehn, John R., Nishawn S. Smagh. Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition, CRS Report No. R46389. Washington, DC: Congressional Research Service. 2020.

Johnston, Gary W. and A. Harfst Richard. "U.S. Army Intelligence and Security Command Strategy." Military Intelligence Professional Bulletin 45, no. 3. 2019. 7-11.

Legere, Mary A. "Army Intelligence 2020: Enabling Decisive Operations While Transforming in the Breach." Army Magazine 62, no. 10. 2012. 165–69. https://search-ebscohost-com.lomc.idm.oclc.org/login.aspx?direct=true&db=mth&AN=82115364&site=ehost-live.

Lewis III, MAJ George E. Army Intelligence Analysis, Transforming Army Intelligence Analysis Training and Doctrine to Serve the Reasonable Expectations. Monograph, Fort Leavenworth, KS: School of Advance Military Studies. 2005.

Lytell, Maria C., Susan G. Straus, Chad C. Serena, Geoffrey E. Grimm, James L. Doty III, Jennie W. Wenger, Andrea M. Abler, 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. https://www.rand.org/pubs/research_reports/RR1851.html.

Maykovich, Andrew and Nick Rife. "Digital Intelligence Systems Master Gunner Course." Military Intelligence Professional Bulletin 42, no. 4. 2016. 17.

Pereira, Jose. "Prioritize to Hone Army's Competitive Edge." Army Magazine 69, no. 5. 2019. 14-15.

Pint, Ellen M., Christopher M. Schnaubelt, Stephen Dalzell, Jaime L. Hastings, Penelope Speed, and Michael G. Shanley. Review of Army Total Force Policy Implementation. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1958.html.

The Policy and Planning Staff, Office of the Secretary of State. The Elements of the China Challenge, 2020.

Richey, Haley Jordan. Operation Jade Helm: A Cultural Analysis of Public Opinion. Undergraduate Research Scholars Program. 2017. Retrieved electronically from http://hdl.handle.net/1969.1/167842.

Riikonen, Ainikki. “Decide, Disrupt, Destroy: Information Systems in Great Power Competition with China.” Strategic Studies Quarterly. 2019. Retrieved from https://web-a-ebscohost-com.lomc.idm.oclc.org.

Scott, W. Harold. "Optimizing the U.S.-China Military-to-Military Relationship." Asia Policy 14, no. 3. 2019. 145-168.

Webber, Reid W. "Persistent Operational Intelligence: An Intelligence Strategy for Joint Force 2020." American Intelligence Journal 34, no. 1. 2017. 59-68.