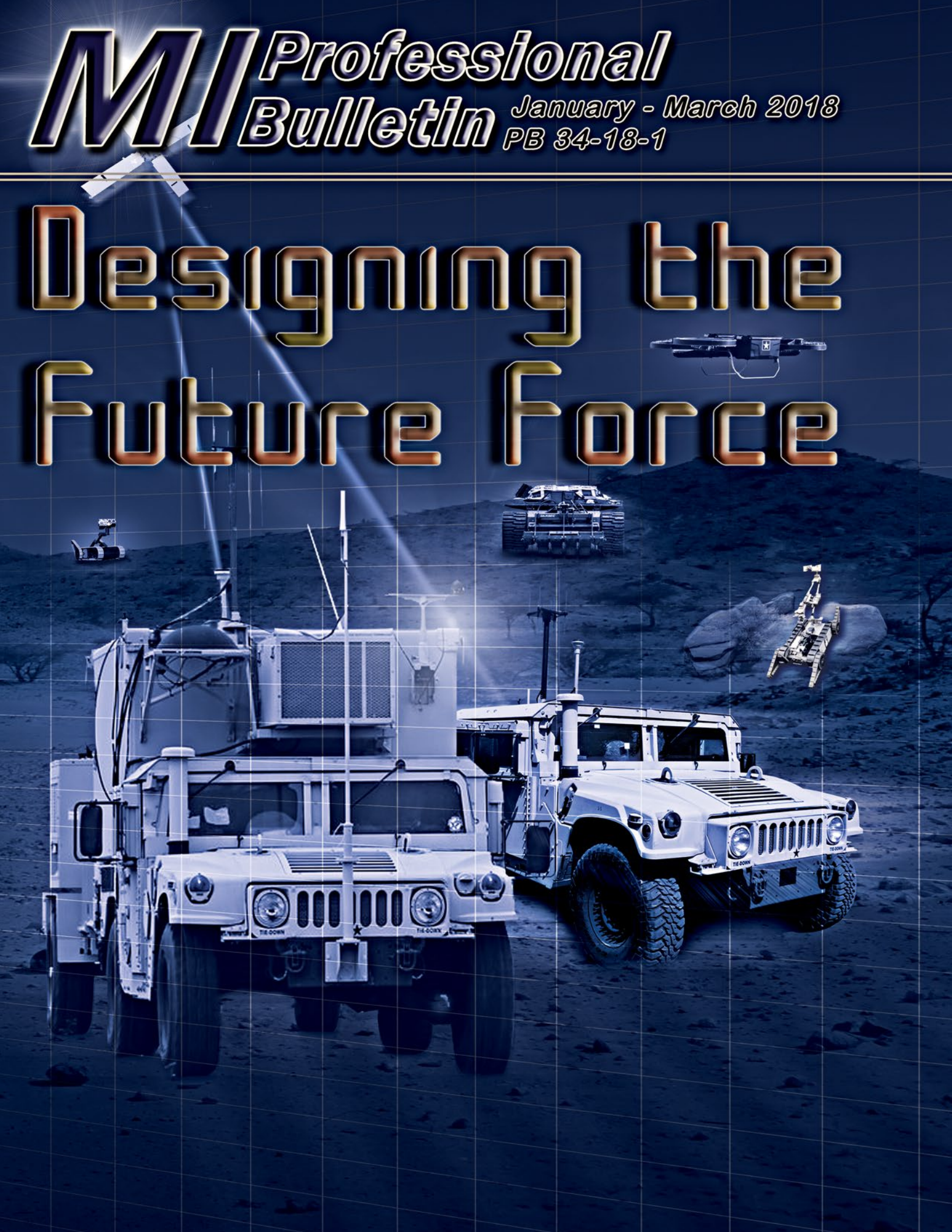
MI Professional Bulletin
January - March 2018
PB 34-18-1

Designing the Future Force



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

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

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

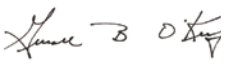
Our mailing address: MIPB, USAICoE, Box 2001, Bldg. 51005, Fort Huachuca, AZ 85613-7002

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

By order of the Secretary of the Army:

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

Official:



GERALD B. O'KEEFE
Administrative Assistant to the
to the Secretary of the Army
1731006

From the Editor

The following themes and deadlines are established:

July–September 2018, *INSCOM 2020*. This issue will focus on how INSCOM supports commanders now and into the future. Deadline for submissions is 3 April 2018.

USAICoE's senior leadership is working to select themes for FY19. Please check our IKN website for theme updates and article submission dates. Future topic ideas include intelligence support in large-scale combat operations, the security force assistance brigade S-2, and intelligence support in special operations.

As always, articles from you, our reader, remain important to the success of MIPB as a professional bulletin. Please continue to send them even if the topic of your article may differ from an issue's theme. Most issues will contain theme articles as well as articles on other topics. We seriously review and consider all submissions that add to the professional knowledge of the MI Corps and the intelligence community.

Please call or email me with any questions regarding your article or any other aspects of MIPB. We welcome your input and suggestions.

Tracey A. Remus

Editor

MI Professional Bulletin

January - March 2018
PB 34-18-1
Volume 44 Number 1

FEATURES

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

Designing the Future Force

DEPARTMENTS

Always Out Front

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

This quarter's theme for the Military Intelligence Professional Bulletin (MIPB) is "Designing the Future Force." The focus of this issue is on the future force requirements and implementation across the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) spectrum. Designing the future force starts with identifying the required Army operational capabilities. These capabilities derive from the national military strategy, the Army Operating Concept, and doctrinal publications—in particular ADP 3-0, ADRP 3-0, and FM 3-0, *Operations*. They are gleaned through lessons learned gained from real-world operations and exercises, as well as experimentation, to determine what is technically feasible along with conducting work to describe and wargame the future operational environment.

This body of work informs our U.S. Army Intelligence Center of Excellence (USAICoE) capability developers who work to determine if the current force possesses the required capabilities and capacities to meet the challenges of the future operational environment. Our training developers' assessments—along with those of the Office of the Chief, Military Intelligence (OCMI)—are critical to ensuring our military intelligence (MI) Soldiers and leaders will possess the correct attributes, skillsets, and career paths to operate in future joint, national, and coalition settings across the full range of military operations. Our force designers work to ensure optimization of our formations to provide the correct mix of Soldiers and leaders to perform reach and expeditionary MI support at echelon. Additionally, our U.S. Army Training and Doctrine Command Capability Managers work to advance materiel solutions to enable these Soldiers and leaders and enhance commanders' decision-making processes. Throughout the process USAICoE Soldiers, Civilians, and contractors work with the Army Capabilities Integration Center, the other Centers of Excellence, the U.S. Army Reserve, the Army National Guard, U.S. Army Forces Command, U.S. Army Intelligence and Security Command, and the Headquarters, Department of the Army staff to ensure all change recommendations are feasible, acceptable, and suitable. Finally, before presentation of any recommendation for decision, our analysts conduct a rigorous course of action analysis that must include a description of the risk to mission accomplishment for not closing the gap along with a cost-benefit analysis.

With this in mind, inside this edition of MIPB, you will discover the Army's instructional design framework used by training developers, gain an understanding of the role of the OCMI, receive an overview of capability development, and learn how the Army utilizes that process to mitigate gaps. The intelligence community is continuously evolving. In his article, "Doctrine? We Don't Need No Stinkin' Doctrine!" Craig Sieting encourages MI professionals to become involved with the development of MI doctrine. I echo his message and urge all MI professionals to read and understand MI doctrine—our professional body of knowledge. Those of us in the MI Corps need to continue to dialogue with one another, encourage each other to think and forecast future problems, and continue to write about our profession.

Always Out Front!

CSM FORUM

by Command Sergeant Major Thomas J. Latter
U.S. Army Intelligence Center of Excellence

How Does the Army Design the Future Force?

We have all at one time thought about and designed in our minds what the future Army military intelligence force should look like based on information we knew at that point in time. I will tell you that if the Army designed the future force based on what I knew as a Staff Sergeant in the early 1990s, we would not have been as successful in adapting to the threats we faced after 9/11. I was good at my job as a Staff Sergeant, but my experience at the time was primarily light infantry, division and below, and Pacific Theater oriented.

GEN Perkins, U.S. Army Training and Doctrine Command (TRADOC) Commander, has repeatedly stated designing the future Army is one of TRADOC's core functions. For Army military intelligence, that is what the U.S. Army Intelligence Center of Excellence (USAICoE) is here to accomplish. The USAICoE Capabilities Development and Integration Directorate (CDID) designs our future force through the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) analysis. The CDID cannot plan and execute this analysis process, explained in a series of articles in this edition of Military Intelligence Professional Bulletin, without understanding the future operating environment and how the Army fights, to include large-scale combat operations.

We need future capabilities that allow us to provide intelligence in phases 0-2, for senior decision makers to deter aggressors and shape the environment; in phase 3, to fight and win against any adversary, to include peer or near-peer, in large-scale combat operations; and in phases 4-5, to execute consolidation of gains and reestablish stability.

As we move from concepts—how we think we are going to fight in the next 10 to 40 years; to doctrine—how we fight today; we need to remain nested with joint capabilities and doctrine as well as the rest of the Army warfighting functions. This requires extensive collaboration, not just with the other centers of excellence within TRADOC, but also with our sister services, various intelligence community partners, and our coalition partners across the world.

Here is the good news: we continue to get better at learning from our past mistakes. Looking at our combat training centers, lessons learned forums, and our recent bottom-up review for military intelligence; the Army strives to apply knowledge earned from hard experience to improve the chances of success in the future. Your engagement in all of these processes is what provides the details needed to plan DOTMLPF-P solutions. To see the results from these influences, review the latest ADP 3-0, ADRP 3-0, and FM 3-0, *Operations*. You will also be seeing rapid revisions of our ADP 2-0 and ADRP 2-0, *Intelligence,* and FM 2-0, *Intelligence Operations,* in fiscal year 2018 incorporating the latest changes, to include multi-domain battle. We need our doctrine nested, solidifying our capabilities-based requirements to mitigate gaps.

Our Army and our Military Intelligence Corps will continue to be in a persistent state of change as we adapt to current operational environments and design an imperfect future force that will give our next generation of military intelligence professionals and leaders the greatest chance to provide commanders with key intelligence to make decisions across all domains. Military intelligence professionals need to be adaptive and make the most of whatever future capabilities the Army develops to meet the threat. We need to continuously ask the "what if" questions to tweak solutions to the problems. You need to stay engaged in our future force design, whether you are the Staff Sergeant out in the force or the developer at USAICoE. As a team we build the capabilities required in the future to dominate our adversaries across all domains.

Always Out Front!

Technical Perspective

Chief Warrant Officer 5 Matthew R. Martin
U.S. Army Intelligence Center of Excellence

Over the last 30 years, military intelligence (MI) professionals have been decisively engaged in a wide variety of operations around the globe that have forced the MI Corps to undergo a number of significant transformations. From stability and support operations in the Balkans, protracted counterinsurgency (COIN) in Iraq and Afghanistan, to our recent efforts to refocus on fighting and winning in a decisive action environment, the MI Soldier has had to be prepared to simultaneously support phase 0 (shape) or phase 1 (deter) operations within every combatant command. Maintaining a trained and ready force to meet these operational challenges demands that we have no MI Soldier "at rest."

For nearly 15 years, the focus of our Army has been on conducting COIN operations throughout the world. The COIN-centric fight significantly affected how we trained, manned, and equipped our MI Soldiers, resulting in an MI Corps that is no longer optimized to fight and win against a peer or near-peer threat. The strain of continuous operations combined with fiscal constraints considerably affects our ability to find, fix, finish, exploit, analyze, and disseminate intelligence information at the speed necessary to decisively defeat our potential adversaries. Some of our historic strengths as an intelligence enterprise are in atrophy and are on the verge of becoming potential weaknesses.

Today's MI Soldier faces what may well be the most dangerous and unpredictable operating environment in our Nation's history. Our potential adversaries continue to build military capacity at record speed as they attempt to exploit perceived U.S. weaknesses and achieve parity with U.S. conventional forces, particularly in the air and maritime domains. They also improve their air defense capabilities, providing increased protection and freedom of maneuver to their ground forces while limiting our joint force intelligence collection and targeting/strike opportunities. Perhaps most significantly, our potential adversaries have made tremendous strides in exploiting U.S. vulnerabilities through the use of commercially available technology and their mastery of the space and cyberspace domains. Our intent is to re-establish intelligence dominance across all domains in order to provide commanders with the intelligence information they need to achieve military objectives.

This edition of MIPB focuses on "Designing the Future Force," which is vitally important to the development and sustainment of a ready and resilient Army intelligence capability to defeat potential threats. To support this effort, several initiatives such as the MI bottom-up review (BUR), the U.S. Army Intelligence Center of Excellence (USAICoE) 30-Year Strategic Modernization Plan, and doctrinal and training developments are well underway. These initatives will not only inform future developments but also posture our MI Corps to defeat all future threats.

The intent of the BUR was to conduct a holistic review of the MI force to inform the total army analysis process. The nearly yearlong process included several travel teams in conjunction with multiple online surveys that sought to identify challenges and capability gaps across all disciplines, echelons, and organizations throughout the MI Corps. While this effort will certainly influence many modernization initiatives within the Corps, our leadership directed priority attention towards several "big ideas" with the intent to transform our force from predominantly COIN-centric to a balanced capability-postured force in order to support the full range of military operations.

The USAICoE 30-Year Strategic Modernization Plan is part of a multipronged strategy that seeks to leverage modern data acquisition, collection, transport, exploitation, and analytic platforms to efficiently create situational understanding and clarity for decision makers. Requirements include the ability to perform intelligence operations in low bandwidth and contested environments with unified and joint partners. It is essential that our MI professionals remain a vital part of the modernization plan; it is through the requirements determination process that we clearly articulate what future capabilities we require to effectively perform intelligence operations, synchronization, and analysis.

For several years, USAICoE has been diligently modifying all levels of professional training and education, which will maintain valuable lessons learned while reintroducing warfighting fundamentals and emerging capabilities from the space and cyberspace domains, to fully address challenges faced within the decisive action environment. The intent is to achieve an educational balance that postures our MI professionals for the unknown or unknowable.

Thanks for all of your enduring efforts, collective professionalism, and selfless service that have been and will remain the bedrock of our MI Corps and Army!

Always Out Front!

Capabilities Needs Analysis: The Foundation for Capabilities Development

by Mr. Jim Staley and Ms. Edwina Kelly

Introduction

The U.S. Army Training and Doctrine Command (TRADOC), Army Capabilities Integration Center's (ARCIC's) Capabilities Needs Analysis (CNA) provides an ordered list of the overall Army-required capabilities. It is a supporting analysis to the Capabilities-Based Assessments (CBAs).[1] The CNA is a 2-year process that focuses on multiple threat scenarios and different operating environments. The CBA is the fundamental analysis process that identifies what the Army must accomplish, what the Army cannot accomplish, and the solutions to solve or mitigate the gaps, now and in the future. Identified solutions are materiel or non-materiel and the Army prioritizes the solutions for capabilities development and/or sustainment. They then compete for budgetary resourcing through inclusion in the Army's program objective memorandum (POM).[2] ARCIC accomplishes the CNA process using the think-learn-analyze-implement framework, shown in Figure 1.[3]

Think

This first step of the framework provides the foundation of the CNA, which is based largely on guidance in joint and Army concepts. The concepts define how the force functions and describe the time frame and conditions in which it must operate. The concepts also describe the physical and organizational characteristics of the future force and what the Army must do (required capabilities) to execute its mission and produce the desired effects on the battlefield. These required capabilities are the cornerstone of the CNA process.

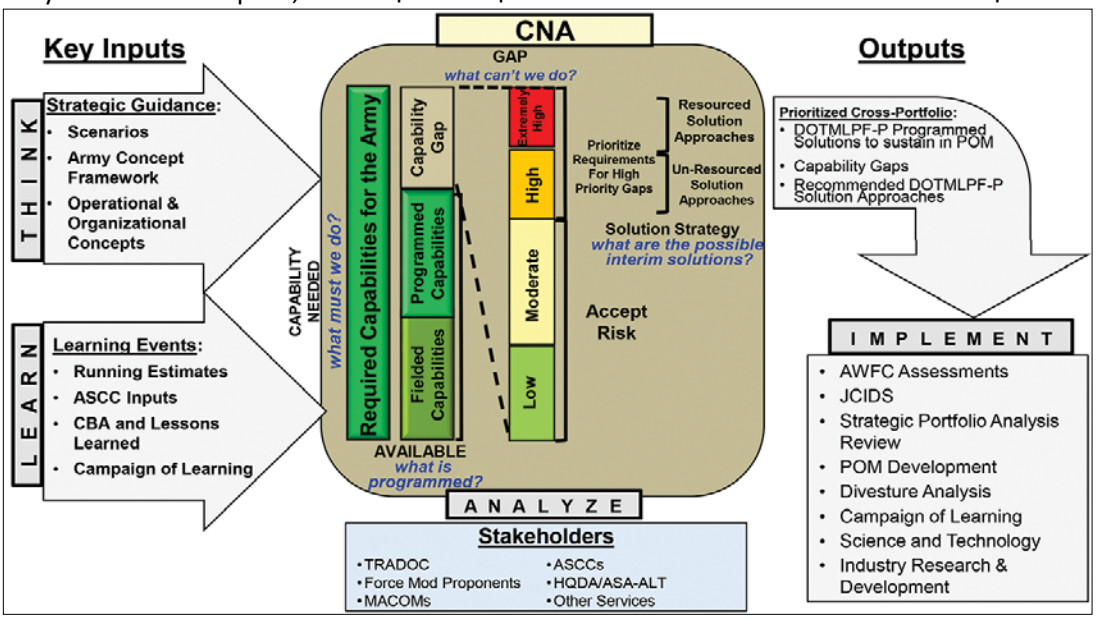


Figure 1. CNA Overview: CNA in Capabiities Development.

Learn

The intent of the learn step is to evaluate operational techniques in a controlled or known environment. These evaluations reveal and/or validate shortfalls that are essential Army capabilities. This step involves multiple resources and evaluation events to glean information about warfighter needs. These resources include—

- Army warfighting challenges (AWFCs) running estimates.
- Combatant command integrated priority lists.
- Operational Needs Statements.
- Joint Urgent Operational Needs Statements.
- Directed CBAs.
- Lessons learned.
- Doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) assessments.
- Experimentation and campaign of learning (CoL) events.

Analyze

The CNA is at the core of the analytical method TRADOC uses to identify capabilities and associated capability gaps within the Army. Once TRADOC identifies gaps, the CNA helps generate and evaluate solutions to mitigate the gaps. Eventually, the Army transforms these recommended solutions into requirements for new or improved capabilities. The U.S. Army Intelligence Center of Excellence (USAICoE), as the military intelligence (MI) proponent, is responsible for the MI portion of the Army's CNA analysis.[4] This analysis includes evaluating intelligence formations, such as the expeditionary MI brigade, MI brigade (theater), MI brigade (aerial intelligence), and select aspects of the U.S. Army Intelligence and Security Command. The analysis also includes intelligence elements of theater Army Service component command headquarters, corps headquarters, division headquarters, and armored/Stryker/infantry brigade combat teams.

The intelligence warfighting function presents CNA results through the AWFC construct.[5] All MI CNA work links directly to AWFC 1–Develop Situational Understanding, and contributes to other AWFCs. The AWFCs are enduring Army challenges; the solutions improve the combat effectiveness of the current and future force. Through the AWFC and CNA processes, proponents identify potential near-, mid-, and far-term modernization efforts for the Army. Properly implemented, the AWFC framework sustains collaboration across the community of practice by providing the foundational analysis for the Army's concept and capability development initiatives. The evaluation of Army capabilities through the AWFCs forces the Army warfighting functions to work together to solve collective problems.

The Army Capabilities Assessment Tool. The ARCIC, as well as all warfighting functions, uses the Army Capabilities Assessment Tool (ArCAT) to perform the CNA/CBA. The ArCAT is a managed software tool specifically engineered to meet CBA analysis requirements. Regimented ArCAT techniques, procedures, and tools provide a standardized means to conduct all three phases of the CNA/CBA: the functional area analysis (FAA), the functional needs analysis (FNA), and the functional solution analysis (FSA).[6] The ArCAT uses a combination of survey questionnaires, assessment scales, subject matter expert input, and computer software to input and analyze data. The ArCAT applies scientific methods to create a repeatable and rigorous capabilities evaluation, yet includes aspects of an "artful" analysis based on the knowledge and experience of the subject matter expert. Using the ArCAT, the CNA provides a thorough, well-reasoned assessment across all DOTMLPF-P domains, warfighting functions, assessed formations, and approved scenarios. Today, the ArCAT is the primary software tool for collecting and processing data to complete the CNA.

Figure 2 depicts the three major analysis steps of the CNA—the FAA, FNA, and FSA.

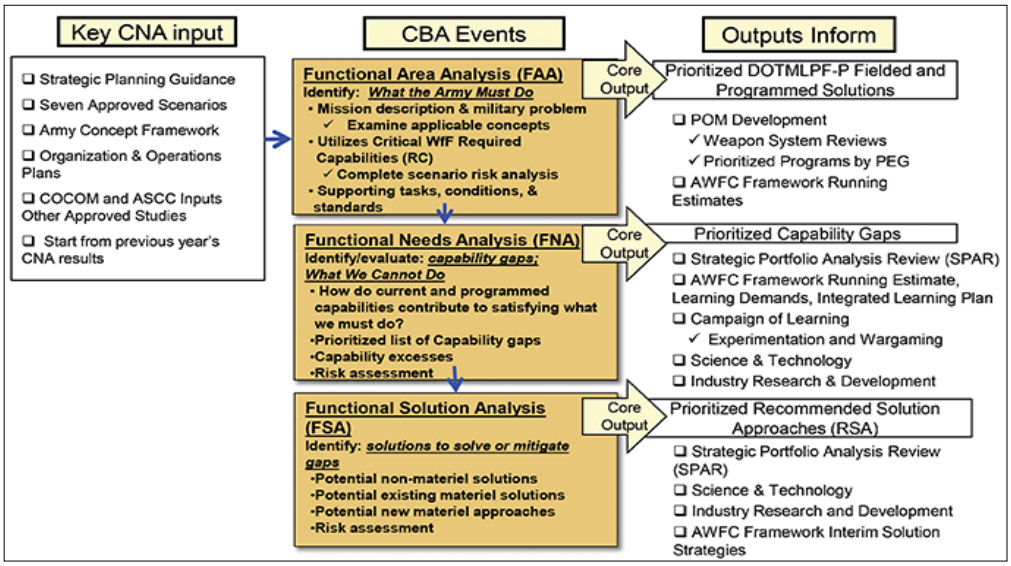


Figure 2. CNA Process.

Functional Area Analysis.[7] The FAA part of the CNA process identifies and assesses what the Army must accomplish

based on conditions described in Department of Defense-approved scenarios. As a foundational part of the process, our CNA analysts identify tasks, conditions, and standards that support the USAICoE-prioritized required capabilities. This initial stage of the CNA is most crucial. Defining accurate and meaningful tasks, conditions, and standards enables our analysts to identify gaps during the next phase of the CNA process. Therefore, it is vitally important that our high-priority tasks undergo a rigorous analysis to verify measures, standards, and conditions for intelligence tasks. Without this meticulous underpinning, it is difficult to define capability gaps accurately.

Functional Needs Analysis.[8] During the FNA, analysts assess formations and evaluate current and fielded capabilities to determine how well these capabilities address the tasks the Army must accomplish. Analysts do this by determining current or programmed capabilities that meet our required capabilities and then assessing how well these capabilities accomplish tasks outlined in the FAA. The FNA then identifies and defines capability gaps, which formally describe what we cannot accomplish.

Functional Solution Analysis.[9] The FSA, the final segment of the CBA/CNA, identifies solutions to solve or mitigate gaps. Analysts divide these recommended solution approaches into two areas—ideas for materiel approaches and ideas for non-materiel approaches.[10] Ideas for material approaches are recommended solutions that build new materiel capabilities (e.g., a new weapon system). Ideas for non-materiel approaches are non-materiel recommendations to mitigate capability gaps; these recommendations do not involve building new hardware. Non-materiel solutions include recommended changes to the Army's DOTMLPF-P domains and improvements to current materiel solutions that significantly mitigate gaps defined in the FNA portion of the CNA.

Implement

So, how does the Army use CNA output? Results of a CNA/CBA provide a list of tasks, conditions, and standards and a prioritized list of DOTMLPF-P solutions to sustain in the POM (these are programmed and current solutions). Output results also include a prioritized list of capability gaps and a prioritized list of potential non-materiel solutions, existing-materiel solutions, and new-materiel approaches to mitigate the gaps. The Joint Capabilities Integration and Development System (JCIDS) process integrates CNA results into the Defense Acquisition System[11] and the planning, programming, budgeting, and execution process.[12] Figure 2, shown previously, lists the capabilities development initiatives informed by CNA output products:

Program Objective Memorandum Development. The CNA evaluates current Army capabilities to create a prioritized list of existing DOTMLPF-P solutions, including making recommendations on what to do with current programs of record. This prioritization helps the Army leadership determine which capabilities to emphasize and assists them with "trade space" decisions between Armywide systems and capabilities.

Strategic Portfolio Analysis Review. The CNA provides prioritized, analytical results to help Army leaders make tough resourcing decisions. The Strategic Portfolio Analysis Review (SPAR) looks at all existing Army programs and then prioritizes them. Each year, as part of a SPAR, the Army rank orders hundreds of its equipment programs—from helicopters, to boots, to rifles—in terms of their impact on warfighting capabilities. The SPAR output helps guide Army leaders when making decisions on how to best allocate dwindling Army modernization funds. In addition to evaluating existing Army programs, the Army uses the SPAR information to assess concepts that the Army does not currently have as a program of record. As such, the SPAR process can accelerate the development of critical capabilities for the warfighter by identifying new programs and new technologies.

Army Warfighting Challenges Framework and Campaign of Learning Events. The AWFCs are enduring first-order Army problems, the solutions to which improve the combat effectiveness of the current and future force. The ARCIC uses the AWFC framework as the organizing construct to lead future force development and capability integration efforts. Capability gaps and solutions the Army identified in the CNA are now evaluated through CoL events. The CoL events are organized evaluations (e.g., gaming exercises and computer simulations) designed to assess and evaluate AWFCs.

Science and Technology and Industry Research and Development. The CNA gaps inform new ideas and learning that drive basic research and may become the basis for subsequent applied research. Applied research identifies emerging technologies that suggest a solution approach to a prioritized, non-system-specific Army capability need (gap). Scientists involved in applied research look at CNA capability gaps and consider multiple imaginative and innovative means to mitigate these Army gaps. Scientists working for organizations such as the Army Research Laboratory, Defense Advanced Research Projects Agency, Intelligence Advanced Research Projects Activity, and Massachusetts Institute of Technology Lincoln Laboratory, as well as industry and academia, are investigating many technologies to mitigate intelligence gaps. Ongoing work will affect tactical and operational all-source intelligence analysis, intelligence

collection operations, processing and exploitation, and intelligence synchronization efforts.[13]

Future Focus of the Capabilities Needs Analysis

Each year, ARCIC enhances the capabilities and efficiencies of the JCIDS analysis process. Upcoming improvements to the ArCAT will focus on improving analysis techniques, increasing the input data standards throughout the CNA, and establishing CoL/experimentation tools. Planned changes to the ArCAT will help improve gap definitions and fidelity, which will help identify more specific and exacting solution recommendations. By having more detailed specifics and rigor, Army leaders can make more informed and confident decisions regarding future warfighter capabilities. To improve data input capabilities for the ArCAT, the ARCIC plans to move the CNA database onto the Secret Internet Protocol Router Network. Once this goal reaches realization, CNA technicians across the Army will use one common platform/server to perform their warfighting CBA and CNA evaluations. This will improve efficiencies to all current input demands of the ArCAT. When it takes less time to input data into the ArCAT, CNA technicians can spend more time conducting the analysis.

Conclusion

The CNA assesses the Army's ability to perform future organizational and functional missions as defined by joint and Army concepts. The CNA process is TRADOC's CBA. As such, the CNA provides the analysis foundation for all follow-on JCIDS documentation work within TRADOC. It takes into account the current and programmed DOTMLPF-P solutions to determine where the Army has gaps in required capabilities. As a capabilities analysis tool, the CNA uses proven methods and straightforward standards to produce credible, defendable, and repeatable evaluations that draw from warfighter experiences, best practices, and lessons learned. Capabilities development across the Army requires analysis, synchronization, and coordination to ensure formations are fielding the right capabilities at the right time—this is a team effort. The objective analysis provided by the CNA informs a wide range of Army procurement processes to ensure that our Army and Soldiers have the capabilities they need, today and in the future.

Endnotes

1. U.S. Army Training and Doctrine Command (TRADOC), Capabilities-Based Assessment (CBA) Guide, Version 3.1 (Ft. Eustis, VA: TRADOC, 10 May 2010), C-2.

2. Ibid., C-9.

3. U.S. Army Capabilities Integration Center, "Capabilities Needs Analysis (CNA) Briefing," 2016.

4. TRADOC Regulation 71-20, Concept Development, Capabilities Determination, and Capabilities Integration (Ft. Eustis, VA: TRADOC, 28 June 2013), 21-22.

5. Ibid., 12.

6. Ibid., 56.

7. Ibid., 57.

8. Ibid., 58.

9. Ibid., 59.

10. Ibid.

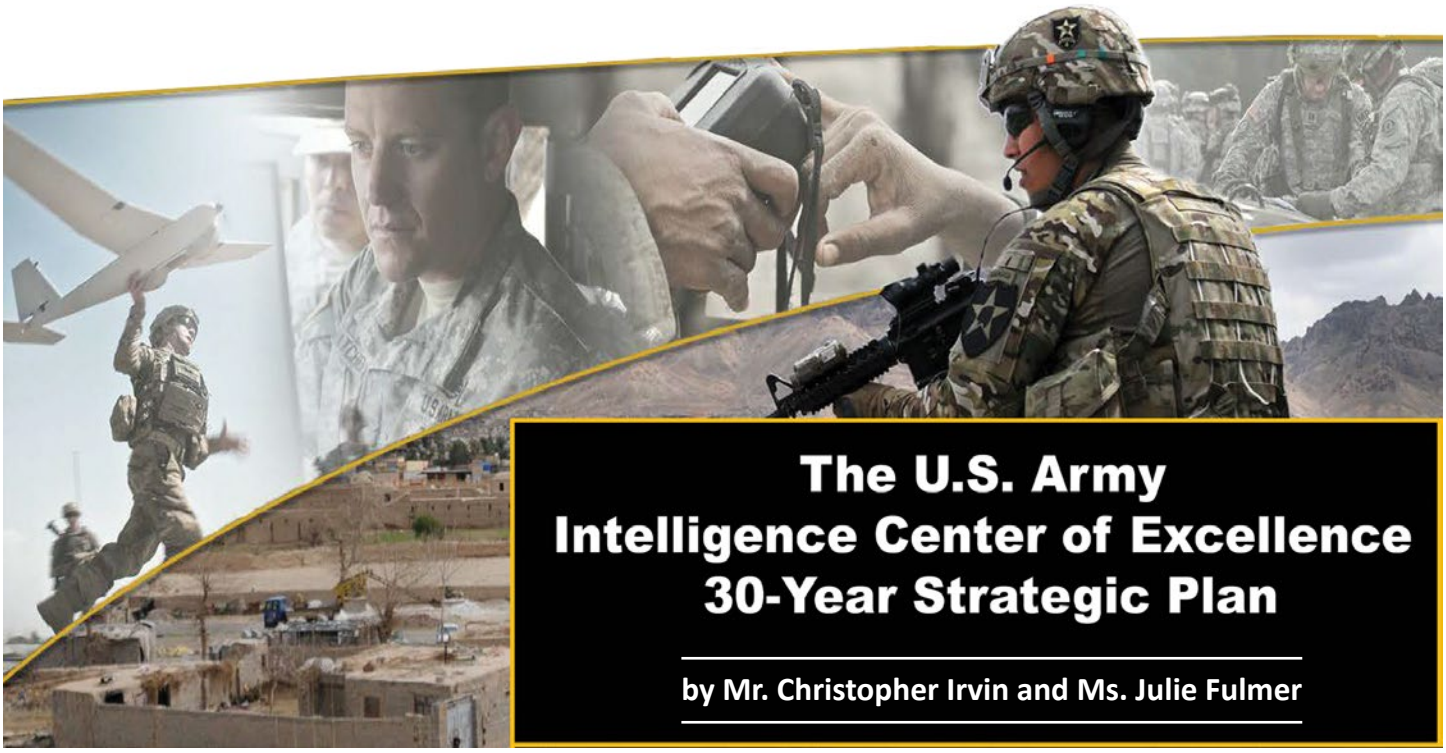
11. Ibid., 96-97.

12. Army Regulation 71-9, Warfighting Capabilities Determination (Washington DC: Government Publishing Office, 28 December 2009), 1.

13. E. Dunlop, "U.S. Army TRADOC's Science and Technology Needs for the Warfighter"(white paper, 7 July 2017); GEN David G. Perkins, TRADOC Commanding General, Letter to Ms. Steffanie B. Easter, Acting Assistant Secretary of the Army for Acquisition, Logistics, and Technology, 31 July 2017.

Mr. Jim Staley leads the Intelligence Capabilities Development Team at the U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. In 2007, Mr. Staley retired from the U.S. Air Force after 23 years of service. He received a bachelor of science in geophysics from Boise State University and a master of science in atmospheric science from Colorado State University.

Ms. Edwina "Genie" Kelly is the USAICoE capabilities needs analysis (CNA) government lead. Since 2006, she has directed and managed CNA team members and USAICoE subject matter experts across the USAICoE Capabilities Development and Integration Directorate. In 2008, Ms. Kelly transferred to the U.S. Army retired reserve after 24 years of service. She received a bachelor of arts in technical drafting from Catawba College and completed the Command and General Staff Officers course.



The U.S. Army Intelligence Center of Excellence 30-Year Strategic Plan

by Mr. Christopher Irvin and Ms. Julie Fulmer

The U.S. Army Intelligence Center of Excellence 30-Year Strategic Plan is a collaborative effort. It involves decision makers across the Department of the Army staff, Training and Doctrine Command, Materiel Command, Forces Command, and Intelligence and Security Command, with input from U.S. academia and industry. To assist in implementation, the plan addresses capabilities across the six operational layers (space, aerial, terrestrial, identity, foundation, and training). Within the context of each layer, the strategy describes decision milestones, science and technology insertions, key recommendations, and budget timelines.

As we build the future Army intelligence enterprise, it is imperative that our strategy meet the required capabilities to defeat our adversaries in multi-domain battle through the full range of military operations. While the future poses many challenges for the Army, unified action partners, and intelligence professionals, the 30-year strategic plan charts a course to successfully operate and win in the ever-changing operational environments. To meet these challenges, Army intelligence must coordinate modernization efforts, including capabilities such as—

- Multi-modal sensing suites that improve the speed of understanding.
- Freedom of maneuver and support to targeting.
- Reconfigurable systems with multi-level security and data transport capability.
- Sufficient bandwidth that is interoperable within unified action partner environments in a distributed processing, exploitation, and dissemination (PED)-enabled enterprise.

The U.S. Army also requires reliable, maintainable, and expeditionary intelligence platforms with mobility characteristics and visual signatures that are interoperable with supported Army formations. New intelligence capabilities must possess modular and scalable designs to support tailored mission packages and sufficient protection against threat spectrums with the ability to protect against small arms fire, small explosive threats, and cyberspace attacks.

Background

The 30-year strategic plan is born out of rigorous analysis, anchored by the Force 2025 governance process, with input from the capability needs analysis, strategic portfolio analysis review, and program objective memorandum. This corporate analysis has yielded a three-phase approach that exploits lessons learned from the Force 2025 Maneuvers Campaign of Learning, which identifies and links potential modernizing solutions to capability requirements. The campaign of learning focuses on critical operational challenges and serves as an important driver for capabilities development.

The campaign of learning consists of an essential series of events that ensures the U.S. Army is a learning and adaptive organization. It is the foundation for credible input to the Army modernization plan, as results from campaign of learning events help identify and link potential modernizing solutions to capability requirements. The Army Capabilities Integration Center, the Combined Arms Center, and each Center of Excellence drive learning and capability development by describing military problems and gaps in current and future force capabilities. These descriptors take the form of Army warfighting challenges. The knowledge gained

from the Army's campaign of learning helps inform senior leaders of the 30-year strategic planning efforts between capability developers, materiel developers, training developers, and supporting science and technology community experts. This integration enables senior leaders within the intelligence community to address the Army's enduring challenges and frame required capabilities for future warfare.

Objectives

The 30-year strategic plan addresses three objectives across near, mid, and far time frames designated by the Army Operating Concept. The near-term phase (present to 2020) objective is to enhance support to regional aligned forces and global response forces by improving existing capabilities. The mid-term phase (2020 to 2030) objective is to incorporate new and improved capabilities into the intelligence enterprise and provide a bridging strategy by leveraging science and technology efforts. The objective of the far-term phase (2030 to 2040) is to integrate the optimized capabilities with the future capabilities to support an extensive range of potential Army mission sets. To accomplish these objectives, the 30-year strategic plan addresses capabilities across the six operational layers (space, aerial, terrestrial, identity, foundation, and training).

Space Layer. The space layer provides support to situational understanding globally in denied areas for indefinite periods of time, and provides the communications paths to enable intelligence support to cyber operations, home-station mission command, and global PED.

Aerial Layer. The aerial layer focuses on producing advanced sensors and technologies that enable the fusion of geospatial intelligence (including full motion video), measurement and signature Intelligence, and signals intelligence collection through cross-cueing. This enhances the overall collection capabilities of current and future aerial intelligence, surveillance, and reconnaissance platforms. The aerial layer is also capable of conducting worldwide operations in austere environments while performing collection efforts against a variety of adversaries. These platforms execute the multi-intelligence collection of enemy personnel, vehicles, surface vessels, ground structures, signal sets, topographic disturbances, and chemical traces related to the production of explosives and narcotics. The end-state is to integrate advanced multi-intelligence and multi-modal sensing capabilities that will further improve enemy threat detection, indications and warning, and overall situational awareness and understanding for tactical commanders. These sensor capabilities will incorporate an open architecture that will enable the technological advancement of existing sensor technologies through an evolutionary process.

Terrestrial Layer. The terrestrial layer provides integrated, interoperable, and networked intelligence capabilities across intelligence disciplines to support decisive action. These capabilities allow synchronization of intelligence resources across partner organizations, while providing responsive support to situational understanding. Human dimension integration and leveraging the human dimension community of practice enhance collective and individual situational understanding in complex and ambiguous operational environments. Science and technology alignment and synchronization with programs of record throughout the 30-year strategy ensure efficient and effective technical improvements to systems. Complementary collection layers (space, aerial, and terrestrial) of Army and unified action partner collectors achieve cross-domain operations synergy. The Army must improve PED capabilities for this layer in conjunction with the aerial and foundational layers to provide a complete solution.

Identity Layer. The identity layer comprises biometrics, forensics, document exploitation, and machine foreign language translation capabilities that provide scalable and sharable

mechanisms to map and monitor the population at the individual identity level.

Foundation Layer. The foundation layer is composed of analytic centers, repositories, other partner data centers, and local systems that store, aggregate, and analyze data to generate information to support operations. Information collection operations and intelligence production will provide responsive and persistent access to the intelligence enterprise hardware, software, and network architecture.

Training Layer. The training layer is the basis of the "no intelligence Soldier at rest" theme. The Army training strategy, the Army intelligence training strategy, and the home-station training strategies inform the framework that makes up the long-range training plan. The focus is a holistic effort with emphasis on the operational training domain.

Way Ahead

As we build the future intelligence enterprise, it is imperative that our strategy meet the required capabilities to defeat our adversaries during future multi-domain battles. Fiscal year 2018 and beyond Army intelligence will continue to align modernization efforts to address Army warfighting challenges identified in the Army Operating Concept and will augment the Chief of Staff's Big 6 + 1 modernization priorities by documenting requirements and driving the development of the following capabilities:

- Multi-modal sensing suites that improve the speed of understanding, freedom of maneuver, and support to targeting.
- Reconfigurable systems design with multi-level security and data transport capability in a distributed PED-enabled enterprise with sufficient bandwidth that is interoperable in unified partner environments.
- Reliable, maintainable, expeditionary platforms with the same mobility characteristics and visual signatures as supported formations.
- Modular and scalable designs to support tailored mission packages.
- Sufficient protection against threat spectrums with the ability to protect against small arms fire, small explosive threats, and cyberspace attacks.

In the near term, the intelligence community must identify modernization goals, support science and technology efforts, and integrate new technologies into individual capabilities while maintaining the integrity of the enterprise. Modernization in the mid and far term requires cautious

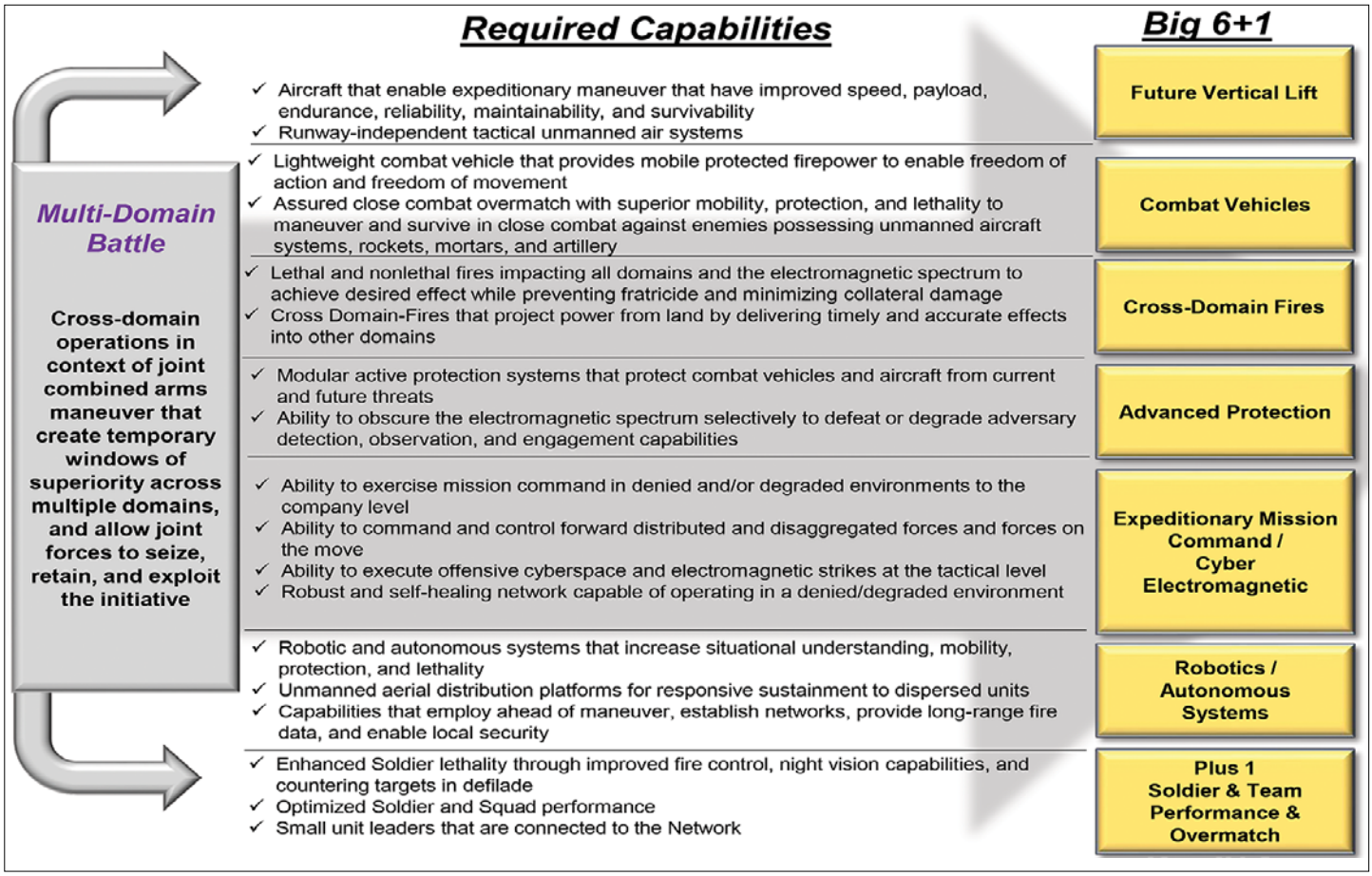


Figure 1. Required Capabilities to support Multi-Domain Battle.

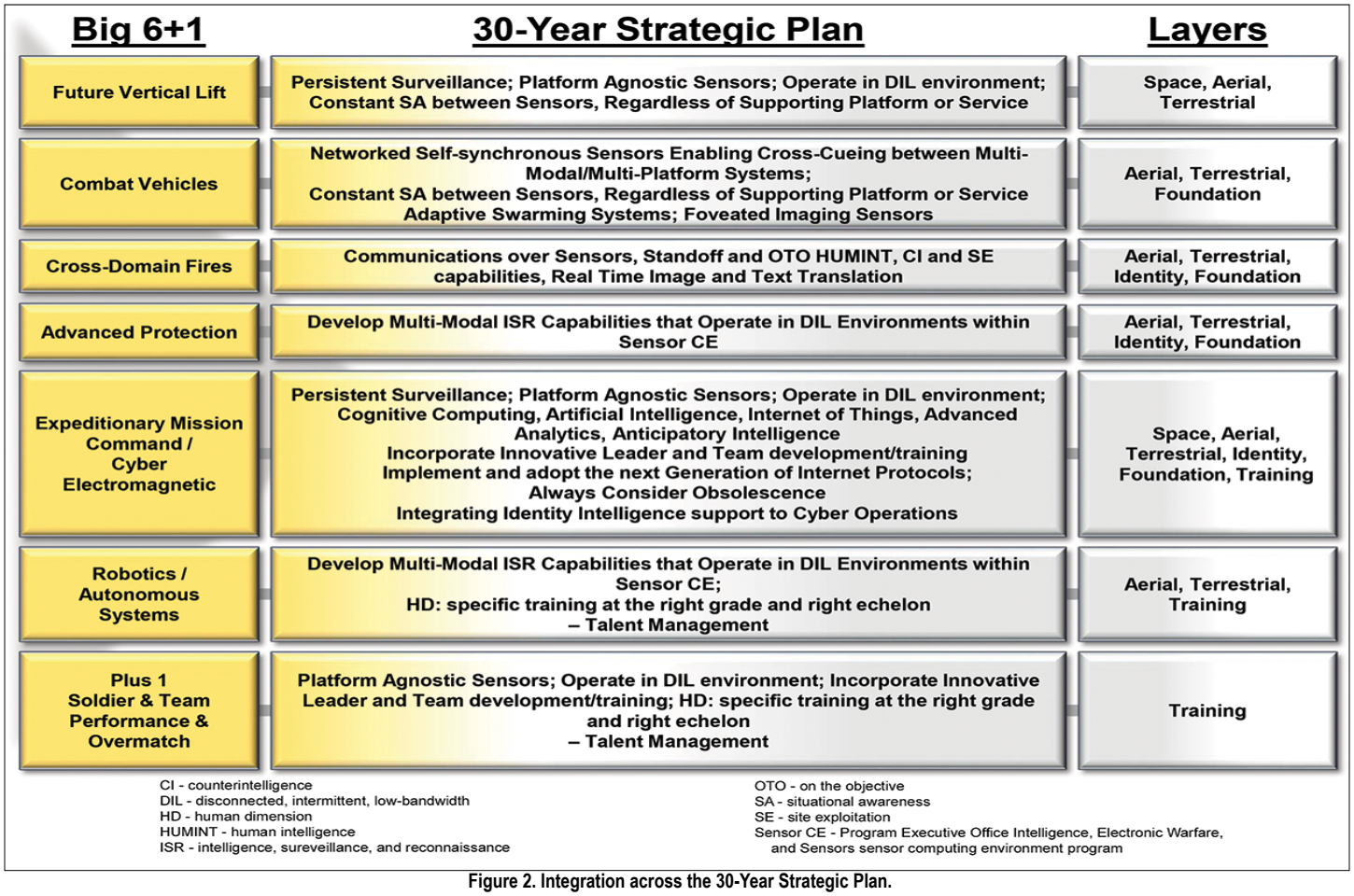


Figure 2. Integration across the 30-Year Strategic Plan.

investments discussed during the strategic portfolio analysis review. Therefore, our fiscal year 2018 30-year strategic plan will synchronize with Army-required capabilities that support multi-domain battle as they align with the Chief of Staff's Big 6 +1 modernization strategy. Figure 1 and Figure 2 show linkages between first order requirements, Big 6 + 1 initiatives, and capabilities within the 30-year strategic plan as aligned by layer.

Conclusion

While the future poses many challenges for the Army, unified partners, and intelligence professionals, the Army Intelligence 30-Year Strategic Plan will continue to chart the course to meet the emerging challenges, improve current capabilities, and function in changing operating environments. The development focus rests squarely on the Army operating concepts and insights yielded from the Force 2025 Maneuvers Campaign of Learning. Using near-, mid-, and far-term objectives metrics during analysis will support initiatives for tangible outcomes to shape and enable future maneuver forces. Army intelligence forces will continue to collaborate with stakeholders and unified partners to enable timely and expeditionary situational understanding, ensuring that future commanders and decision makers operate from a point of relative advantage to fight and win in a complex world.

Mr. Christopher Irvin is chief of the Integration and Analysis Division for the Requirements Determination Directorate, U.S. Army Intelligence Center of Excellence (USAICoE), Fort Huachuca, AZ. Mr. Irvin served 20 years as an Army enlisted Soldier and officer, and 16 years as a Department of Defense contractor and Army Civilian. He has a bachelor of arts in economics and statistics from Campbell University and is a graduate of the Federal Executive Institute. He has a master of science in military operational art and science from Air University through the U.S. Air Force Command and Staff College.

Ms. Julie Fulmer is the USAICoE Force 2025 and Beyond Modernization and Portfolio government lead at Fort Huachuca, AZ. Since 2003, she has managed information exchange and knowledge management among various independent Joint Capabilities Integration and Development System activities across the intelligence warfighting function. Ms. Fulmer received her master of business administration from the University of Phoenix.

The Intelligence Warfighting Function in the Joint Capabilities Integration and Development System

by Mr. Andrew J. Valdez

Introduction

As a young Soldier, I recall driving around the various U.S. Army Training and Doctrine Command (TRADOC) installations and seeing the signs for the Combat Developments Directorate. I would say to myself: "That sounds pretty interesting. I wonder what they do there." I have since learned that the directorate, now called the Capabilities Development and Integration Directorate (CDID), is where many recommendations originate that later become U.S. Army capabilities. The CDID at the U.S. Army Intelligence Center of Excellence is responsible for the functions that result in modernizing the intelligence warfighting function. These ongoing modernization efforts involve the Army's capability development process, the Joint Capabilities Integration and Development System (JCIDS), and the overall acquisition process. This article will explore the intricasies of the JCIDS process, and the role JCIDS plays in development of the future force intelligence warfighting function.

Overview of the Joint Capabilities Integration and Development System

JCIDS is a needs-driven, joint capabilities-based requirements generation process. The primary objective of JCIDS is to ensure that the Department of Defense receives the capabilities required to successfully execute its mission. The Army utilizes JCIDS to validate and prioritize warfighting requirements. It is the lynchpin for supporting the Defense Acquisition System and the planning, programming, budget, and execution processes.

A key output of JCIDS is to produce a development strategy across the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy

Doctrine	☐ Provide operational guidance
Organization	☐ Assess force design ☐ Determine basis of issue
Training	☐ Individual training ☐ Team training ☐ Determine training/skill requirements ☐ Combined Arms Trng Strategy (CATS)
Materiel	☐ System modifications ☐ System upgrades (CCD modifications) ☐ New system start
Leadership and Education	☐ Leader Development Action Plan (LDAP)
Personnel	☐ Soldier development memorandum
Facilities	☐ MILCON memorandum (new construction) ☐ SRM funding request (modify existing)
Policy	☐ General goals and acceptable procedures

Figure 1. DOTMLPF-P Domains.

(DOTMLPF-P) domains, shown in Figure 1, which are the elements of a capability.

JCIDS operates as an integrated, collaborative process, applying strategic guidance for the development of new capabilities through changes in DOTMLPF-P. To optimize the Army's ability to operate, the Army submits the resulting recommendations to the appropriate domain leads. The JCIDS process consists of several standardized documents that become Army requirements. These include:

- Initial Capabilities Document.
- Capability Development Document.
- Capability Production Document.
- DOTMLPF-P Integrated Change Recommendation (at the joint level, this is called the DOTMLPF-P Change Recommendation).

JCIDS relies on a multi-phased methodology nested in joint and Army concepts, which includes an analysis phase embedded in the capabilities-based assessment (CBA).

The Capabilities-Based Assessment Components

The CBA is a deliberate process that identifies current or future capability requirements (needs) measured against the current or projected threat, senior leader guidance, and statutory or regulatory directives. The resulting product of a CBA shows redundant or outmoded capabilities, recommends the most effective approach or combination of solutions, and documents the attributes of effective solutions. The output of a CBA is a recommended DOTMLPF-P materiel or non-materiel solution to solve an Army capability shortfall. The components of a CBA are the functional area analysis (FAA), the functional needs analysis (FNA), and the functional solution analysis (FSA) of non-materiel and materiel approaches. Figure 2 depicts the basic CBA phases.

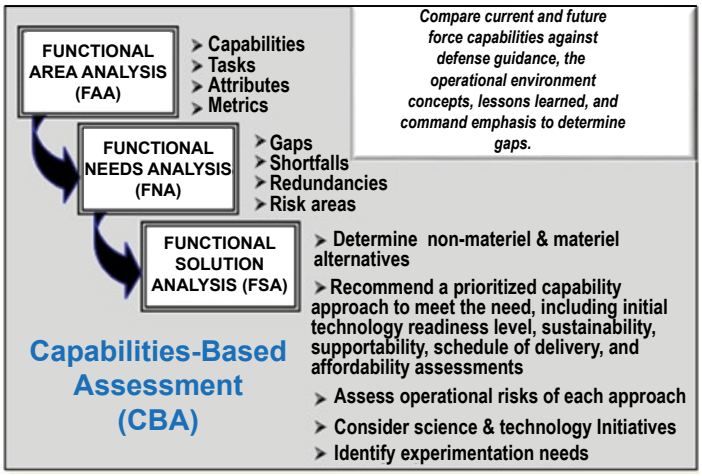


Figure 2. The Capabilities-Based Assessment Phases.

Functional Area Analysis. The FAA is a snapshot in time of the Army's existing ability to accomplish a mission in terms of operational tasks, conditions, and standards, and it identifies what the Army needs to accomplish a new mission area. The FAA's output is a list of required capabilities with their associated tasks, conditions, and standards. Often, the input to the source document from which the capabilities derive is an approved functional concept or a concept of operations that describes—

- How the force will operate.
- The operational environment and time frame.
- The needed capabilities to accomplish a mission.
- The force's defining physical and operational characteristics.

Functional Needs Analysis. The FNA is the second analytic phase in the CBA. The initial output of the FNA is a list of all gaps in the capabilities required to execute a concept to standard. Applying a risk analysis to these gaps allows capability developers to create a list of prioritized gaps (needs)—capabilities for which solutions must be found or developed. Not all capability gaps will become needs. The FNA assesses the ability of current and programmed Army capabilities to accomplish the tasks identified in the FAA. The FNA determines which tasks identified in the FAA cannot be performed, performed to standard, performed in some conditions, or performed in the manner that the concept requires in the current or future force. It also determines which of these capability gaps pose a sufficient operational risk to constitute needs that require a solution. By definition, capability needs are those capability gaps that may present unacceptable risk.

Functional Solution Analysis. The FSA is the third analytic phase in the CBA. The FSA describes the ability of specific ways to mitigate the gaps identified in the FNA. The FNA high-risk capability gaps are inputs to the FSA. The outputs of the FSA are the potential materiel and/or non-materiel solutions to resolve the capability needs of the Army. The FSA is a two-step process that looks at ideas for non-materiel solutions to capability gaps (DOTMLPF-P domains) and ideas for materiel solutions to capability gaps. Potential non-materiel recommendations include one or more of the following:

- Changing policy.
- Changing doctrine.
- Reorganizing the force.
- Training and educating in innovative ways.
- Acquiring materiel that improves existing acquisition programs (or acquiring more).
- Increasing personnel strength.
- Realigning, improving, or creating facilities to support new mission areas.

Materiel initiatives tend to fall into three broad categories:

- Information systems.
- Evolution of existing systems.
- New start systems that differ significantly in form, function, operation, and capabilities from existing systems.

Capabilities Documents and DOTMLPF-P Solutions

Materiel requirements documentation establishes the need for a materiel acquisition program, describes employment of the materiel, and specifies what the materiel must be capable of doing. As an acquisition program progresses, required performance and design specifications become

more specific. The Initial Capabilities Document (ICD) initiates the Defense Acquisition Management System and establishes the enduring need for an acquisition program. The Capability Development Document (CDD) and the Capability Production Document (CPD) define the system capabilities required to satisfy an approved materiel need, and project managers must use them to progress through an acquisition program using Army-provided funding.

Initial Capabilities Document. The ICD is a broad statement of a required materiel capability that can possibly support more than one developmental system. For example, the counter-concealment ICD provides the basis for sensors designed to deny an enemy the ability to conceal activity. This ICD is the foundation for the creation of sensors such as hyperspectral imagery and the U.S. Air Force's challenging targets capabilities. The document describes capability gaps derived from the CBA in warfighting concepts and integrated architectures. The ICD describes why non-materiel solutions do not fully mitigate capability gaps and the need for a materiel solution. In essence, the ICD proposes a materiel solution based on analysis of the various solutions and describes how the recommended solution best meets the required capability.

Capability Development Document. The CDD serves as the "living" document to carry the program and its increments through the acquisition process. It is the primary means to define measurable capabilities for an acquisition program. It captures the information necessary to deliver an affordable and supportable capability using mature technology. In short, the CDD is the roadmap for planning, directing, and managing an acquisition program to satisfy a validated materiel requirement. The CDD describes a technically mature and affordable increment of a militarily useful capability demonstrated in a relevant environment. The capability described in a specific increment may provide only a partial solution of the ultimate desired capability; therefore, the first increment's CDD must provide information regarding the strategy to achieve the full capability. Subsequent increments, leading to the full capability, are also described to give an overall understanding of the program strategy. The components of a CDD are many:

- Operational capability.
- Threat.
- Integrated architectures.
- Required capabilities.
- Program support.
- Supportability.
- Force structure, DOTMLPF-P impact, and constraints.
- Schedule.
- Program affordability for the system.

Most importantly, the CDD identifies the operational performance attributes that are testable or measurable. It defines key performance parameters (KPPs) and key system attributes (KSAs) that guide the development, demonstration, and testing of the capability.

Capability Production Document. The CPD further refines the KPPs and KSAs, leading to the production of a specific materiel solution. The ICD, CDD, and results from developmental and operational testing guide development of the CPD. It provides the operational performance characteristics necessary for the project manager to produce and field a specific system. The CPD presents performance characteristics, including KPPs and KSAs, to guide the production and deployment of the system. The refinement of performance attributes and KPPs is the most significant difference between a CDD and a CPD.

DOTMLPF-P Integrated Change Recommendation. DOTMLPF-P solutions are the preferred method for mitigating gaps in required capabilities because they are often the quickest and most cost-effective means of implementation. A DOTMLPF-P Integrated Change Recommendation (DICR) is generated when a change is needed to mitigate a gap

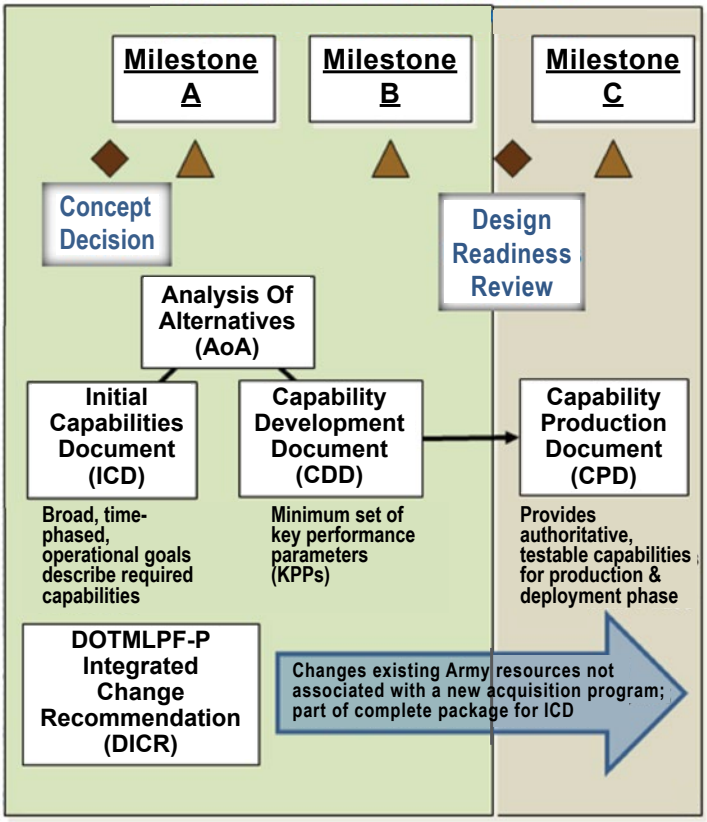


Figure 3. Materiel/Non-materiel Process.

identified during capability analysis, experimentation, or lessons learned but the change cannot be implemented using a force modernization proponent's normal resourcing or a TRADOC reprogramming action. The Army uses the DICR to apply recommended changes to existing Army resources when the changes are not associated with a new defense acquisition program. It is a tool used to inform Army staff processes for integration and synchronization purposes. A DICR can often be tied to an ICD to complete a packaged approach to solving or mitigating critical gaps in required capabilities. There is no policy or guidance specifying which proposed DOTMLPF-P change requires a DICR; therefore, the proponent makes this decision in coordination with the Army Capabilities Integration Center and Combined Arms Command. The recommendation is staffed for Army approval, and provides TRADOC with a vehicle to articulate requirements for which TRADOC is the lead but DOTMLPF-P solutions are beyond programmed resources. Figure 3 (on page 15) shows where the capabilities documents and DICR fit within the acquisition schedule.

Conclusion

JCIDS is only one segment of the Army's capabilities planning approach. It implements a "70 percent solution" with the ability to adjust within the flexibilities provided. The upfront analysis is a key component of the process. The CBAs or other analyses are critical to success. JCIDS captures and prioritizes proposed capabilities through collaboration with other departments, agencies, and the field. Capability developers are highly dependent on concepts and plans that set the stage and inform the institutional Army of existing and emerging needs. Ultimately, the JCIDS process seeks to identify ways to improve Army capabilities through the identification of non-materiel alternatives. When the need arises, JCIDS provides the foundation to implement a strategy for materiel development; therefore, actively engaging the acquisition, test, and science and technology communities early minimizes long-term risk to the overall program. Likewise, engagement with the field by expanding its role in the process enhances the development of capabilities particularly to many in the institutional Army who must "live" vicariously through what is read or available online. In the end, TRADOC is the Army's integrator of capabilities and point of entry to the JCIDS process.

References

Chairman of the Joint Chiefs of Staff Instruction 3170.01I, *Joint Capabilities Integration and Development System* (JCIDS) (Washington DC: Government Publishing Office, 23 January 2015).

Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS), 12 February 2015. https://www.intelink.gov/wiki/JCIDS_Manual.

U.S. Army War College. *How the Army Runs: A Senior Leader Reference Handbook, 2015-2016* (Carlisle, PA: 2015).

U.S. Army Training and Doctrine Command. "DOTMLPF-P Integrated Capabilities Recommendation (DICR) Guide, Version 1.5." 1 June 2016. https://arcic.tradoc.army.mil/ext/jcids/default.aspx.

Mr. Andrew Valdez has been a capability developer since 2004 and is currently Chief of the Capabilities Development Division, Requirements Determination Directorate, U.S. Army Intelligence Center of Excellence. He is a retired CW3 352P, Voice Intercept Technician. His past assignments include 204th Military Intelligence Battalion (Colombia), 10th Mountain Division (Bosnia), and 3rd Armored Division (Desert Storm). He has a master of science in strategic intelligence from the Joint Military Intelligence College and a bachelor of arts in government/history from New Mexico State University.

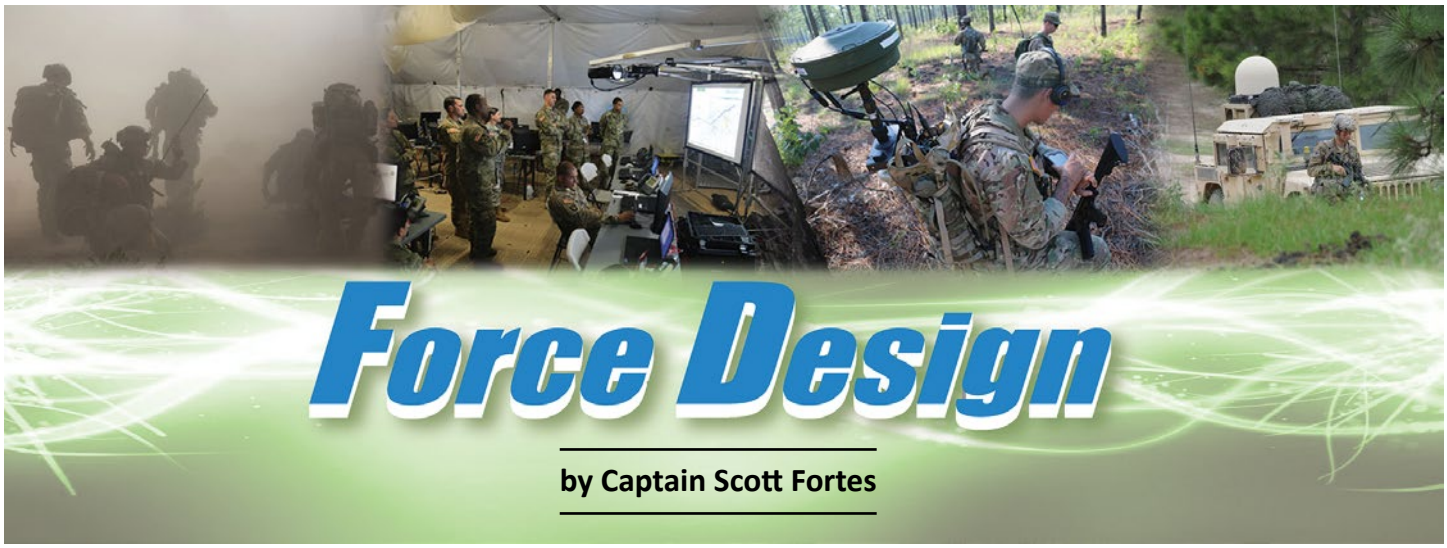
MI History Trivia

On 15 April 1918, Major Ralph Royce made the first American photo reconnaissance flight over enemy territory. How many aerial photographs were taken and reportedly used for intelligence purposes by the U.S. Army during World War I?

A. 13
B. 1,300
C. 130,000
D. 1.3 Million

See answer on page 42.

Aircraft of the 1st Aero Squadron



Force Design

by Captain Scott Fortes

Introduction

During the American Revolution, our new leaders identified a need to establish a professional Army. On June 14, 1775, the Continental Army was formed, and George Washington took command on July 3, 1775. Since then, the U.S. Army has vigilantly protected our Nations's interests while dealing with many challenges and needs. One of these needs is to provide the right forces with the right capabilities to meet numerous responsibilities.

The Army recruits, organizes, trains, and equips Soldiers who operate as members of the joint, interagency, intergovernmental, and multinational teams in an integrated manner.[1] Determining the design of a military intelligence (MI) organization and its capabilities depends on national strategic guidance; in this case the U.S. strategy. This strategy comes from numerous places, starting with the U.S. President's national security strategy under Title 10 of the U.S. Code. The national security strategy provides input to the Secretary of Defense's national defense strategy and quadrennial defense review.

The Chairman of the Joint Chiefs of Staff, who is the principal military advisor to the U.S. President, uses the national defense strategy and quadrennial defense review to implement guidance within the national military strategy; these documents help shape the Department of the Army General Orders and the Army Plan. The guidance identifies—

- The range of military operations that national leaders expect their military forces to perform.
- The results they must achieve.
- The attributes they must possess.
- The locations where they must operate.
- The type and size of force needed to execute those operations.[2]

Force designers use this guidance to develop organizations and equip them with the necessary capabilities to carry out national strategic objectives. Sometimes the needs of combatant commanders determine requirements.

The goal of this article is to provide an overview of the intricate process of capability development used to mitigate gaps that may hinder the Army from performing its role in achieving national, defense, and military strategies.

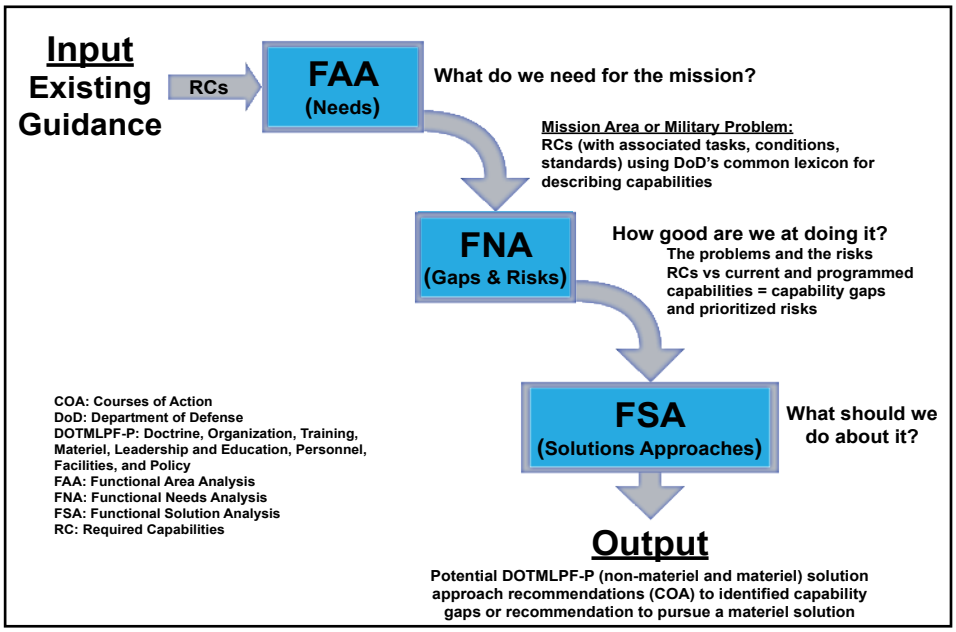
How to Determine the Right Stuff

The Army conducts a capabilities-based assessment (CBA) to determine if the MI force/enterprise has the right "capabilities" to carry out its national strategic guidance. The CBA is a formula used to identify and document capability gaps, determine the attribute of a capability or combination of capabilities that would resolve the gaps, and identify nonmateriel and/or materiel approaches for possible implementation. The CBA comprises three steps:

- **Functional area analysis (FAA).** Performance standards found in the Army Universal Task List and the Universal Joint Task List provide the basis for the FAA.
- **Functional needs analysis (FNA).** The FNA assesses the Army's ability to perform tasks in the FAA using current and future Army capabilities under the full range of military operations. This phase identifies any capability gaps.
- **Functional solution analysis (FSA).** The FSA phase uses the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) approach to determine which capability best mitigates a gap. For example, this could be a change in policy, an update to training methods, or a new type of weapon system.

All solutions to Army gaps begin with the Joint Capabilities Integration and Development System (JCIDS) process. The JCIDS produces a set of DOTMLPF-P solutions that collectively provide the required capabilities needed to fulfill national strategic guidance.

Determining the right capabilities is the responsibility of the Army's Training and Doctrine Command (TRADOC). TRADOC has the mission to develop, educate, and train Soldiers, Army Civilians, and leaders; support unit training; and design, build, and integrate a versatile mix of capabilities, formations, and equipment to strengthen the Army.[3] Under TRADOC are eight centers of excellence (CoEs), including the U.S. Army Intelligence CoE (USAICoE) at Fort Huachuca, Arizona. Each CoE is responsible for identifying any gaps that may cause risks to the national strategic objective. We achieve this through the CBA process, but this is not the only way a gap is determined.



Capabilities-Based Assessment Process.[4]

Field units identify some capability gaps that then make their way into the Army CBA process through an Operational Needs Statement (ONS), an Urgent Operational Needs Statement (UONS), and/or a Joint Urgent Operational Needs Statement (JUONS). An example of this comes from Operation Iraqi Freedom, when improvised explosive devices were the greatest threat to Army Soldiers. This threat created an urgent need for a capability to mitigate improvised explosive devices. The result was a "materiel" solution in the fielding of a new armored vehicle, the Mine-Resistant Ambush Protected. The Army uses these need-statement documents when fielding of a capability must occur quickly, so the Army permits forgoing the entire Total Army Analysis (TAA) cycle. These needs statements are only a few of the documents that contribute to the overall Army CBA process. If an organizational solution is the outcome of the CBA process, that is when force development begins.

Building an Organization

Force development consists of five phases:

- Develop capabilities.
- Design organizations.
- Develop organizational models.
- Determine organizational authorizations (number and rank of personnel).
- Document organizational authorizations.

At Fort Huachuca, Arizona, under the Capabilities Development and Integration Directorate, Requirements Determination Directorate, Operations Support Division, is the Force Design Branch. The job of the Force Design Branch is to develop and document MI personnel and equipment requirements, as well as authorizations for Army intelligence organizations. We work closely with the Operations Support Division, Studies and Analysis Team, and the USAICoE, Office of the Chief, Military Intelligence (OCMI), when determining the best organization for the Army. When you think of force design, think of it in two parts—the "art" and the "science." The Studies and Analysis Team develops the concept, which is the art; and force design is the science because it involves implementing the concept into a design structure. OCMI's role is to determine if the Army can sustain the personnel structure within the organization while not disrupting the grade plate table within the total MI force structure. For example, one question might be, Does the organization create too many captains within the MI force?

The FSA determines whether a new or modified organization is required, and then the process begins with a force design update (FDU). The FDU encompasses many documents, including the unit reference sheet, the table of organization and equipment (TOE) basis of issue plan, and the TAA. The Army uses the FDU to develop consensus changes to existing organizations and to obtain and implement decisions.[5] Not all documents are required to conduct an FDU. Force Design staffs the unit reference sheet for comments throughout the Army before sending it to Headquarters, Department of the Army. The Army staff conducts a force integration functional analysis and analyzes affordability,

supportability, and sustainability. The TOE describes the doctrinal mission of the organization, its dependencies and limitations, essential wartime manpower, and structure or other requirements. The basis of issue plan specifies the planned placement of new or improved items of equipment and personnel in TOEs at 100 percent of wartime requirements.[6] The TAA is the process of how the Army implements force structure, from planning to programming. It determines the best mix of forces that are sustainable while achieving the national strategy.

Conclusion

Force design is only one part of the intricate processes within the TAA cycle. National strategy is the driving force when deciding what military capabilities are required to achieve strategic objectives, with JCIDS being the first stage of capability development. The CoEs continually update capability gaps to ensure they are providing the appropriately trained and equipped leaders, Civilians, Soldiers, and formations capable of carrying out their mission to achieve national, defense, and military strategies. These strategies come from many different sources, including the national security strategy, the quadrennial defense review, national military strategy, and the Army Plan. The CBA comprises three phases—FAA, FNA, and FSA—as the primary method to identify and document gaps, but gaps can be determined outside of the CBA process. Three products—ONS, UONS, and JUONS—describe capability gaps discovered in the field. The Army uses these needs statements to fill capability gaps as rapidly as possible without going through the entire TAA cycle. Force design is a 2- to-5-year process that encompasses multiple stages—too many to describe in this article. Instead, this short overview summarizes the many steps and organizations involved with developing a new military unit or updating an existing one.

Endnotes

1. U.S. Army War College, *How the Army Runs: A Senior Leader Reference Handbook, 2015-2016* (Carlisle, PA: 2015), 1-3.

2. Ibid., 5-1.

3. Ibid., 3-3.

4. Ibid., 3-15.

5. Ibid., 5-12.

6. Ibid., 5-16.

CPT Scott Fortes has served in all three components of the U.S. Army and has accumulated over 20 years of service. He is an Active Guard Reserve officer at Fort Huachuca, AZ, and serves as the Deputy Chief, Force Design Branch. He attended the How the Army Runs course at Fort Belvoir, VA, and earned the additional skill identifier 3R, Force Manager.

The Identity Crisis Facing Echelons Above the Brigade–Building the Future by Remembering the Past

by Lieutenant Colonel (Ret.) Stuart E. Deakin, First Sergeant (Ret.) Irene Zehmisch, and Master Sergeant (Ret.) Wesley M. Good

Editor's Note: This article is part two of a two-part feature split between this issue and the previous quarterly issue. The scope addresses themes of both issues—echelons above brigade and designing the future force. Part one looked to the past; where we have been. It discussed the Cold War and the strategic design of AirLand Battle, contingency operations of the 1980s and 1990s, the modular force transformation, and the impacts of the Global War on Terrorism. Part two continues this examination of force design and will look to the future; where we are going.

> ***Some of the best lessons we ever learn are learned from past mistakes. The error of the past is the wisdom and success of the future.***
>
> ***—Dale Turner, American Singer-Songwriter***

Drawdown: Force Design by Price Tag (2010-2016)

The U.S. budget drove Army force design in the 2010s–or more accurately, the lack of one. The Budget Control Act of 2011 was the final chance, in a series of proposals, to resolve the 2011 U.S. debt-ceiling crisis. All proposals put forth prior to this failed to gain enough support to move into law, as the deadline for an unprecedented U.S. sovereign default drew nearer and nearer. Finally, the White House proposed establishing a compulsory trigger—sequestration—that would go into effect if Congress was unable to reach another agreement by a future date. The intent of sequestration was to secure the commitment to future negotiation toward a true budget by means of an enforcement mechanism that would be unpalatable to Republicans and Democrats alike. However, even this "forcing function" did not result in an approved budget.

After several months of denying that it could or would plan for the implementation of sequestration cuts, the Department of Defense finally began planning in December 2012, with less than one month to go before the directed implementation. The Budget Control Act of 2011 forced the Army to seek the means to deconflict Army readiness with decreased budget levels.

To accomplish this, the Army established Focused Area Review Groups to determine how best to achieve a rapid reduction of the force. Echelons above brigade (EAB) headquarters became the first target for cuts. After all, a generation of Soldiers had "grown up" in an Army that had little use for, or experience with, divisions and corps. A 25 percent reduction was the target for EAB headquarters. Through several iterations, the Army arrived at its current multi-component concept and design for corps and divisions.

The first step was to repurpose the headquarters staff's two command posts. The tactical command post (TAC CP) would be the principal expeditionary command post with all personnel required for execution of forward-deployed operations. The TAC CP saw an increase in size at the division and corps levels allowing for all capabilities required to control current operations and targeting with a minimized capability to plan future operations.

The second step was to develop a multi-component, home-station main command post (MCP) with reduced active strength. The MCP structure contains only those functions performable as reachback for forward-deployed elements. This headquarters design operates primarily from home station during smaller-scale, limited contingency operations. The MCP construct provides longer-term planning and analysis reachback for its forward-deployed, expeditionary command post. The primary sizing constraint for the MCP was to have the capacity to operate 24/7 for at least 90 days until Reserve Component (RC) augmentation arrived. When needed, the design intended to restore operational capacity through activation of an RC operational detachment to augment the MCP. The unit where RC personnel would reside was termed the Main Command Post-Operational Detachment.

This organizational design relies heavily on a trusted Army information network to provide assured communications between forward and main command posts. However, the design lacks the resiliency required for extended or

prolonged operations. Because of the dependency on RC to restore capacity, the design does not adequately account for rapid activation in response to crises. Providing the necessary training and readiness oversight for aligned reserve subordinates in preparation for operational deployments is a strain for EAB commanders.

At the same time as these budget-driven force design decisions, the Army realized that after a decade of persistent conflict our forces faced severe gaps in personnel, technology, training, and readiness. No longer could we assure matching against a near-peer threat.

Back to the Future—Confronting Near-Peer Adversaries Again (Present to Future)

While the U.S. Army was weathering the sea changes throughout the decades of the Global War on Terrorism (GWOT) and drawdown, our former adversaries continued to modernize their technology, modify their force structure, and radically redefine their strategy and tactics. A study commissioned by the U.S. Army Training and Doctrine Command (TRADOC), titled "Russian New Generation Warfare" (RNGW), detailed how the Russians refined their military posture to target United States/North Atlantic Treaty Organization weaknesses instead of overmatching our strengths. Political subversion, coercive demonstrations of strength, and negotiated manipulation are some cornerstones of this strategy geared toward winning public support through information operations before the West could consider any military movements. Our brigade combat team-based Army needed to learn some new concepts and relearn some old ones. Looking to the future, our force design initiatives focus along three lines of effort:

- **Regain** reconnaissance and surveillance capabilities formerly conducted by armored cavalry regiments (ACRs).
- **Sustain** the capability to conduct security force assistance (SFA) missions remaining from the GWOT.
- **Innovate** the successor to AirLand Battle, adding the battlespace domains of space and cyberspace to the classic domains of air, maritime, and land—the multidomain task force.

Reconnaissance and Security Strike Group, or Modernized ACR. The original guidance was to modernize the old ACR design to have similar capabilities to those currently in the armored brigade combat team (ABCT). Multiple courses of action (COA) are under consideration with the directive to consider the lessons from the RNGW study. Cost is still a critical, if not the prime, decision driver.

Course of Action 1, Modernized Armored Cavalry Regiment. COA 1 is an update to the older ACR table of organization and equipment (TOE) with current weapons systems, mission command, unmanned aircraft systems, electronic warfare, cyberspace, and intelligence capabilities. Headquarters, Department of the Army directed that this design would not exceed 4,850 TOE Soldiers, but should be able to conduct reconnaissance and security missions similar to those of legacy "Army of Excellence" ACRs.

The Military Intelligence (MI) Troop under COA 1 consists of 135 Soldiers with a major as the commander. This troop's construct is similar to the brigade combat team (BCT) military intelligence company (MICO), but includes an expanded synchronization and collection management section. The design also includes—

- An intelligence processing team to conduct processing, exploitation, and dissemination (PED).
- A tactical intelligence ground station (TGS).
- Two intelligence communications teams utilizing the Trojan Special Purpose Integrated Remote Intelligence Terminal system (also called Trojan SPIRIT).
- Three multifunctional platoons that each include—
  - A human intelligence (HUMINT) operations management team (OMT).
  - A signals intelligence (SIGINT) control team.
  - Only two multifunctional teams, as a capacity versus cost compromise.

Photo by SGT Juana Nesbitt

Soldiers with Anvil Troop, 1st Squadron, 91st Cavalry Regiment, 173rd Airborne Brigade, conduct aerial reconnaissance procedures, outside Johvi, Estonia, during day one of Operation Siil. Anvil serves as a Reconnaissance Surveillance Target Acquisition Troop and uses tools such as the Raven, a small-unmanned aircraft, to increase the avenues of approach upon an objective.

Resourcing of Troop/Company Intelligence Support Teams (T/CoIST) would be at two per cavalry troop, as a similar capability/capacity/cost design decision. The design assigns the T/CoIST to the squadron S-2 section for training and readiness in garrison, and attaches the T/CoIST to the cavalry troops for operational missions.

Course of Action 2, Reconnaissance and Security Strike Group (-). COA 2 is a compromise between the Modernized ACR design and an objective, unconstrained Reconnaissance and Security Strike Group (RSSG) described in COA 3 below. Just as COA 1 was limited to a personnel strength of 4,850 Soldiers, this design refines the ACR design based on experimentation and analysis. The RSSG (-) integrates select new capabilities to address extremely high-risk capability gaps against peer competitors. The RSSG(-) MI Troop consists of 154 Soldiers. This troop is similar to the COA 1 Modernized ACR MI Troop but expands the multifunctional platoon to include three multifunctional teams.

Course of Action 3, Objective Reconnaissance and Security Strike Group. COA 3 is the resource-unconstrained Objective RSSG design. It is based on conclusions from TRADOC's Campaign of Learning and the RNGW study. The design integrates capabilities that improve lethality and survivability, and addresses additional U.S. European Command and U.S. Army Europe gaps at EAB (e.g., long-range fires, electronic warfare/cyberspace, engineer mobility/counter-mobility, SIGINT/electronic intelligence, and enhanced sustainment). The RSSG would be capable of conducting decentralized operations, fighting across multiple domains, and performing reconnaissance and security missions at either division or corps levels.

The Objective RSSG design includes an MI Squadron consisting of 355 Soldiers. A Headquarters Troop consists of—

- Standard elements required by organizational design standards.
- An intelligence and electronic warfare systems integration section.
- Two intelligence communications teams utilizing Trojan SPIRIT.
- A motor maintenance section.

The Information Collection Troop consists of 125 Soldiers. This troop includes—

- A counterintelligence (CI) and HUMINT platoon consisting of—
  - One CI OMT.
  - Four CI teams.
  - One HUMINT OMT.
  - A 17-Soldier HUMINT (interrogation) section.
- A PED platoon consisting of two TGS/PED sections similar to the expeditionary MI battalion TGS/PED sections.
- An information collection platoon for intelligence support to the RSSG headquarters commander/S-2.

This objective design will most likely be too expensive to implement fully. Headquarters, Department of the Army is reconsidering increasing the number of ABCTs and buying back some of the combat power lost during sequestration force reductions.

The Security Force Assistance Brigade. The Chief of Staff of the Army (CSA) directed the design of a concept and force structure for continuing and emerging SFA missions. This design will include the basic security force assistance brigade (SFAB) with EAB SFA division and corps headquarters. Since the need is current and ongoing, this capability will develop rapidly—fielding of the first SFAB will be as early as fiscal year 2018.

The core mission of the SFAB is to organize, train, advise, and support foreign security forces in coordination with joint, interagency, and multinational forces to improve partner capability and capacity and facilitate achievement of U.S. strategic objectives.

The SFAB will primarily operate forward deployed in theater as an SFA organization partnered with equivalent or higher echelon host nation security forces to conduct training, unit organization, and support operations. However, the SFAB can also be directed to conduct distributed, task-organized, cross-functional security cooperation activities in support of a Combatant Commander Theater Security Cooperation Plan. The organization of the SFAB is along the same lines as the Army's regular brigades with all warfighting functions represented—mission command, movement and maneuver, intelligence, fires, sustainment, and protection. This organization serves as a cadre organization that can rapidly absorb additional personnel and equipment to serve as a fully functional Army BCT.

The SFAB can detach cross-functional advisory teams at approximately platoon size to increase the area and number of partnered training activities and events. These task-organized formations can support extended duration operations forward in specific theaters by providing a rotational capacity, thereby avoiding continuous deployment of the entirety of the SFAB.

The Multi-Domain Task Force. This is, by far, the most forward-looking and challenging new concept in force design.

Photo Courtesy U.S Army.

A pair of Prophet Enhanced system trucks sit in a training area during a recent field training exercise. The Prophet system has sensors that can intercept enemy radio communications and radio frequencies, and allows the Soldiers manning the trucks to conduct analysis.

Peer adversaries have invested in and deployed capabilities in all domains that can challenge and fracture the employment of the joint force. Our modern adversaries present two main challenges to U.S. military deterrence. First, they can (and will) operate with (and through) proxies and surrogates to employ all instruments of national power to achieve their strategic objectives below the threshold of armed conflict. Subversion, information warfare, and unconventional warfare are inherently difficult, if not impossible, to deter. Second, adversaries will impose great cost and risk to U.S. and combined forces through use of sophisticated, all-domain, anti-access (A2), and area denial (AD) capabilities. If not countered, these A2 and AD capabilities will delay deployment and employment of expeditionary forces across strategic and operational distances. Currently fielded adversary capabilities can exploit existing U.S. weaknesses; such as force deployment responsiveness (due to time and distance) and vulnerabilities in the homeland and partner nations (e.g., fixed bases, ports, and domestic populations). The ability to delay the deployment of forces may enable an adversary to take rapid, decisive action and consolidate gains before U.S. and allied forces can respond with sufficient force. How will the Army, as part of the joint force, and with partners, deter and defeat increasingly capable peer adversaries intent on fracturing allied and joint force cohesion both in the competition period short of armed conflict and, when necessary, in armed conflict?

The CSA directed development of the Multi-Domain Task Force (MDTF) to specifically address the Army's A2 and AD warfighting capability gaps and capacity shortfalls. The MDTF coordinates, synchronizes, integrates, and employs cross-domain fires through assured mission command networks to neutralize enemy A2 and AD strategies by opening windows of advantage for joint force exploitation. The MDTF is manned, equipped, organized, and trained to employ cross-domain fires in support of Army Service component command or joint task force (JTF) requirements. The MDTF's attached combat power and multi-domain capabilities allow the MDTF to support the JTF commander's deterrence and security cooperation activities, provide early warning, preserve combat power, and provide joint force freedom of action while setting conditions for successful follow-on offensive operations.

Due to emerging growth requirements, the CSA constrained the MDTF to a 2,000 personnel formation. This constraint focuses on balancing affordability with capabilities by resourcing the MDTF headquarters and only the unique multi-domain capabilities that cannot be task organized by existing force structure. There are currently four draft COAs (of which COA 4 is viewed as the most likely) under consideration by the Army staff as being affordable. All of the MI designs include—

- Three Prophet collection systems.
- One or two Trojan SPIRIT systems.
- A TGS.
- An Advanced Miniaturized Data Acquisition System Dissemination Vehicle.
- Multiple Distributed Common Ground System-Army components.

The MDTF Brigade Headquarters design has about 19 intelligence professionals assigned. They are located in the Headquarters/Current Operations and Intelligence Center Section, which includes a target development element and a geospatial intelligence cell. The Intelligence, Cyber, Electronic Warfare, and Space (ICEWS) Battalion within the MDTF is composed of about 335 personnel. The ICEWS Battalion provides multi-domain intelligence collection, PED, and analysis. It synchronizes and employs capabilities that generate non-kinetic effects in cyberspace, the electromagnetic spectrum, and space.

The 61-person MICO within the ICEWS Battalion conducts multi-discipline intelligence analysis, PED, and collection in direct support of ICEWS electronic warfare, cyberspace, and

space operations and in general support of multi-domain (air, land, maritime, cyberspace, and space) situational awareness. It consists of—

- A synchronization and collection management section.
- Cryptologic support teams/technical control and analysis element.
- An intelligence electronics warfare systems integration section.
- A TGS/PED and sensor analysis section.
- A SIGINT collection team, which provides support to electronic warfare and cyberspace operations in addition to its primary collection function.

The MICO also supports MDTF force protection and counterintelligence operations.

Photo by U.S. Army SGT Steven Gallimore

In the Multi-Domain Battle concept, howitzers might one day protect U.S. ships from enemy vessels by firing anti-ship projectiles. Shown here, two CH-47 Chinook helicopters perform tactical maneuvers to place two M777A2 howitzers in position on Sicily Drop Zone at Fort Bragg, NC, May 25, 2017.

In August 2017, MDTF designs and concepts were scheduled for review and approval by Army staff for a decision presentation to the CSA.

The complexity and uncertainty in the global environment mean the Army must become more agile, flexible, and prepared to tackle a broad range of operations through the development of innovative, low-cost, and small-footprint approaches to achieve U.S. security objectives. Echelons above brigade are still experiencing an identity crisis; however, the Mission Command Center of Excellence is leading efforts forward with experimentation and concept development. The future will always be different from how we currently envision it, and the Army 30 years from now will likely look as different from today as today looks from the era of AirLand Battle. Despite our vision for the future, force developers will always need to remember the mistakes—and successes—of the past.

Mr. Stuart E. Deakin is a retired career intelligence officer. Since retiring from active duty as a Lieutenant Colonel in 2004, Mr. Deakin has served as the leader of the U.S. Army Intelligence Center of Excellence (USAICoE) Requirements Determination Directorate Force Development Test/Experimentation Team; a contract support team that provides subject matter expertise and product support to a wide variety of force development tasks for several USAICoE directorates and activities. Relevant Army assignments include serving as the Senior Test Officer at the Intelligence Electronic Warfare Test Directorate and as a Deputy U.S. Army Training and Doctrine Command Systems Manager for Aerial Common Sensor.

Mrs. Irene Zehmisch is a retired First Sergeant currently serving as a contract future force development analyst for the USAICoE. A career 98G/35P, Cryptologic Linguist, she was one of the original 20 military linguists selected to conduct inspections under the Intermediate-Range Nuclear Forces Treaty. She is a veteran of Operations Desert Storm, Joint Guard, and Joint Endeavor. During her career, she achieved Master Parachutist rating. Mrs. Zehmisch holds a bachelor's degree in psychology from Pennsylvania State University.

Mr. Wesley Good has a bachelor's degree in computer information systems with a minor in business. He served 22 years in the Army, retiring as a Master Sergeant. As a former infantryman, he served in units like air assault infantry battalion. After transitioning to military intelligence, he served in assignments ranging from Joint Exercise Planning Observer/Trainer to Life Cycle Manager for the 96B/35F, Intelligence Analyst, military occupational specialty in the Office of the Chief of Military Intelligence. He is currently working as a contractor in the Studies and Analysis branch at the USAICoE with over 17 years of force design experience.

Strength Begins with Science and Technology

by Mr. Daniel C. Tuttle and Mr. Robert D. Sensenig II

Year 2030: An Operational Vignette

The year is 2030. A military intelligence multifunctional team supports a mobile, electronically inconspicuous U.S. Army tactical task force as the task force closes along multiple axes to destroy a defending enemy battle task group. Cyber electromagnetic camouflage techniques conceal the task force from enemy electronic attack, surveillance, and target acquisition sensors. The task force's networked systems are protected from unrelenting enemy denial-of-service and other cyberspace attacks.

Synchronized with nanosatellites and other space surveillance platforms, multifunctional team Soldiers employ a vehicle, which enables them to move within range to support the task force with any number of electronic support or electronic attack actions, while identifying signatures associated with an enemy tank company. Cross-domain guards designed into the intelligence architecture allow the multifunctional team to immediately alert a scout platoon leader to the location of the enemy tanks. Scouts launch an autonomous micro-unmanned aircraft system (MUAS) capable of dynamic in-flight learning, replanning, and reconnaissance. Carrying a miniaturized, integrated hyperspectral and electro-optical sensor, along with a micro-radar sensor for obstacle avoidance, the MUAS flies toward the enemy's location. The automatic target recognition software onboard the MUAS detects the enemy tanks, generates threat track data, and transmits the enemy tank's location to a multi-domain cloud. Operating in the same tip-to-dip kill web, algorithms onboard another unmanned aircraft system—one designed as a low-cost, loitering bomb—employ real-time track data to conduct a time-sensitive strike on the lead tank.

Months earlier, indigenous collaborators working with U.S. Army Special Forces emplaced hundreds of pebble-sized, ultra-low-power unattended radio frequency, acoustic, and seismic microsensors in the nearby city's underground catacombs, tunnels, and sewers. Twelve of these sensors end their dormancy when triggered awake by the movement of 20 people through an underground passage located hundreds of meters from where a military police company protects a coalition headquarters. Developed at a cost of less than $8 per sensor and designed to dissolve if tampered with, these sensors exfiltrate data when emplaced above or below ground.

Assisted by a team of artificial intelligence agents (aka bots) that estimate threat actions from terabytes of ingested multi-intelligence data sources, the bots alert their human teammates to underground movement. A military police company operations sergeant becomes aware of the event seconds after initial detection. The operations sergeant dispatches an armed quick reaction force with a vehicle-mounted, atom-based gravimeter and several handheld accelerometers to find and fix the underground actors. An intelligence analyst assigned to the headquarters exploits infrastructure and security sensors to support the quick reaction force with tactical overwatch and to help the military police determine whether the movement detected underground is friend or foe. Back in the continental United States, cyber warriors use forward-based electronic warfare systems to turn the enemy's own sensors against the attackers.

At the joint task force J-2, intelligence analysts use information technologies with integrated machine learning, high-performance computing, and a number of specialized computer agents and bots to update a global graph of hundreds of millions of interrelated threat and non-threat entities. Analysts interrogate and traverse the graph using simple interfaces that help the analysts make sense of exabytes of hard and soft data from local and regional social media, radio and television broadcasts, traditional sensors, and battlefield situation reports. These agile, flexibly programmed agents help the commander and staff to perceive holistically how dozens of constantly evolving "micro- and macro-situations" impact the overall campaign plan across a complex, fluid battlefield.

Whether this futuristic vignette or any like it materializes depends on how adroitly and imaginatively the Department of Defense (DoD), the intelligence community, and the Army science and technology (S&T) community plan and execute in an age of reduced S&T and acquisitions funding. This article provides an overview of how S&T analysts, technical intelligence experts, requirements managers, scientists, and engineers collaborate to resourcefully develop and transition technologies to provide military intelligence (MI) Soldiers with a measurable, competitive advantage over future adversaries. This article explains how S&T program planning and execution make future capabilities, like the ones described in the operational vignette, possible.

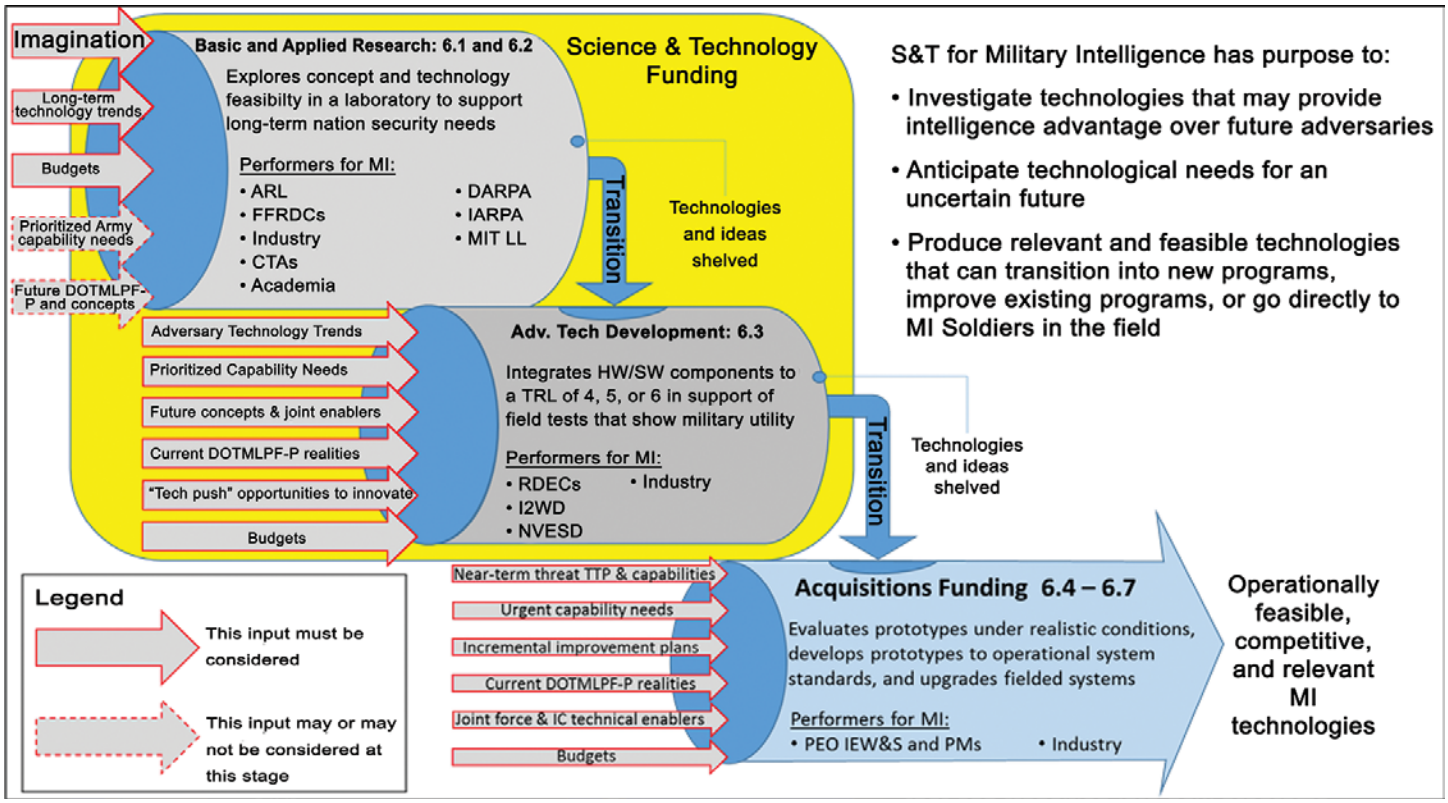


Figure 1. Science and Technology Process and Performer Overview.

As shown in Figure 1, S&T starts with unconventional and unconstrained imagination. Future adversaries will not lack ingenuity or imagination, while technologies once available only to the United States and great powers become available to more and more threat actors. Scientists, researchers, and requirements managers involved in S&T must anticipate future threats, and must think and operate in a much wider orbit beyond the narrow domain of intelligence. Scientists working in basic research quite often begin their work by asking, "What if we could do this?" For them, "this" involves an operational capability thought at the time to be fanciful. Similarly, personnel involved in basic and applied research, the first two funded steps in S&T, must begin their respective efforts with a mind to finish, i.e., to do everything possible in their orbits to see that their ideas and technologies transition to competitive capabilities fielded to MI Soldiers.

Basic Research

Basic research is the study and experimentation designed to exploit new, emerging, and over-the-horizon technological opportunities in support of national security. Basic research occurs across government, industry, and academia. The S&T team supporting the U.S. Army Intelligence Center of Excellence (USAICoE) routinely collaborates with scientists at—

- Army Research Laboratory (ARL).
- Air Force Research Laboratory.
- Defense Advanced Research Projects Agency (DARPA).
- Intelligence Advanced Research Projects Activity.
- Massachusetts Institute of Technology Lincoln Laboratory.
- Numerous private corporations.
- Academic institutes, such as the Calspan-University at Buffalo Research Center.

While personnel engaged in basic research do not necessarily have to be conversant in specific MI capability gaps, nor possess a piercingly clear understanding of current or planned Army MI doctrinal, organizational, training, and materiel paradigms, scientists involved in basic research quite often welcome the chance to understand challenges associated with individual and collective MI tasks on the battlefield.

The Army spends over half of its basic research budget at universities. Each year, the USAICoE S&T team manages studies under the Army study program. Study findings provide Army senior leaders with timely, high-quality insight on critical issues likely to affect the future force. Recent MI studies helped Army and joint force senior leaders to better understand—

- Opportunities to develop multi-sensor data fusion capabilities in support of wide-ranging MI, logistics, medical, fires, and mission command needs.
- Signal propagation and collection opportunities in dense urban environments.
- Technology-based opportunities to provide training that is more realistic.
- How agent-based simulation might lead to consideration that is more rigorous of both friendly and enemy courses of action during deliberate planning.
- The feasibility of entry tests to determine an entrant's aptitude for intelligence analysis.
- Execution of regional alignment as a driver of regional expertise for MI Soldiers.

Applied Research

Ideas and learning gleaned from basic research become the basis for subsequent applied research. Applied research identifies emerging technologies that suggest a solution approach to a prioritized, non-system-specific Army capability need. Scientists participating in applied research look at capability needs and consider multiple imaginative and innovative means to close the gaps.

Today, scientists at ARL, Air Force Research Laboratory, DARPA, Intelligence Advanced Research Projects Activity, and Massachusetts Institute of Technology Lincoln Laboratory collaborate with partners in industry and academia to develop—

- Micro-autonomous systems.
- Manned-unmanned teaming.
- Artificial intelligence and machine learning.
- High-performance computing.
- Natural language processing.
- Quantum computing.

They also develop other technologies that could change the way future MI Soldiers conduct intelligence analysis, synchronization, collection, and processing.

Not all the technologies investigated and developed with applied research monies transition to the advanced technology development stage. Scientists conducting applied research always have the goal to mature and transition the most promising technologies to one of the Army's Research, Development, and Engineering Centers (RDECs), but the Army shelves many of the ideas and technologies investigated during applied research until the right interest or opportunity comes along. It is worth noting that several of the most dominant technologies developed during applied research over the years were not a result of a capability need articulated by the requirements community to scientists. Instead, these capabilities were developed because of "technology push," i.e., scientist and research community recognition of opportunities to significantly improve a U.S. military competitive advantage, such as—

- Global positioning system.
- Radar.
- Nuclear weapons.
- Stealth technologies.
- Reconnaissance and surveillance satellites.
- The internet.
- Long-dwell unmanned aircraft systems. [1]

Advanced Technology Development

The RDEC that plans and executes advanced technology development for future MI capabilities is the Communications-Electronics RDEC, home to the Intelligence and Information Warfare Directorate (I2WD) and Night Vision and Electronic Sensors Directorate (NVESD). I2WD is the Army's center for research and development of advanced cyberspace capabilities, electronic warfare, signals intelligence, radar, and intelligence analysis, exploitation, and dissemination capabilities. NVESD researches and develops sensor and sensor-suite technologies for air and ground intelligence, surveillance, reconnaissance, and target acquisition under adverse battlefield conditions for day and night operations. The I2WD and NVESD design and engineer prototypes for either field experiments or testing in a simulated environment. These two directorates further demonstrate the technological feasibility of a prototype, but not necessarily the operational feasibility.

In recent years, whether via technology pull (based on existing requirements) or technology push, I2WD's engineers developed and transitioned a number of seminal capabilities vital to ongoing global intelligence and electronic warfare missions. These capabilities include the Distributed Common Ground System–Army, Trojan Special Purpose Integrated Remote Intelligence Terminal system (also called Trojan SPIRIT), Common Ground System, Wolfhound, Vigilant Pursuit, Duke, and Warlock.

Looking to the future, I2WD's engineers are developing a number of imaginative, creative ideas to—

- Assist all-source intelligence analysts in making sense of and explaining complex situations.
- Make Army MI competitive versus a near-peer's means of anti-access/area denial.
- Collect in dense urban environments.
- Integrate multi-purpose cyberspace/electronic warfare/signals intelligence functions onto affordable, survivable, and power-efficient platforms.

DoD personnel involved in advanced technology development for MI must collaborate with their counterparts in the intelligence community. DoD and intelligence community systems integration must start early in the advanced technology development stage so that the future force benefits from the full potential of the intelligence enterprise. Today, engineers at I2WD are challenged to integrate the intelligence community's information technology enterprise with DoD's joint information enterprise, all under the standards of the Defense Intelligence Information Enterprise.

Formally, under today's laws and regulations, S&T funding ends with advanced technology development. The system of systems engineering that occurs next receives funding within the acquisitions community, not within the S&T community. Informally, however, S&T continues as is evident in the nature of rapid capability or quick reaction efforts. Today, the Army G-2 leads the Army MI S&T community of interest in an effort to transition the best available ideas and technologies into the force at a much faster pace than is currently practiced within both the S&T and acquisitions communities. Three relatively new organizations designed to close military S&T gaps consist of the Army's Rapid Capabilities Office, DoD's Strategic Capabilities Office, and Defense Innovation Unit Experimental, a fast-moving government organization that provides non-dilutive capital in the form of pilot contracts for commercial innovation to solve technology-related problems in 90 days or less.[2]

Engineers working with advanced technology development funds hand off prototypes to engineers working for one of the program executive offices. For example, I2WD engineers hand off matured prototypes and technologies to the Program Executive Office, Intelligence Electronic Warfare & Sensors. Today, as in the past, technology transition from the S&T community to the acquisitions community has proven to be formidable. S&T transition is a contact sport.[3] Some pretty good players get roughed up and never finish the game.

The following technology vignette adds clarity to the S&T processes just described. The technology vignette employs the scene from the earlier operational vignette with the purpose to exemplify how ideas and technologies from basic and applied research might transition to advanced technology development.

Technology Vignette

A few months ago, indigenous collaborators working with U.S. Army Special Forces emplaced hundreds of pebble-sized, ultra-low-power unattended radio frequency, acoustic, and seismic microsensors in the nearby city's underground catacombs, tunnels, and sewers. Twelve of these sensors end their dormancy when triggered awake by the movement of 20 people through an underground passage located hundreds of meters from where a military police company protects a coalition headquarters. Developed at a cost of less than $8 per sensor and designed to dissolve if tampered with, these sensors exfiltrate data when emplaced above or below ground.

Figure 2 shows the evolution—from basic research, to applied research, to advanced technology development.

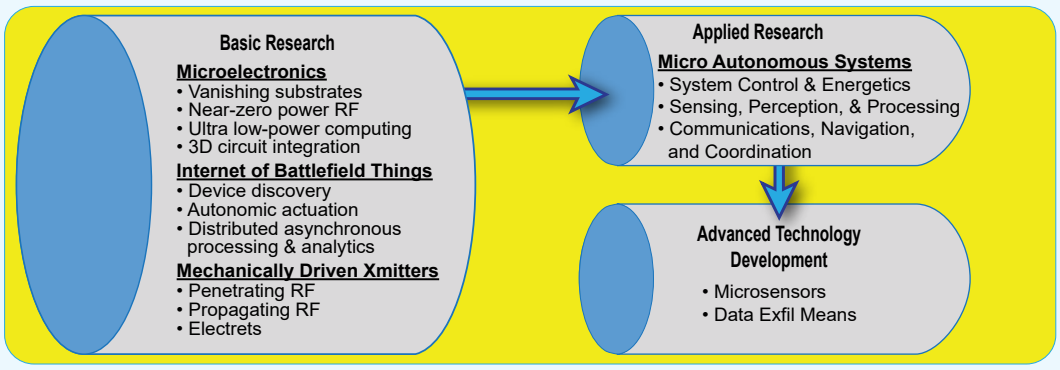


Figure 2. Basic Research to Advanced Technology Development.

Basic Research

The technology vignette begins when requirements managers from the special operations community describe an operational need to scientists at DARPA. The Special Operations Command needs the capability to resupply Operational Detachment-Alpha (ODA) using a concept that does not require the ODA to recover or pack out an unmanned delivery platform. Leaving options wide open, a DARPA scientist takes this approach: "What if the technologies involved in resupply could be made affordable and be made to dissolve, disintegrate, or disappear? What if there was nothing sensitive left to pack out, nothing for the enemy to capture and reverse engineer?" The scientist makes his initial pitch. He explains the possibilities associated with vanishing substrates and cajoles the reluctant. He soon receives sponsorship to develop technologies that enable microelectronic systems to vanish in a controlled manner.[4] Basic research with vanishing substrates leads to advanced technology development of a prototype air-delivery vehicle that rapidly and physically disappears following safe payload delivery. Requirements managers working on MI futures take notice and imagine opportunities to deliver surveillance sensors.

Aware of operational challenges associated with power expenditure in unmanned systems, the same scientist develops an unprecedented ability to remotely wake up microelectronic circuitry in a miniaturized sensor to greatly extend the sensor's duration before battery replacement. A research program he calls "Near Zero Power RF [radio frequency] and Sensor Operations (N-ZERO)" enables remote, unattended sensors that can operate for months, or possibly years, on extremely low power.[5] Each sensor is off, yet constantly alert, retaining greater than 95 percent of the sensor's battery life for sparse signal detection when the time comes. DARPA's N-ZERO research and development directly benefits research conducted by ARL, other government organizations, and affiliated entities exploring potential with numerous other military applications.

At Aberdeen Proving Ground, Maryland, scientists working at the ARL form a collaborative technology alliance with researchers from academia and industry to develop a concept known as the Internet of Battlefield Things (IoBT.)[6] DARPA's N-ZERO project directly benefits development of the IoBT. An IoBT is a set of interdependent and interconnected entities, such as sensors, actuators, computers, weapons, networks, on-node analytics, and Soldiers. These entities are dynamically composed to meet multiple missions in a highly fluid, resource-constrained environment (i.e., an environment in which energy, power, bandwidth, and infrastructure are severely limited). One of the research questions is how might Soldiers on patrol discover and use mission-relevant data from a cooperative sensor? Another research thrust called autonomic actuation asks, how might the IoBT self-configure, self-heal, self-optimize, and self-protect? A third research thrust challenges scientists to consider novel ways to help Soldiers make use of networked sensors that the Army does not own or fully control.

Years earlier, the Army realized that the migration of people across the world to urban centers could eventually lead to operations in dense urban environments, including requirements for subterranean operations. Considering operations in underground spaces, scientists explore ideas for antennas that can transmit and receive signals in low-bandwidth, RF-denied, global positioning system-denied environments, whether underwater or underground.

Applied Research

Basic research in these three areas—microelectronics, the IoBT, and mechanically driven transmitters—contributes to applied research in micro-autonomous systems at the ARL. The ARL's Micro Autonomous Systems and Technology's Collaborative Technology Alliance had the purpose to enhance tactical situational understanding in urban and complex terrain by enabling the autonomous operation of a collaborative ensemble of multi-functional, mobile microsystems to provide timely intelligence, surveillance, and reconnaissance for dismounted Soldiers.[7] One of the research thrusts explores sensing and perception for processing constrained micro-platforms. Another looks at communications architectures needed to transport time-sensitive data to dismounted Soldiers as part of tactical intelligence overwatch.

Advanced Technology Development.

Scientists at ARL hand off results to engineers working in both industry and government. In this case, the technology readiness levels of the various applications and components

Photo courtesy of DARPA

Vanishing Programmable Resources.

needed to design a pebble-sized unattended microsensor are relatively low. Engineers at I2WD begin work with applications that are still speculative or are lacking in proof or detailed analysis to support assumptions. I2WD engineers must integrate basic technological components to demonstrate that they will work together.

Strength begins with S&T. The Army's S&T strategy relies on the unconventional and unconstrained imagination of its professionals to develop and mature technology that will enable transformational capabilities in the future force. At the same time, we must continue to pursue opportunities to accelerate technology maturity for transition into current force systems through basic research, applied research, and advanced technology development.

Endnotes

1. "Course CLE 045, Introduction to DoD Science and Technology Management," *Defense Acquisition University,* 6 January 2016, https://learn.dau.mil.

2. "Work With Us," Defense Innovation Unit Experiments, accessed 1 September 2017, https://diux.mil/work-with-us/companies.

3. U.S. Department of Defense, Manager's Guide to Technology Transition in an Evolutionary Acquisition Environment Version 1.0 (Washington, DC, January 31, 2003), 4-40, https://www.acq.osd.mil/dpap/Docs/AQ201S1v10Complete.pdf.

4. Dr. Roy (Troy) Olsson, "Vanishing Programmable Resources (VARP)," Defense Advanced Research Projects Agency, accessed 1 September 2017, https://www.darpa.mil/program/vanishing-programmable-resources.

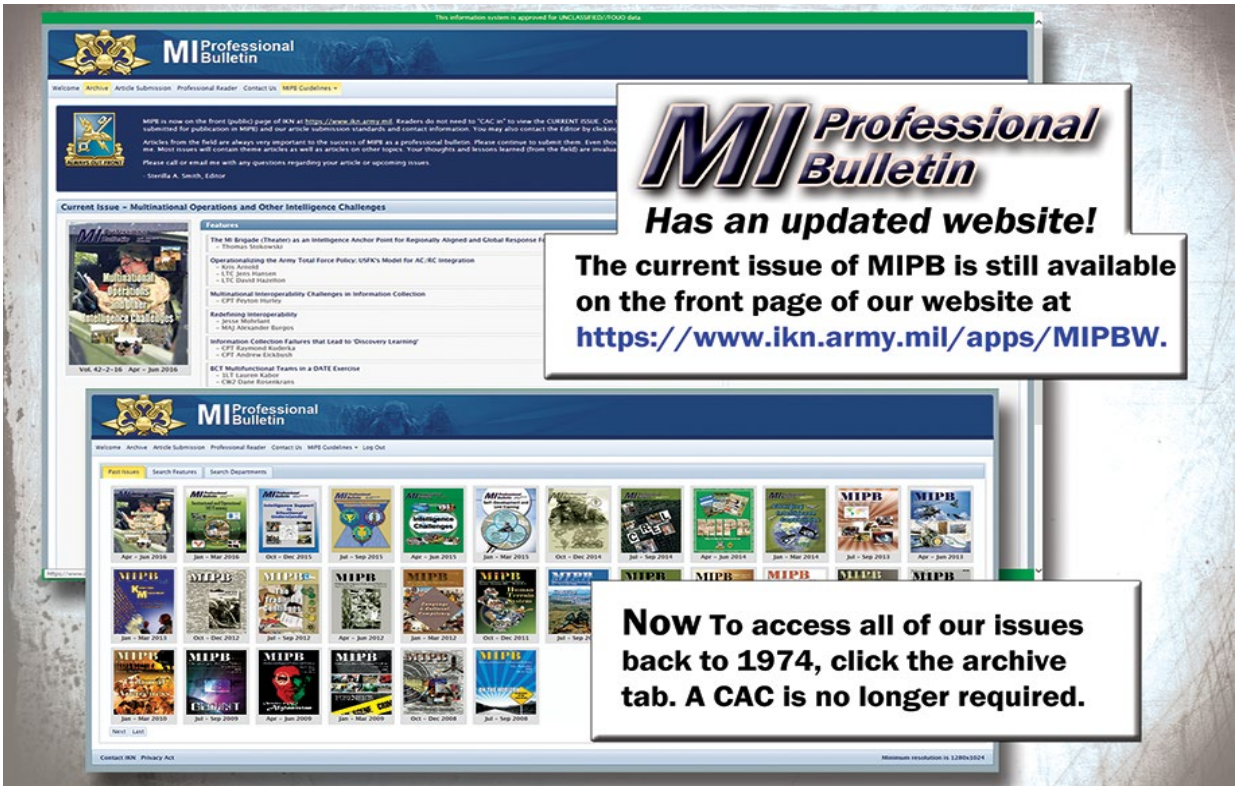
5. Dr. Roy (Troy) Olsson, "Near Zero Power RF and sensor Operations (N-ZERO)," Defense Advanced Research Projects Agency, accessed 1 September 2017, https://www.darpa.mil/program/near-zero-rf-and-sensor-operations.

6. Dr. Stephen Russell, "Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA) Opportunity Day," U.S. Army Research, Development and Engineering Command, 27 March 2017, https://www.arl.army.mil/www/pages/3050/IOBT_CRA-Overview_20170327.pdf.

7. Brett Piekarski, "Micro Autonomous Systems and Technology CTA," U.S. Army Research, Development and Engineering Command, last modified 3 September 2014, https://www.arl.army.mil/www/pages/332/mast-cta-overview-9-1-14.pdf.

Mr. Daniel Clark Tuttle is a retired Army signals intelligence and all-source analysis warrant officer. He now serves as the Science and Technology chief in the Experimentation and Analysis Directorate, Capabilities Development and Integration Directorate, at the United States Army Intelligence Center of Excellence. He is also the U.S. Army Training and Doctrine Command manager for Research, Development, and Engineering Command technology initiatives. He has a bachelor of science from the University of Maryland.

Mr. Robert D. Sensenig II is a retired Army all-source intelligence warrant officer. He served in a variety of assignments and combat tours supporting tactical, joint, and strategic units and is currently assigned to the U.S. Army Intelligence Center of Excellence, Experiments and Analysis Directorate, Science and Technology.



Enterprise Challenge 2018: Multi-Domain Battle Experimentation

by Major Jermaine Carter and Mr. Matthew Malanowski

In their 2017 article about the future of war, General Robert Brown and General David Perkins wrote:

> ***"People like to talk about how the future of warfare will be different, but it has already started to arrive...Across these battlefields, rival powers made investments and developed doctrine, providing ample evidence that future wars promise extreme lethality not seen since World War II...The next fight will be defined by a violent intensity that will test the U.S. military's might in the cauldron of battle...In attempting to remake the global order, these actors are developing and employing technologies and tactics that offset America's military dominance on land, at sea, in the air, and in space and cyberspace."***[1]

The Problem

Studies of the emerging operational environment describe a future of contested norms and persistent disorder.[2] In this environment, the U.S. military will compete with sophisticated peer adversary threats in which all domains are contested—land, maritime, air, space, cyberspace, and across the electromagnetic spectrum. In response to these challenges, the Army is developing a new warfighting concept called "Multi-Domain Battle" (MDB). MDB is a joint combined arms concept that not only outlines required capabilities for the physical domains (land, sea, air, and space) but also places significant emphasis on the cyberspace and information spheres. Examples of some of the major challenges or questions facing the Army under this construct include:

- How do U.S. forces deter the escalation of violence, defeat threat operations to destabilize the region, and turn denied spaces into contested spaces should violence escalate?
- How do U.S. forces maneuver from contested strategic and operational depth with sufficient combat power in time to defeat enemy forces?
- How do U.S. forces conduct deep maneuver by air, naval, and/or ground forces to suppress and destroy enemy indirect fire and air defense systems and reserve forces?
- How do U.S. ground forces defeat the enemy in the close area?

Competing with the future operating environment and the emerging demands of MDB, Army intelligence leaders are reviewing all aspects of current and projected intelligence capabilities. These demands on Army intelligence are broad and far-reaching and include attributes such as platform mobility and survivability, growing access to the intelligence enterprise, and sensor diversification. A significant demand continues to be the development of a high degree of interoperability with our joint, interagency, and coalition partners.

Enterprise Challenge

One event that focuses on those future interoperability challenges is Enterprise Challenge. Sponsored by the Office of the Under Secretary of Defense for Intelligence and managed by the National Geospatial-Intelligence Agency, this annual event drives the development and integration of intelligence enterprise components and architectures, while ensuring baseline interoperability and data exchanges. This annual event is conducted at multiple locations and includes participants from across the Department of Defense, coalition partners, and industry. Enterprise Challenge assesses the Defense Intelligence Information Enterprise alignment and the intelligence, surveillance, and reconnaissance mission workflows; validates interoperability with partners; and creates a low-risk opportunity to demonstrate future intelligence capabilities.

For Army intelligence professionals, the pathway to Enterprise Challenge is through the U.S. Army Intelligence Center of Excellence (USAICoE) Battle Lab. In May 2018, USAICoE will host the Army portion of Enterprise Challenge 2018 at Fort Huachuca, Arizona. In order to address those MDB demands, we are challenging our agency, service, industry, and internal Army partners to help answer important questions such as these:

Photo courtesy U.S. Army

The Winch Aerostat Small Platform, or WASP, is a mobile, tactical-sized aerostat capable of carrying a variety of payloads in support of military operations.

- How can we enhance interoperability and collaboration (i.e., share the capabilities, distribute workflow, etc.) with joint, interagency, and multinational partners?
- How can we strengthen, develop, and validate architecture requirements in an age of big data?
- How can we improve "reach" among partners to increase Army intelligence expeditionary capabilities?
- Is it possible to modify or replace existing sensors to remain effective in the operating environment?
- Can we introduce a "system of systems" approach to persistent surveillance using a variety of alternate sensor platforms (e.g., high-altitude, low-cost, small unmanned aircraft systems; space-based, disposable unmanned ground systems; etc.) regardless of who owns them?

Conclusion

The overall goal of Enterprise Challenge 2018 is to explore with our joint, interagency, and multinational partners those capabilities required to support the emerging MDB concept. While we rely on the willingness of organizations to fund their own participation, we have a multi-year record of successfully integrating many diverse capabilities and objectives. Consider this guiding direction from Generals Brown and Perkins:

> ***"In the future fight, we must evolve from a system defined by stovepipes and parochialism. Future commanders will have a profound breadth and depth of information and access to capabilities providing cross-domain effects, maneuver, and fires. Provided in a federated package of solutions, however, no matter how well executed, our joint capabilities will be vulnerable to a peer adversary with a more united solution. Now is the time to establish a shared visualization and understanding of what the future U.S. military will look like. The U.S. Army is committed to being part of an integrated solution across the services. A solution built on testing, experimentation, and clearly articulating the lessons and subsequent requirements derived therefrom—thus, setting the conditions to design the transformation of the Army from the one that will fight tonight, tomorrow, and in the future."[3]***

Endnotes

1. GEN Robert B. Brown and GEN David G. Perkins, "Multi-Domain Battle: Tonight, Tomorrow, and the Future Fight," *War on the Rocks* (Texas National Security Network), 18 August 2017, https://warontherocks.com/2017/08/multi-domain-battle-tonight-tomorrow-and-the-future-fight/.

2. U.S. Army Training and Doctrine Command, "Multi-Domain Battle: Combined Arms for the 21st Century" (white paper, 24 February 2017), 2, www.tradoc.army.mil/multidomainbattle/docs/MDB_WhitePaper.pdf.

3. Brown and Perkins, "Multi-Domain Battle."

MAJ Jermaine Carter serves as chief of the capabilities and evaluation team for the U.S. Army Intelligence Center of Excellence Battle Lab at Fort Huachuca, AZ. Previous assignments include battalion intelligence officer with the 94th Military Police Battalion in Yongsan, South Korea, and brigade intelligence officer with the 5th Armored Brigade at Fort Bliss, TX. He has a bachelor's degree in history from Delaware State University. He attended the Military Intelligence Captain's Career Course at Fort Huachuca, AZ, and the Army Command and General Staff College at Fort Leavenworth, KS.

Mr. Matthew Malanowski is a retired master sergeant. He is now a Department of the Army Civilian, serving as an intelligence specialist for the Experiments and Analysis Directorate (EAD), U.S. Army Intelligence Center of Excellence at Fort Huachuca, AZ. Before joining EAD, he worked with the U.S. Training and Doctrine Command Capability Manager–Terrestrial and Identity. He has a bachelor's degree in business management from Loyola College and a master's degree in business administration from the University of Georgia.

Doctrine? We Don't Need No Stinkin' Doctrine!

by Mr. Craig Sieting

Doctrine serves many purposes, to include implementing future force capabilities. Doctrine is one of the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) domains that play an important part in the capabilities-based assessment processes. Doctrine fulfills this role by helping to mitigate capability gaps. From one viewpoint, doctrine and training are two of the last bridges between the current state and the final implementation of future force capabilities. This is also a reality because doctrine must have a far more near-term focus—from right now to no more than a few years out.

During the implementation of future force capabilities, doctrine often flows from concepts. Concepts are ideas for a significant change based on proposed new approaches to the conduct of operations or introduction of new technology. These concepts become part of the U.S. Army's institutional process for incorporating change into operations. These ideas propose significantly different methods that the force might eventually use, usually 5 to 15 years in the future. The Army experiments with, and modifies or validates, these concepts, and ultimately the validated concepts result in DOTMLPF-P solutions.[1]

However, there are far more inputs to doctrinal changes than just concepts and other DOTMLPF-P solutions. Changes to law and policy; changes to allied, joint, and other Army doctrine; senior leadership guidance; lessons learned; and input from the field can all drive doctrinal changes. The U.S. Army Intelligence Center of Excellence (USAICoE) considers many different inputs when deciding what doctrinal changes are necessary and how and when to implement those changes.

So What Is Doctrine?

The textbook answer is, "*Army doctrine* [is the] fundamental principles, with supporting tactics, techniques, procedures, and terms and symbols, used for the conduct of operations and which the operating force, and elements of the institutional Army that directly support operations, guide their actions in support of national objectives. It is authoritative but requires judgment in application. Army doctrine is the approved…body of knowledge that is taught and used for the conduct of operations."[2]

Here are some other theoretical aspects of doctrine:

- Doctrine reflects a unique body of professional knowledge and establishes a professional vocabulary and philosophical framework for operations.
- Doctrine is dynamic and changing but is not established arbitrarily.
- Doctrine in and of itself is usually descriptive, not prescriptive, although doctrine can capture laws, policies, and regulations or specific procedures that are prescriptive.
- Doctrine discusses capabilities, some systems, and generic unit structures without going into a level of detail that would render doctrine obsolete within a short period of time.
- Doctrine is not intended to replace training material or standard operating procedures, nor is it theater-specific.

To be honest, doctrine reflects the senior leadership's guidance, the writing team's best professional military judgment, the effectiveness of doctrinal process execution, and the participation of organizations and units (other than the writing team) in the doctrine development and review process. The content within these publications is a best attempt to discuss the information needed to support training and answer the needs of the force.

How Do You Come Up With This Stuff?

There are both excellent and poor examples of doctrine. Of the many developmental processes across the Army, the doctrine development process is fairly sound. However, it cannot be overly emphasized that external participation in the development process is absolutely critical.

At USAICoE, we consider all input received when updating or revising military intelligence (MI) publications. We endeavor to work with contributors to ensure we fully understand the intent and justification of their recommended changes. We can then address the concerns within the four phases of the doctrine development process, shown in Figure 1.[3]

- **Phase 1, Assessment.** During the assessment phase, the doctrinal proponent conducts research to determine what doctrine is available on a given subject.

Based on that assessment, the team makes a determination whether there is a doctrinal gap or shortcoming. If there is an issue, the doctrinal proponent decides to start a new publication, revise or change the existing doctrine, or rescind the publication. Not every doctrinal gap necessitates a new publication.

- **Phase 2, Planning.** During the planning phase, the doctrinal proponent conducts further research, develops an outline, and establishes timelines or milestones. The doctrinal proponent decides how to develop the specific publication and starts to build an informal network to assist with subsequent development.
- **Phase 3, Development.** During the development phase, the doctrinal proponent forms the writing team and the team drafts the publication. The proponent staffs the publication Armywide at least once for comment, and the writing team adjudicates all comments received. Throughout this process, we address those concerns using the comment resolution matrix. The last steps in this phase are approval of the final draft and submission of the document for publishing.
- **Phase 4, Publishing and Implementation.** During this final phase, the official documentation is signed and sent to the Army Publishing Directorate (APD) for authentication. Once APD authenticates the publication, they post it to the online doctrinal library on the APD website at http://www.apd.army.mil/. At this point, the publication is official doctrine for use by trainers and the operational force. Current authenticated MI doctrine is also available at https://ikn.army.mil/apps/IKNWMS/Home/WebSite/Doctrine.

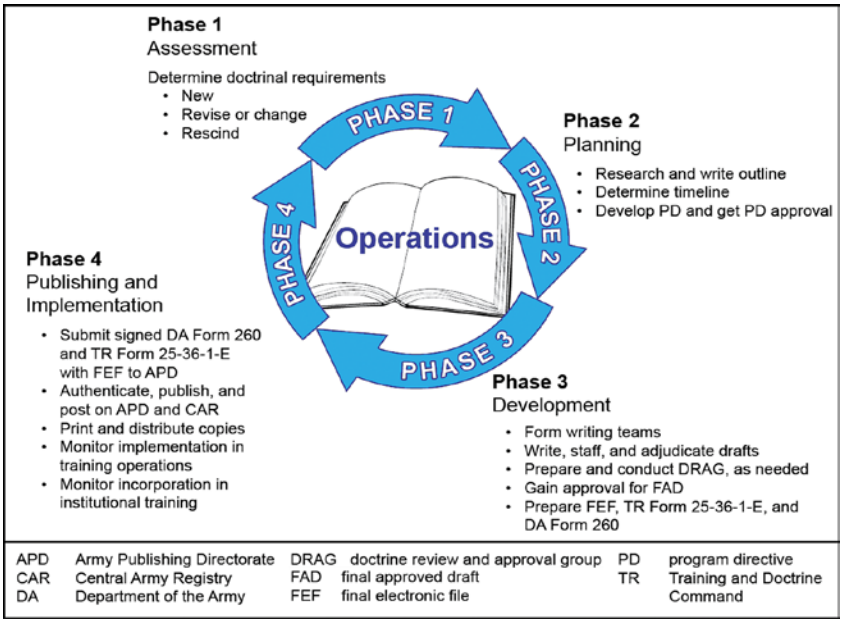


Figure 1. Army Doctine Development Process.[4]

What about Army Intelligence Doctrine?

At USAICoE, the Doctrine Directorate is responsible for all Army MI doctrine. We have some unique challenges in producing Army MI doctrine. One of those challenges is the diversity of technical capabilities across the intelligence warfighting function. However, we also have some advantages over most other Army doctrinal proponents. The most notable is the size of USAICoE's Doctrine Directorate, which helps offset the challenge of the diverse capabilities.

The Doctrine 2015 initiative set a new baseline for Army doctrinal publications. By completing the initiative, we have restructured Army doctrine so that the doctrine hierarchy of publications is smaller and more focused. The Doctrine 2015 construct consists of four levels of publications:

- **Army doctrine publications (ADPs).** The ADPs contain the fundamental principles by which the operating forces and elements directly support operations and guide their actions in support of national objectives. These publications are normally around 10 pages.
- **Army doctrine reference publications (ADRPs).** These publications provide a more detailed explanation of the principles contained in the ADPs.
- **Field manuals (FMs).** FMs contain principles, tactics, procedures, and other doctrinal information that describe how the Army trains and conducts operations.
- **Army technique publications (ATPs).** These publications contain techniques for task, mission, and operations execution. ATPs make up the bulk of MI doctrine.
- **Military intelligence publications (MIPs).** Not technically doctrinal publications, MIPs are useful for Army MI professionals. We often use MIPs for emerging topics or for providing a greater level of specificity than that allowed within doctrine. For example, MIP 2-01.2 *Intelligence Architecture*, provides guidance for planning, preparing, and deploying the intelligence architecture.

Since December 2015, we continue to change MI doctrine based on operational lessons learned; new threat doctrine; and new doctrinal concepts for multi-domain battle, large-scale ground combat operations, new battlefield frameworks, and peer/near-peer threats expressed in FM 3-0, *Operations*. As part of the effort to maintain relevant doctrine, we are reviewing and updating the MI doctrinal library more frequently to address critical and major shortcomings. By increasing the frequency of doctrinal updates, we will reduce

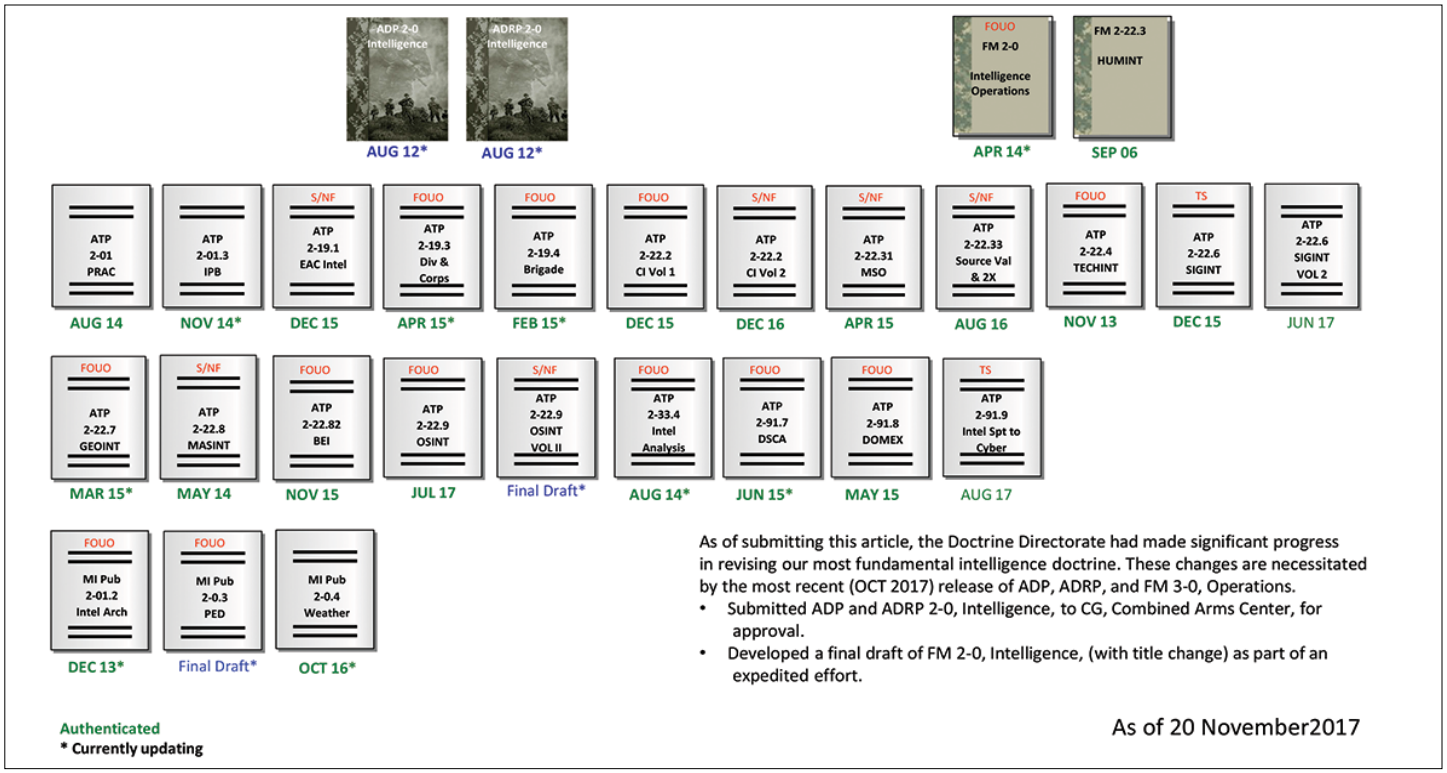


Figure 2. Military Intelligence Doctrinal Library.

the need to conduct time-consuming full revisions of those publications. Figure 2 shows the current MI doctrinal library and the status of MI doctrine.

So What Is My Role?

Army MI doctrine is your doctrine, so participate in its development! Periodically contact us and talk to us. We can give you updates on the status of MI doctrine and tell you about new efforts that are underway. We rely heavily on input from the Army at large. The most direct way to influence doctrine during the development process is to review draft doctrine during staffing to the Army and to submit clearly stated comments, with justification, in the provided comment resolution matrix. USAICoE doctrine reviews all comments carefully and works with commenters to ensure we fully understand their input and agree on solutions. A second way to affect doctrine is to let us know if you see any issues in the current approved doctrine. If you do, contact us through the USAICoE Doctrine Directorate email at usarmy.huachuca.icoe.mbx.doctrine@mail.mil. We check this email frequently, and any input submitted we give to an action officer who specializes in the particular subject area. You can also affect doctrine by participating when the USAICoE Lessons Learned teams come to talk to your unit. The Lessons Learned teams work closely with the Doctrine Directorate by communicating responses from the field and collecting best practices, which can ultimately drive a doctrinal change.

Endnotes

1. U.S. Army Doctrine Publication 1-01, *Doctrine Primer* (Washington, DC: U.S. Government Publishing Office [GPO], 2 September 2014), 2-6.

2. Ibid., 1-2.

3. U.S. Army Training and Doctrine Command (TRADOC) Regulation 25-36, *The TRADOC Doctrine Publication Program* (Fort Eustis, VA: TRADOC, 21 May 2014), 25.

4. Ibid.

Mr. Craig Sieting is the U.S. Army Intelligence Center of Excellence Doctrine Directorate Writing Branch Chief. He served 21 years in the U.S. Army as a Human Intelligence Collection Technician and retired at the rank of chief warrant officer 4. His active duty deployments include Haiti, Bosnia, Somalia, Iraq, and Afghanistan.

by Chief Warrant Officer 4 Cerida Browning

Introduction

In order to support effective training of the future force, the U.S. Army Training and Doctrine Command (TRADOC) recently combined the Army Learning Concept and the Army Training Concept into one document—TRADOC Pamphlet (PAM) 525-8-2, *The U.S. Army Learning Concept for Training and Education 2020-2040*. The audience for this pamphlet is Army leaders and Department of the Army Civilians who are in a position to make decisions regarding learning within the training domains (operational, self-development, and institutional). The pamphlet defines learning management as broader than just what occurs at the institutional level by emphasizing a shared responsibility between the learner, the education training enterprise, and the chain of command. Furthermore, it defines specific roles in the continuous learning model for officers, warrant officers, noncommissioned officers, and Army Civilians.

TRADOC PAM 525-8-2 has a direct influence on the development of training materials at the U.S. Army Intelligence Center of Excellence (USAICoE). For the Military Intelligence (MI) Corps, USAICoE at Fort Huachuca, Arizona, is the Army's school for professional MI training that provides the basic (initial military training) and advanced (professional military education) skills needed to effectively operate in complex, ambiguous, and multi-domain operational environments. Entry-level Soldiers arrive at USAICoE to attend initial military training in their respective military occupational specialties (MOSs). They will receive the education and training that will give them the baseline knowledge expected of all MI professionals. Course instructors, managers, and designers focus on the observable, measurable pattern of skills, knowledge, abilities, and other characteristics that individuals need to perform work roles or occupational functions successfully—in other words, the competencies. TRADOC PAM 525-8-2 divides competencies into technical (i.e., job tasks) and non-technical (i.e., soft skills such as leadership and social cognition). The Analysis, Design, Development, Implementation, and Evaluation (ADDIE) process provides the Army with guidelines to develop training courses designated to graduate Soldiers and leaders that are MOS qualified. USAICoE courses produce agile, critical, and creative thinkers capable of accomplishing all assigned missions and required duties across the full range of military operations while exhibiting the leadership competencies the Army requires.

The Analysis, Design, Development, Implementation, and Evaluation Process

The ADDIE process is the Army's instructional design framework used by training developers to build a variety of learning products that together form a course's program of instruction. The process involves five interconnected phases: analysis, design, development, implementation, and evaluation. While there can be many triggers to revise a course, the ADDIE process most often begins in conjunction with an MOS or area of concentration's critical task site selection board. Subject matter experts (SMEs) conduct a job analysis to identify critical tasks Soldiers must complete to successfully accomplish the associated missions and duties. From that they develop a critical task list. Once complete, the critical task list provides the performance steps, performance measures, and resources needed by Soldiers to perform the tasks.

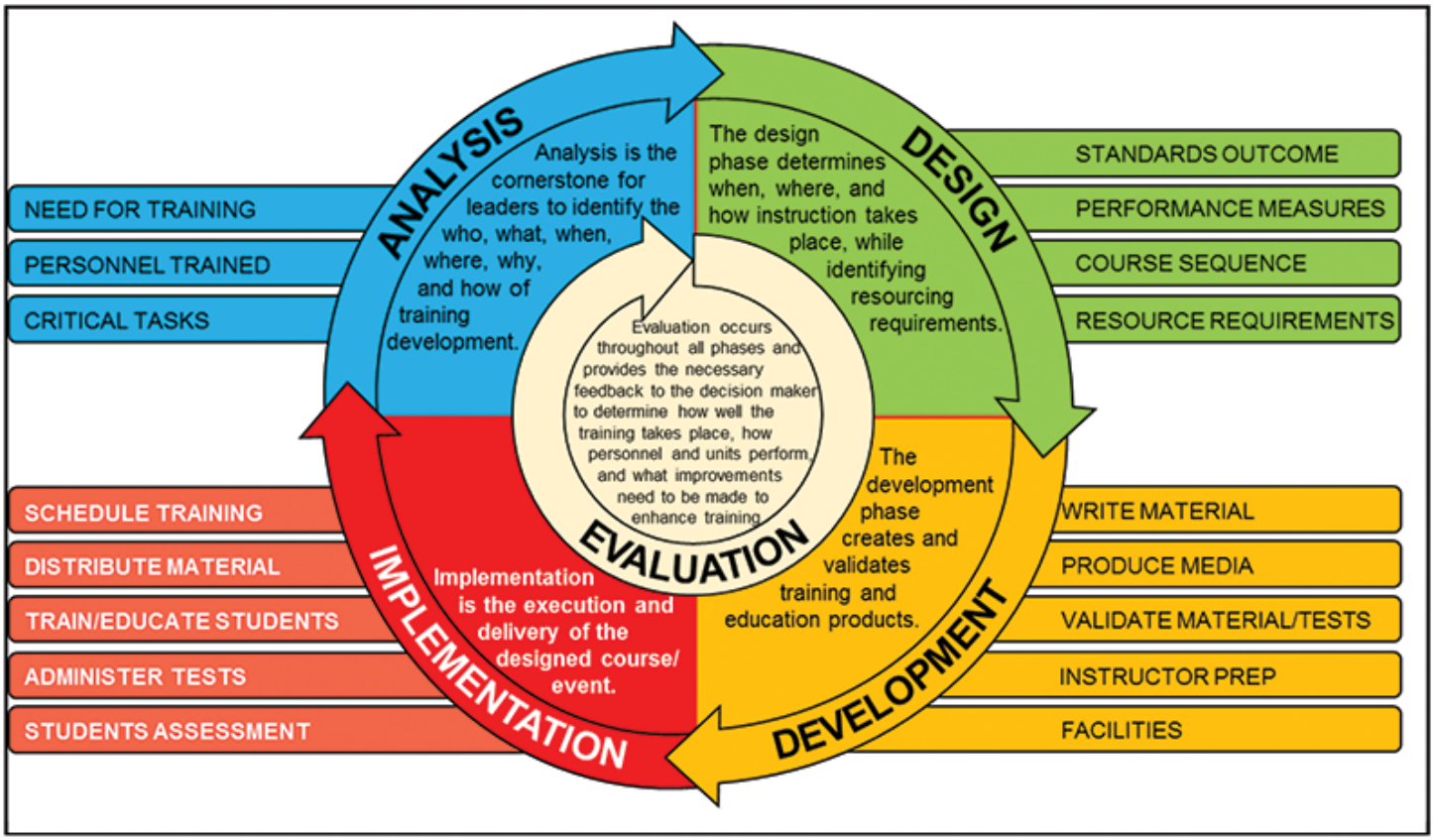
Internal to USAICoE's ADDIE process was the creation of discipline technical advisors (DTAs) to provide overall management of the ADDIE process. The DTAs facilitate communication between, and serve as the principal advisors to, USAICoE senior leadership and the training organizations regarding MOS curriculums (officer and enlisted). The DTAs, who are normally senior officers and warrant officers, ensure both technical and non-technical competencies are progressive across their respective discipline from entry-level training through the Noncommissioned Officer Academy courses and the warrant officer branch. Monthly integrated development team forums, which the DTAs lead and coordinate, enhance the coordination and collaboration between various USAICoE elements, make the best use of USAICoE resources, and ensure effective training for each discipline.

In the ADDIE process, just as in the military decision-making process (MDMP), each step begins with specific inputs that act as building blocks to learning outcomes, and each step has outputs that drive subsequent steps. Any omissions or shortcuts early in the process will affect later steps. However, unlike the MDMP, the analyst design team (ADT) may complete the ADDIE process in a non-linear sequence by working multiple avenues concurrently.

Analysis Phase: The What. In the analysis phase, the ADT identifies what will be included in the training. It is the brainstorming and coordination/communication phase. It is in the analysis phase that the ADT identifies and scopes training gaps. Information on gaps can come from field surveys, lessons learned, and combat training centers. Recommendations from SMEs, leader and instructor interviews, and a document review of current training materials help the ADT identify ways to revise training in order to close identified gaps, always emphasizing the operational need. During this phase, the ADT considers potential or anticipated changes in the operational environment, doctrine, strategies, concepts, and force structure to ensure all training developed is in accordance with the current and future military environment.

Design Phase: The How. During the design phase, instructional designers work with course SMEs to focus on the how. The appropriate method of instruction and evaluation methods for measuring student comprehension of skill level tasks are deliverables for this phase. Design outputs include objectives, assessments, lesson plan outlines, personnel requirements, and time and technology resources needed for the course. This phase is important because discussions will help ADT participants identify resource requirements for senior leadership consideration. Because of the Department of Defense's program objectives memorandum resource allocation decisions (i.e., programmed needs for 5 years), short-notice course-support requests are more difficult to fund. For example, it is sometimes difficult to forecast officer and enlisted training requirements identified by the operational force, the Department of the Army, TRADOC, and other senior leaders 5 years out.

Development Phase: The Material. The development phase expands on the products of the design phase by producing the material of training. In this phase, the training unit adds specificity and depth to the design documents by writing assessment questions, developing complete lesson plans, and creating multimedia to support the lessons. The primary goal of development is to produce learning products ready for implementation and use, develop evaluation tools, and validate assessment instruments and instructional materials.



The ADDIE process for learning product development.[1]

Implementation Phase: To Teach. In the implementation phase, instructors teach the materials produced. The ADDIE process does not stop with implementation. The ADT monitors implementation; continuously assessing ways to make the courseware more effective and efficient in order to achieve the best student outcomes.

Evaluation Phase: Quality Control. The evaluation phase is the quality control tool; the systematic and continuous process to determine the quality, effectiveness, and efficiency of newly developed/updated learning materials and testing. Evaluation is not the last step, but occurs throughout the entire process. It ensures the Soldiers will receive the training required to demonstrate proficiency and expertise and meet the force requirements.

Conclusion

The Army designs a future force by arming Soldiers with the skills, knowledge, and abilities crucial for military operations in the complex environment of the 21st century and beyond. MI professionals must develop and maintain several analytical competencies to be successful in their MOS and respective skill level against unpredictable enemies operating in complex and ambiguous multi-domain environments. The training received from USAICoE courses affects the development and retention of key analytic competencies and, in turn, MOS proficiency, and mission accomplishment. Designing the future force without meeting the training needs of today's Army leaders, Soldiers, and Department of the Army Civilians may lead to operational force requirements going unfilled. The Army Learning Concept for Training and Education lays the foundation for developing the force and establishes a shared responsibility between the operational and institutional Army. Focusing USAICoE training on the technical and non-technical competencies identified by the critical task site selection boards using the ADDIE process ensures effective, efficient training and education, and certifies all MI professionals are able to complete their missions.

Endnote

1. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-8-2, *The U.S. Army Learning Concept for Training and Education 2020-2040* (Washington, DC: Government Publishing Office [GPO], 13 April 2017), 14.

References

"ADDIE Model." *Training Industry*. June 26, 2013. https://www.trainingindustry.com/wiki/entries/addie-model.aspx.

Castagnolo, Chuck. "The ADDIE Model: Why Use It?" *The eLearning Site*. 1 March 2011. http://theelearningsite.com/2011/03/the-addie-model-why-use-it/.

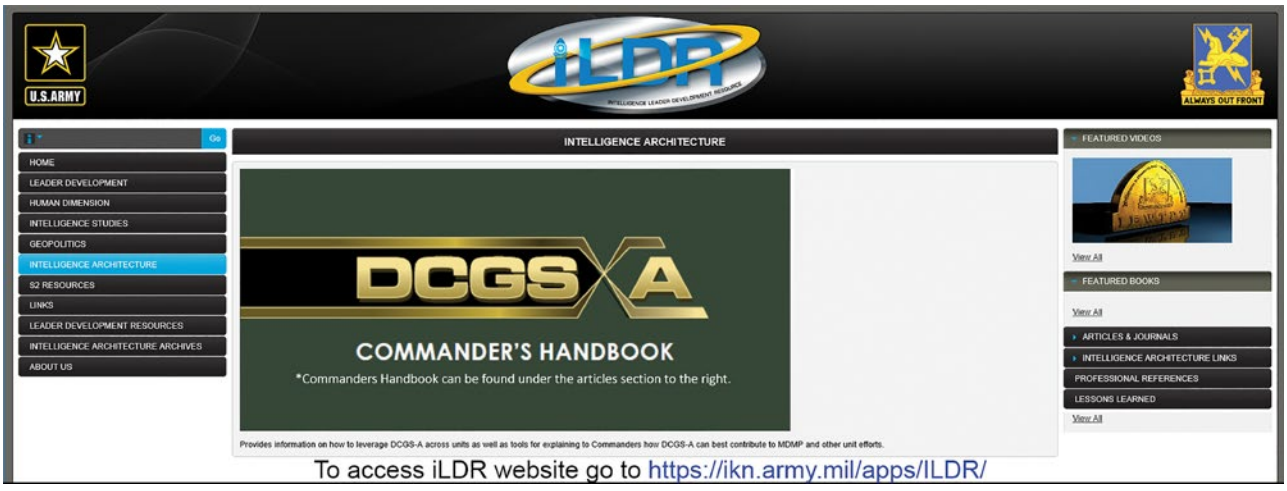
Clark, Donald. "ADDIE Timeline." *Big Dog & Little Dog's Performance Juxtaposition*. Last modified September 6, 2015. http://www.nwlink.com/~donclark/history_isd/addie.html.

Leeder, Beth A. "United States Army Center of Excellence Regulation 350-70 Training Development System." Information Paper, 2 August 2017.

U.S. Army. ATP 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*. Washington, DC: GPO, 26 March 2015.

U.S. Army. TRADOC Regulation 350-70, *Army Learning Policy and Systems*. Fort Eustis, VA: TRADOC, 10 July 2017.

CW4 Cerida Browning has served in a multitude of intelligence positions throughout her more than 17-year career from tactical through strategic. Previous assignments include 305th Military Intelligence Battalion, 35F10 Committee; U.S. Army Africa G-2; Joint Intelligence Center, Central Command Iraq Team; 25th Infantry Division G-2; and 25th Infantry Division, 3rd Infantry Brigade Combat Team S-2 team. She holds a bachelor of arts in economics from Kean University. She is currently the All-Source Discipline Technical Advisor at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ.



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

OCMI's Role in Personnel Life-Cycle Management

by Sergeant First Class Clinton Van Winkle

Introduction

As the personnel proponent for U.S. Army military intelligence (MI), the Office of the Chief, Military Intelligence (OCMI) executes the *personnel* process functions relative to DOTMLPF-P[1] for Career Management Field (CMF) 35 (MI Branch) and Functional Area (FA) 34 (Strategic Intelligence) in support of MI proponent force modernization and the Commanding General, U.S. Army Intelligence Center of Excellence. OCMI safeguards the life cycle of MI personnel by—

- Evaluating data.
- Identifying issues.
- Developing initiatives.
- Formulating alternatives.
- Validating impacts concerning—
  - Standards of grade.
  - Mission support.
  - Zero sum gain.
  - Bill payers.

As force structure and personnel policies change, OCMI ensures the MI Branch remains healthy with respect to accessions, promotions, retention, and career management. When policies change, OCMI revises the affected Department of the Army Pamphlets (DA PAMs). These include:

- **DA PAM 600-3, *Officer Professional Development and Career Management.*** This pamphlet outlines officer development and career management programs for each of the Army's career branches and functional areas. It describes the full spectrum of developmental opportunities an officer can expect throughout a career.
- **DA PAM 600-25, *U.S. Army Noncommissioned Officer Professional Development Guide.*** This pamphlet provides guidance on noncommissioned officer professional development programs for each of the Army's military occupational specialties (MOSs).
- **DA PAM 611-21, *Military Occupational Classification and Structure.*** This pamphlet gives procedures and prescribes the method of developing, changing, and controlling officer, warrant officer, and enlisted military occupational classification structure.

There are also electronic, web-based copies for DA PAM 600-3 and DA PAM 611-21, known as *Smartbooks.* The Smartbooks are living documents that receive updates/modifications regularly. DA PAM 611-21 "contains information on the classification of individuals by identifiers and classification of positions (duty position title, identifier(s) and grade in requirements and authorization documents)."[2]

Fostering Relationships and Capabilities

OCMI fosters and maintains relationships with the other MI DOTMLPF-P domain process representatives ensuring proper coordination of actions affecting other branches, FAs, or commands, and the two Army components: the active component and the reserve components (consisting of Army Reserve and the Army National Guard). OCMI ensures these elements receive adequate consideration in each proposal, action, and review. When necessary, personnel development steering committees, comprised of regular Army, National Guard, and Army Reserve members, assist with personnel management and military policy recommendations and changes. Recommendations are submitted through the Commander, Training and Doctrine Command (TRADOC) and are processed by Department of the Army G-1.

OCMI ensures healthy career progression and professional development models by MOS; prepares and submits centralized promotion board guidance and analysis and command slating guidance (COL, LTC, and CSM); and maintains accurate standards of grade that provide supportable grade structure and grading guidance for force structure documents. Every proponent must maintain a healthy relationship with the U.S. Army Human Resources Command (HRC) and Army recruiters (each component) regarding talent management, accessions, and assignment considerations.

OCMI reviews and updates MOS prerequisites in accordance with AR 611-1, *Military Occupational Classification Structure Development and Implementation*, every 3 years and submits branch and functional area qualifications for

initial entry and professional development through TRADOC to the Department of the Army G-1. When applicable, OCMI reviews requests for exceptions to proponent MOS prerequisites and may grant exceptions to policy. Submission of military occupational classification and structure (MOCS) revisions can also result from analysis of each CMF and MOS review. When OCMI personnel identify the need for a MOCS revision, they develop a proposal and submit it through TRADOC. A MOCS proposal is any change or directive that provides the Army a means of managing personnel requirements, authorizations, and training in manning documents. The proposal must identify the issue(s), recommend a solution, and validate any impacts the proposal has throughout the DOTMLPF-P domains for each component. MOCS revisions can include any additions, deletions, or modifications to—

- MOS.
- Area of concentration.
- Additional skill identifier.
- Skill identifier.
- Special qualification identifier.
- Personnel development skill identifier.

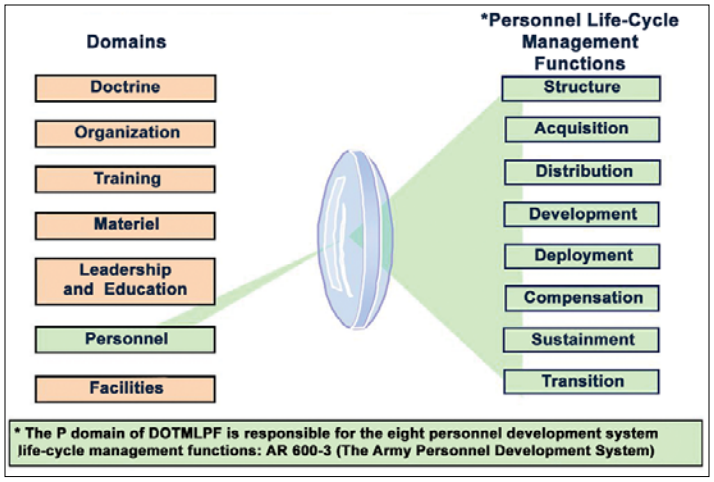
Some of the reasons for MOCS actions are:

- Changes in doctrine, organization, and/or mission.
- New, improved, or obsolete equipment systems.
- Changes in personnel acquisition or training strategies.
- Resolutions or improvements to the management of personnel assets.
- Initiatives directed to improve basic force structure.

Life-Cycle Management Functions

Former President Harry S. Truman once said, *"Men make history and not the other way around. In periods where there is no leadership, society stands still. Progress occurs when courageous, skillful leaders seize the opportunity to change things for the better."*[3] With this in mind, OCMI personnel remain focused on Army 2020 and beyond for changes, while maintaining proper alignment of the eight personnel development system life-cycle management functions. These functions outlined in AR 600-3, *The Army Personnel Development System*, are:

- Structure.
- Acquisition.
- Distribution.
- Development.
- Deployment.
- Compensation.
- Sustainment.
- Transition.[4]



Personnel Development.

Structure. Structure describes the personnel developer dimension of the Army's force development function. Force development defines military capabilities and creates force structure required to provide those capabilities, which then produces the personnel authorizations for each of the Army's units.[5] The structure function is used in concert with both the *Acquisition* and *Distribution* functions. Among many other tasks associated with force structure, OCMI analyzes and makes recommendations regarding—

- Individual positions in the Force Management System for interchangeability coding and additional identifiers.
- Tables of organization and equipment (TOEs).
- Tables of distribution and allowances (TDAs).
- Mobilization tables of distribution and allowances.
- Development of core documents.
- Standardization of job descriptions.
- Performance of standards.
- Establishment of career progression.
- Alignment of career fields or functional categories.

Standards of grade tables are the basis for grading positions in requirement (TOE) and authorization documents (Modified TOE/TDA) that identify appropriate grading and standard duty titles for military positions (officer, warrant, and enlisted). Standards of grade tables do not authorize positions, but provide a basis for determining equitable grades for positions after the number of positions and MOSs is identified. OCMI has the responsibility to manage the provisions in the standards of grade tables and take action to correct errors or deficiencies. Standards of grade tables create a sustainable grade structure that supports

development of skills corresponding to grade levels through experience and training, which supports the overall MOCS and Army Personnel Management systems.

Acquisition. Acquisition is the personnel developer dimension that manages the "total Army end-strength."[6] The acquisition function ensures proper staffing of Army units with the appropriate number of personnel in the correct grades and skills, within the Army's manpower budget, to meet requirements.

There are three important and interrelated dimensions within the acquisition function:

- **Manpower management dimension** "develops forecasts and establishes manpower targets" used for the second dimension.[7]
- **Accession, attrition, and retention management dimension** "converts the accession and retention targets to missions and ensures that they are effectively executed by the responsible agency."[8]
- **Training integration dimension** "establishes training programs and ensures an efficient flow of trainees and students."[9]

OCMI works closely with HRC, U.S. Army Recruiting Command, and U.S. Army Cadet Command to establish accession and retention strategies and criteria for all officers, warrant officers, and enlisted personnel within the MI Branch CMF.

Distribution. Distribution is the function of allotting personnel to units based on Army requirements according to Headquarters, Department of the Army priorities. This includes newly trained Soldiers and Soldiers ready for new assignment. Personnel are alloted in order to maximize readiness and support the development of Soldiers.[10] OCMI supports the distribution function by evaluating the current inventory of MI personnel and recommending adjustments that support both current authorizations and future force structure changes. As the need arises, OCMI recommends changes to HRC regarding the distribution or redistribution of personnel. OCMI utilizes three tools to determine appropriate personnel distribution:

- **Average Grade Distribution Matrix** prescribes the ideal structure by MOS, ensures sustainable career progression, and supports a reasonable promotion structure for each MOS that neither stagnates nor promotes eligible personnel.
- **Grade Cap Distribution Matrix** (GCDM) determines the maximum allowable grade structure for a CMF or designated MOS group for the Active Component. The GCDM allows flexibility but must not exceed aggregate CMF grade structure (plus or minus 5 percent).
- **Personnel Management Authorization Document** (PMAD) is the Army G-1's primary personnel planning structure document that captures force structure within constraints of law and policy. It identifies all military positions within the Army by MOS and grade for Active Component and U.S. Army Reserve Component. The PMAD is based on the Army Authorization Documents System and Master Force, which affects recruiting, retention, promotions, assignments, and school forecasts.

Development. Development is the "process of developing people mentally, morally, and physically…[including] both character and leadership development, education, and training."[11] OCMI develops, reviews, and maintains professional development models for each MOS to advise Soldiers and supervisors on a path for continued career progression, including organizational assignments, institutional training, and lifelong learning through civilian education. OCMI provides recommendations for the Army Educational Requirements System and Training with Industry positions, and approves course prerequisites and selection criteria for technical MOS-producing courses. OCMI provides presentations for centralized enlisted selection boards to assist board members in evaluating candidates for promotion.

Deployment. Deployment is any "movement of troops, civilians, cargo, weapon systems, or a combination of these elements to a theater of operations using any or all types of transport."[12] As personnel developers, OCMI provides recommendations for mobilization planning and management and assists in the evaluation of the effects of mobilization on the personnel development system.[13]

Compensation. Compensation is associated with all of the functions involving Soldier pay, entitlements, and benefits. OCMI develops concepts for the use of compensation and benefits to improve the health of the MI Branch, and recommends changes to Civilian compensation policies.[14]

Sustainment. Sustainment focuses on the "quality of life and the well-being of Soldiers, Civilians, retirees, their Families, and the employers of RC members."[15] At all times, OCMI "represents the professional interest of members" and maintains communication with the force on new and upcoming changes in personnel management, systems, and programs affecting the CMF.[16]

Transition. Transition is an "integrated function focused on assisting Soldiers, Army Civilians, and their families through changes associated with moving among components and/or to the private sector."[17] When necessary, OCMI

recommends shortages within the MI Branch and FA 34 as an exception to separation policy. OCMI recommends changes to analyze impacts of retirement, retention, force reduction, service obligation policies, credentials, and the Personnel Transition Management Program.[18]

Conclusion

OCMI affects the career of every officer, warrant officer, and enlisted Solider within the MI Branch through the various missions and responsibilities entrusted to them as the MI personnel proponency office. For additional information about OCMI, its missions, and contact information, please visit our webpage on Intelligence Knowledge Network at https://ikn.army.mil/apps/IKNWMS/IKN_Websites/USAICoE/OCMI/ocmi_homepage.htm (CAC required).

Endnotes

1. DOTMLPF-P is an acronym used by the Department of Defense in the Joint Capabilities and Integration Development System process. It stands for doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

2. Department of the Army Pamphlet 611-21, *Military Occupational Classification and Structure* (Washington DC: Government Publishing Office [GPO], 2016), 1. https://www.milsuite.mil/book/groups/smartbookdapam611-21 (CAC required).

3. Gerald Boerner, "On this Day in History…July 17th: Truman, 'The Buck Stops Here!'," *Prof. Boerner's Explorations* (blog), July 17, 2010, http://www.boerner.net/jboerner/?p=13466.

4. Department of the Army Regulation 600-3, *The Army Personnel Development System* (Washington DC: GPO, 2009), 8-10, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/r600_3.pdf.

5. Ibid., 8.

6. Ibid.

7. Ibid., 9.

8. Ibid.

9. Ibid.

10. Ibid.

11. Ibid.

12. Ibid.

13. Ibid., 10.

14. Ibid.

15. Ibid.

16. Ibid.

17. Ibid.

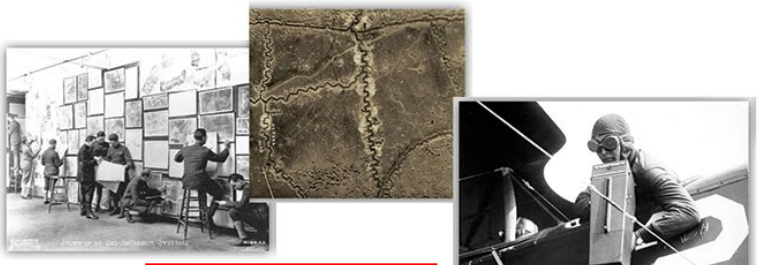
18. Ibid.

SFC Clinton Van Winkle was assigned to the U.S. Army Intelligence Center of Excellence in 2015 as the noncommissioned officer in charge and senior instructor/writer for Phase II for the 35G Geospatial Intelligence (GEOINT) Imagery Analyst Advanced Individual Training. In March 2017, SFC Van Winkle became the 35G Life-Cycle Manager, Office of the Chief, Military Intelligence. He attended the Personnel Proponency Course in June 2017. Previous assignments include 3/82nd Airborne Division at Fort Bragg, NC; 138th MI Company at Warner Robins Air Force Base,GA; and 1-10th Special Forces Group(A) in Stuttgart, Germany. SFC Van Winkle enlisted as a 96H, Common Ground Station operator, and later became an Airborne Target Surveillance Supervisor aboard the Joint Surveillance Targeting and Attack Radar System. When his military occupation specialty merged with GEOINT, he attended the Imagery Analyst Transition Course at Fort Huachuca, AZ, in 2011.

MI History Trivia

On 15 April 1918, Major Ralph Royce made the first American photo reconnaissance flight over enemy territory. How many aerial photographs were taken and reportedly used for intelligence purposes by the U.S. Army during World War I?

A. 13
B. 1,300
C. 130,000
D. 1.3 Million between 1 July and 11 November 1918



From question on page 16.
*Correct answer in **RED***

Maj. Ralph Royce (later Maj. Gen.) is also credited with being the first American Army pilot to fly an airplane in combat.

Doctrine for Tomorrow:

Targeting the Army's Millennial Leadership

by Chief Warrant Officer 2 Tony Hoffman and Chief Warrant Officer 2 John Mark Penfield, Jr.

The views and opinions expressed in this article are those of the authors and do not reflect any official policy or position of the Asymmetric Warfare Group, U.S. Army Training and Doctrine Command, or the United States Army.

Introduction

Commanders frequently ask tough, complex questions of military intelligence (MI) leaders concerning enemy disposition, strength, or intelligence training. Answers and assessments come from an understanding of models and processes used to develop useful intelligence estimates or training strategies, which are explained in various doctrine and training manuals. These documents are the ultimate resource for all echelons of leadership. As warfare challenges have become more complex, the Army and MI Corps have updated existing doctrine or have developed entirely new doctrine to address these evolving challenges. However, the Army and MI Corps have not changed the presentation or delivery methods to keep pace with generational learning styles—in this case, the learning style of the millennials, who are now the Army's junior leaders.

The Millennial Factor

The ranks of junior leaders typically range from sergeant to staff sergeant, and from first lieutenant to captain. They are usually between 18 and 27 years old and belong to the largest demographic of the American workforce—millennials, also known as Generation Y.[1] To put this in perspective, one in three American workers is a millennial.

Today, more than 20 doctrinal publications exist for MI, which require an inordinate amount of time to download and sift through. Research time is limited at the tactical level because it competes with multiple requirements from the brigade, battalion, company, and platoon training calendars. As an example, ATP 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*, provides guidance for one of the foundational analytic processes for Soldiers in the field or in a deployed environment. It is over 200 pages in length.

Commands task junior leaders with training Soldiers to maintain their section's proficiency in intelligence preparation of the battlefield (IPB) among other associated duties. These junior leaders generally have less than a month to prepare the training, and they have a limited amount of common access card (CAC)-enabled computer time at the company/platoon level for research and preparation. The primary methods of providing digital training manuals and handbooks to these junior leaders require an update to correspond with how millennials review, process, and retain information.

Update the Presentation and Delivery Method

The Army produces, formats, and disseminates doctrine in the same manner as it did 40 years ago, albeit digitally. Every doctrinal publication contains tens of pages that define the relevant Army jargon, explain why the document is needed, and provide instructions to the reader, along with additional text that conveys changes, administrative remarks, tables of contents, roles and responsibilities, etc.

How can we expect MI professionals to understand the operational environment in 2030 and beyond, while training them with outdated structure and delivery? Our current publication structure assumes a target audience that reads at length. The number of Army leaders who find this format and delivery of information useful is decreasing rapidly. Very few junior Army leaders use these types of references; the reality is, most of them use Google or Bing to find their answers, relying on the results to be accurate, and then sometimes verifying the information in the doctrinal publications.

Besides the endless burden of tasks the Army places on tactical leaders, leaders of this generation do not appreciate information provided through traditional learning models; they believe context is more important than content.[2] They can apply concepts across a broad range of challenges with efficiency, and they have the critical-thinking skills a commander desires from them; however, doctrine provides content, not context. In the age of social media, millennials turn to Facebook, Amazon, and other online sources, rather than to CNN, Fox News, or traditional local libraries.

Millennial MI leaders are not going to spend the little spare time they have digging through traditional doctrinal documents, even though these leaders are motivated to learn and interested in seeking novel answers to difficult problems that doctrine may provide.[3]

Millennials view the absence of interactive technology as outdated, even primitive; printed or digital doctrine does not allow them to interact with concepts and information, forcing them to become passive learners. Junior MI leaders have used the internet and rapidly developing technology for most of their lives and they quickly obtain information from their computer or smartphone. Mobile applications, videos, and collaborative learning are key to teaching junior leaders the concepts that commanders will expect them to apply to complex problems.

Junior leaders saw the disappearance of phone booths and welcomed smartphones; they stopped using library card catalogs and started relying on Google and Wikipedia for quick, easy-to-access answers. Now they keep pace with the latest gadgets and online information resources. Their increased reliance on technology has resulted in a generation that expects to engage with their surroundings in an interactive, game-like environment.[4] Their learning experiences, much like video games, are trial and error, demonstrating to them that mistakes and learning from them is the fastest way to mastering a game because mistakes present a hands-on opportunity to learn. Tasks that require synthesis, application analysis, reasoning, interpretation, and complex thinking and processing engage junior leaders in deeper learning and enhance critical-thinking skills.[5]

As the Army embraced the return of sergeants' time training to tactical formations, some units began to develop a balance between the requirements of training tactical tasks, such as warrior tasks and battle drills, and military occupational specialty-specific skills, such as IPB and interrogation. Leaders also re-introduced hip-pocket training, which noncommissioned officers could perform with little preparation or equipment to teach a capability or correct a deficiency. Hip-pocket, or opportunity, training evolved from the Soldier's Manual of Common Tasks that leaders could carry in their cargo (hip) pocket and use as an efficient reference tool. New training methods like the Army intelligence training strategy and MI gunnery are quickly becoming institutional support documents to assist junior leaders in communicating a training need to their combat arms commanders. In addition, they help provide a strategy for a capable and ready MI force for Combat Training Center rotations, regionally aligned force missions, and deployments. The critical question is, How many junior MI leaders (at the brigade combat team and MI company level) have access to these strategies or even know they exist? Often at the tactical level, CAC-enabled computer access is limited to platoon sergeants, platoon leaders, noncommissioned officers in charge, and officers in charge. However, junior leaders do have access to their smartphones most of the time.

U.S. Army Photo

The Army is rolling out a gaming system, Operation Overmatch, that Soldiers can use to test virtual versions of gear and operation concepts that could be implemented in the future.

Junior leaders must train their subordinates to improve their foundational MI skills. Similar to the hip-pocket training example, junior leaders still expect a mobile tool to enable opportunity training. The MI Corps should endeavor to deliver this product in a secure, mobile application. The mobile app should be easy to access and include video and Graphics Interchange Format examples. Of course, the new technology will enhance our training environments, but it will never replace traditional, formal training.[6]

Conclusion

In the next 20 years, the millennial junior leaders of today will become the Army's senior leaders of tomorrow. We need to get them thinking about "doctrine for tomorrow" by involving them in updating the current training methods and delivery. The benefit of their involvement is twofold: They will know how to make these applications more innovative than we could ever imagine, and it will prepare them for the learning environment challenges they will ultimately face—training junior leaders of the next generation, Generation Z.

Endnotes

1. Richard Fry, "Millennials Surpass Gen Xers as the Largest Generation in U.S. Labor Force," Fact Tank News in the Numbers, *Pew Research Center*, May 11, 2015, http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/.

2. Akanksha Sharma, "Designing Learning for Millennials," *Talent Development*, Association for Talent Development, June 2016, 60-65, https://www.td.org/Publications/Magazines/TD/TD-Archive/2016/06/Designing-Learning-for-Millennials.

3. David H. Roberts, Lori R. Newman, and Richard M. Schwartzstein, "Twelve Tips for Facilitating Millennials' Learning," *Medical Teacher*, 2012, 274-278, doi: 10.3109/0142159X.2011.613498.

4. Ibid.

5. Ibid.

6. Ibid.

CW2 Tony Hoffman is an all-source intelligence technician assigned to the Asymmetric Warfare Group in Fort Meade, MD. He has served at company, battalion, brigade, and combatant command echelons, including deployments to Iraq and Afghanistan. He is pursuing a bachelor's degree from American Military University, majoring in international relations with a concentration in African studies.

CW2 John Mark Penfield, Jr., serves as the operational management team chief for 1st Brigade Combat Team, 101st Airborne Division (Air Assault) at Fort Campbell, KY. He has had three deployments to Iraq and one deployment to Afghanistan. His previous assignments include the Asymmetric Warfare Group, 173rd Infantry Brigade Combat Team (Airborne), 4th Military Information Support Group, 504th Battlefield Surveillance Brigade, and 1st Cavalry Division. He holds an associate of arts in Middle East studies, an associate of applied science in intelligence operations, and a bachelor of science in liberal studies. He is also a graduate of the Modern Standard Arabic course at the Defense Language Institute.

Cyber Ugly Duckling or Cyber Frog Prince(ss)?

by Major Danielle Gonzalez

Today's hostilities are no longer restricted to air, land, and sea. They are also in cyberspace, which is filled with a slew of cyberspace actors who engage in cyberspace espionage and crime, hacktivists, and those who are determined to prove their nation's might through the power of a few keystrokes. Senior leaders at the U.S. Cyber Command (USCYBERCOM), part of the United States' front line in the cyberspace domain, are developing an agile and knowledgeable cyber mission force focused on securing our national interests and defending our cyberspace borders from those who wish to do us harm. In the years since the formation of USCYBERCOM and the creation of the Cyber Mission Force, the U.S. Government has poured money, time, and effort into creating an elite cyber force by recruiting individuals with computer science degrees, experience in computer network exploitation, and beginner level understanding of structured programming.[1] This article seeks to address a consequence of building a cyber force that focuses on technical attributes, and it attempts to highlight the benefits of what a non-technical cyber "ugly duckling" or cyber "frog prince(ss)"[2] can bring to the cyberspace fight. The Army Intelligence Development Program–Cyber (AIDP-C) is a key part to creating a cyber-knowledgeable component within the Army officer corps and is a fantastic opportunity for military intelligence (MI) officers to develop new skills to help fight our future wars.

Like many people in the world today, I decided I wanted a piece of the cyberspace pie. It was 2013, and I was only aware of Cyber with the capital "C." It was the next big thing and, as near as I could tell, my way of staying relevant in modern warfare. I did not have a computer security certificate to my name, had the furthest thing from a computer science degree, and certainly didn't have a server farm buzzing in my basement. However, I had a goal to buy a slice of the cyberspace pie and set out to find a way to bring enough skills and attributes from my MI background to the table to contribute to the cyberspace fight of the future. At the time, I didn't look like a techie, my resume didn't read like a techie's, and I only spoke like a techie on occasion. Nevertheless, I did have some skills that I felt were critical to the future of the cyberspace fight:

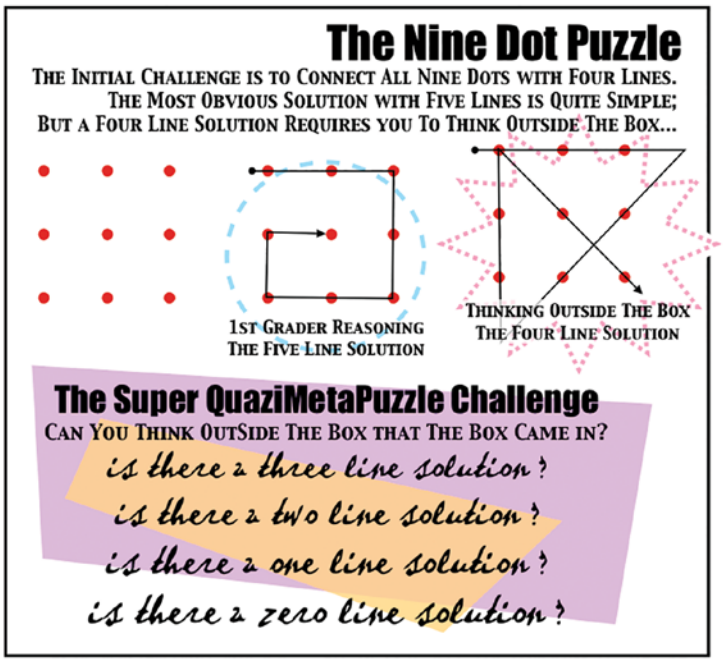
- I am not afraid to ask the stupid question.
- I can sell the product to the customer.
- I know the box is man-made.

These skills, and the experience I gained as an AIDP-C intern from 2014 to 2016, represent what I hope other future Army officers possess as they contribute to our Nation's fight in multiple domains.

Ask the Stupid Question

In October 2014, the U.S. Army Human Resources Command released the first military personnel message requesting applications for Army officers who wished to transfer to the new Cyber (17-series) Branch. Included in the prerequisites for application were the completion of a science, technology, engineering, and mathematics (STEM) degree, completion of industry-standard training, and/or extensive experience within cyberspace work roles. The inclusion of these important skillsets makes sense—to defend against the world's cyberspace actors, the military must include individuals with extensive cyberspace training and experience. As the cyber mission forces continue to develop to meet the Nation's current and future threats, we will need well-trained and combat-ready Soldiers who understand how to operate in the cyberspace domain. However, are these skills all we need?

In the early 1970s, J.P. Guilford was one of the first academic researchers to conduct a study of creativity. Guildford's test required participants to solve a nine-dot puzzle by connecting all the dots, using four straight lines, while never lifting the pencil from the paper. Only 20 percent of the participants could "think outside the box" and solve the puzzle. Unsure of the original results, later researchers conducted a similar study and told half of the participants the "trick" to solve the puzzle. Yet only 25 percent of the participants completed the puzzle, showing that direct and explicit instructions to think outside the box did not help people actually think outside the box.[3]



The results of this creativity study are also applicable to the cyberspace community. The selection criteria to fill the ranks of the Army's Cyber Branch call for Soldiers who have STEM degrees, industry-standard certificates, or extensive real-world cyberspace experience. Once these billets are filled, Soldiers will be required to confront some of the greatest cyberspace challenges facing the United States, from things like the Office of Personnel Management data breach[4] and attacks against the U.S. banking sector.[5] These challenges will require innovative and creative ways to confront the enemy. As Guilford and other researchers have shown, telling someone to "think outside the box" may not be enough to spur creativity, even if the answer is staring them right in the face.

I have always been told there is no such thing as a stupid question. Nevertheless, in a room full of highly trained technical professionals, a question from a less technical person can seem unintelligent, annoying, and unlikely to help solve the problem. Perhaps the solution to a catastrophic cyberspace event can come from an outsider—a cyber ugly duckling or a cyber frog prince(ss). In fact, research conducted at The Wharton School supports this theory. Despite the fact that human resource managers want to hire people with experience in a particular industry, the study found that companies may be better off investing in training fresh recruits in order to have more control over how the new workers adapt.[6] What's more, the research suggests the relationship between prior related experience and performance may not be wholly positive.[7] While not the cyberspace silver bullet, a focus on only a small number of technical attributes to select the Army's cyber force may not always be the best way for the cyber force to confront an ever-evolving threat over time. The cyber force should not only include well-trained technical individuals but also more diverse experts who can provide a fresh perspective about a particular problem and take the organization to the next level.

MI officers with cyberspace training, like those who complete the AIDP-C program, are able to provide a perspective in the cyberspace domain that other officers may not. For starters, MI officers receive training during the Officer Basic Course to be enemy-minded, which includes a large component of creativity and "thinking outside the box." Thinking like one's enemy requires a mix of science and art—science to study the enemy's past behavior, and art to apply a "best guess" of how an enemy may act or react in a given situation. What's more, MI officers have the benefit of experience in consuming and developing multi-source products, providing multiple vantage points of a particular problem that a cyberspace perspective could only augment. MI officers are also known to ask many questions, to challenge assumptions, and to keep digging for more information in order to understand the entire situation. These qualities are exactly what the cyber force needs to successfully characterize and understand malicious cyberspace actors and to build plans to counter these actors in cyberspace. What an MI officer can do on land, in the air, or on the sea, so too can an MI officer do in cyberspace.

Sell the Product

Malcolm Gladwell's 2000 book *The Tipping Point* discusses the phenomenon of the moment in time when an idea, trend, or behavior crosses a threshold and tips, spreading like wildfire.[8] In the book, he describes three kinds of people—the maven, the connector, and the salesman. A salesman has the skills to persuade someone who is unconvinced, and then the salesman becomes critical to "tipping" the idea or the event.

As warfare in the cyberspace domain becomes more prominent and crosses the physical domains of land, air, sea, and space, the Army will more frequently use cyberspace as a means to retain freedom of movement and to accomplish the joint force commander's objectives. The cyber mission force will need people to effectively sell the product to its customers.[9] The cyber force should have the best salesmen to engage their customers—brigade and battalion commanders, industry partners, Department of Defense office leaders, to name a few—and ensure the customer fully understands the capabilities a cyberspace warrior brings to the fight, and how a cyberspace warrior can defend the Department of Defense networks and, if necessary, engage the enemy in cyberspace.

The 780th MI Brigade at Fort Meade, Maryland, is bringing cyberspace support to Corps and below echelons of the Army. As part of the cyberspace mission, Soldiers from the 780th MI Brigade train with brigades and battalions at the National Training Center at Fort Irwin, California. The rationale for this in part is to demonstrate to tactical commanders what cyberspace capabilities can bring to their overall mission and to educate tactical leaders on how to employ cyberspace assets in combat. However, is it enough to be a technical computer warrior to sell cyberspace to a tactical commander?

Photo by Steve Stover

Cyber operations on mission in the 780th Military Intelligence Brigade operations center at Fort Meade, MD.

I submit the answer is no. Those engaging with the customer need to be the best sales people cyberspace has among its ranks. Many consider cyberspace too confusing and too technical, and some may view it as unnecessary to accomplish tactical missions. After all, tactical commanders have been engaged in warfare for the past 16 years in Iraq and Afghanistan, largely fighting the enemy without cyberspace assets. Cyberspace sales people must be able to relate to the tactical commanders, to the infantry Soldiers, and to the staff officers. They must fully understand the customer's mission and best business practices, and they must be able to communicate how to integrate cyberspace capabilities to maximize effectiveness on the battlefield across all domains.

The Harvard Business Review published an article describing the best salesman. The research found that a very high proportion of those engaged in selling could not sell, mainly because two special characteristics are required to be a good salesman—empathy and ego drive. "The salesman's empathy, coupled with his intense ego drive, enables him to home in on the target effectively and make the sale. He has the drive, the need to make the sale, and his empathy gives him the connecting tool with which to do it."[10] Most of those selected for cyberspace work roles should certainly have a strong technical skillset. Some, however, must be able to empathize with the customer in a way that not only encourages the sale but also guarantees it. This skillset may not always be found in a highly technical person, but it may be found in a cyber ugly duckling or cyber frog prince(ss). Therefore, those filling the ranks of the cyber force, and the Army force in general, should be encouraged to seek personnel with the salesman skillset (and who understand the customer's mission) and those who also possess the ability to learn about the product. The cyber force needs the non-techie salesman to be smart enough to learn the technical components so that they can portray technical proficiency.

MI officers, again, are groomed to possess this skill. From the joint operations center floors during the battle update briefs, to conference rooms during joint targeting working groups, to midnight reviews of unmanned aircraft system (UAS) feeds, MI officers are often salesmen of an intelligence product. In most cases, these officers sell the intelligence product to decision makers in support of assessments about enemy activity, to recommend routes for upcoming missions, or to assess the outcome of an operation and the enemy's response. The MI Corps sold the benefits of signals intelligence to ground commanders in Iraq and Afghanistan, resulting in signals intelligence teams alongside infantry Soldiers on foot patrols in both conflicts. Similarly, the benefits of the largest UASs were sold to tactical units, leading to the smallest UASs being launched from a Soldier's fingertips to deliver much needed visibility from the sky.

The AIDP-C program is very selective; it accepts highly skilled MI officers with proven records of accomplishment in tactical and strategic organizations. This means, MI officer-graduates from the 2-year cyber internship possess approximately 10 years of MI experience and 2 years of dedicated industry-standard training and on-the-job experience within the National Security Agency (NSA) workspaces. This creates a very powerful tool for any military organization to use. These officers will not only be able to sell their product, they are the product—a well-trained, well-spoken officer with knowledge and experience in both the field of MI and cyberspace; a multi-purpose tool a commander can use to make the most informed decisions about the enemy.

The Box is Man-Made

Joint Publication 3-12 (R), *Cyberspace Operations,* describes cyberspace in three layers: physical network, logical network, and cyber-persona. The physical network layer comprises the geographic component and the physical network components, the medium where data travels. Geographically, the network can reside in the land, air, sea, or space domains. In the logical network layer, elements of the network form relationships that are not tied to an individual, specific path, or node. Finally, the cyber-persona layer is a higher level of abstraction of the logical network in

cyberspace and uses rules that apply in the logical network layer to develop a digital footprint of an individual or entity in cyberspace. Cyber-personas are very complex because attributing responsibility and targeting in cyberspace is very difficult.[11] When considering the multiple intricate layers of cyberspace, is having a cyber technical skillset enough to effectively target individuals or entities within cyberspace?

Photo by SGT Aaron Ellerman

LTC Kirk John Junker, seminar lead instructor and director of the Joint Targeting School in Dam Neck, VA, discusses key points and principles of joint targeting during a targeting seminar at Camp Arifjan, Kuwait, October 12, 2016. The open forum seminar allowed key leaders to learn and discuss important strategies and doctrine concerning the concept of joint targeting.

I do not think so. To be an effective targeteer takes extensive education about the target or target system and experience performing targeting work. Fixing an enemy in cyberspace is not easily accomplished with a technical skillset alone. Two examples come to mind. First, the Department of Defense hosts the Joint Targeting School at Naval Air Station Oceana-Dam Neck, Virginia. It is a 6-week-long course with a mission to provide doctrinally based joint targeting education and training to prepare service, interagency, and allied personnel for operational-level targeting duties.[12] The course includes a staff course, an applications course, and battle damage assessment and collateral damage estimation courses to provide a baseline understanding of targeting in a joint military environment. However, being a successful targeteer in the cyberspace environment requires more than a 6-week course. It requires experience and potentially more training and education. The Central Intelligence Agency's (CIA's) job sheet for a targeting analyst leads credence to this theory. "Targeting analysts use unique datasets, specialized tools, and network analysis techniques to identify and analyze key threats to the U.S., identify opportunities to disrupt them, and evaluate the risks and benefits of proposed operations. Targeting analysts regularly produce a range of sophisticated short and longer-term analytic targeting intelligence products and provide close analytic support to operations for U.S. policymakers, military officials, and law enforcement agencies. Targeting analysts focus on regions of the world and on functional topics including terrorism, weapons proliferation, narcotics trafficking, counterintelligence, and cyber threats."[13] The extensive application process is not just for sensitive access to classified information. The process is in large part to determine the level of skill and experience the applicant has in targeting individuals and systems. These skills are not easily replicated and cannot be developed overnight.

In much the same way, senior cyberspace leaders should seek to broaden the workforce to include those who have extensive experience in targeting highly complex systems and extremely hardened targets. Like the CIA's call for targeting analysts who have an excellent analytical ability, solid interpersonal skills, and the ability to work under tight deadlines, the cyber force should include individuals who are targeteers first and cyberspace warriors a close second. It is not enough to understand the hardware and system software of the target (physical network layer). It is not enough to understand how multiple physical locations host accessible content through a single uniform resource locator (logical network layer). A targeteer must understand a person made the box; in turn, a person—or a group of people—controls the box and uses a series of boxes to attack U.S. interests in cyberspace (cyber-persona layer). The cyber force must consider hiring people who know more than just the ones and zeroes.

Much like the work of analysts in the CIA, MI officers and analysts have, for hundreds of years, contributed to the fight on land, in air, and at sea. From human sources informing General George Washington in the 1700s to the most technically precise use of today's MI tools, MI officers and analysts are at the cutting edge of decision making in these domains because they know the enemy. MI officers know the enemy is not only the cell phones or weapon systems they use. MI officers know both the technology and the human behind the technology. It makes sense that MI officers and analysts will do the same in the cyberspace domain. MI officers and analysts must know and understand both the capabilities and the technical analysts and operators of the cyber force. This will facilitate their collaborative work in achieving shared, not conflicting, end states that ultimately provide the commander with situational awareness and understanding.

The AIDP-C program is one method to give MI officers cyber experience, and it does so in a way that MI officers can tailor it to their interests. Over the course of 2 years, AIDP-C interns receive the flexibility to attend as much training as they like, gaining industry-standard certificates

like Network+, Security+, and Certified Ethical Hacker, while also being able to receive targeting, planning, and operator-like training courses. In conjunction with work role tours throughout the NSA footprint, AIDP-C interns have the flexibility to work alongside NSA employees with 20 or more years of experience, and USCYBERCOM and Cyber National Mission Force members. At the conclusion of the internship, each graduate brings to the table a perspective inclusive of MI and cyberspace (the ability to ask the outside-the-box question) and knowledge of how cyberspace capabilities are useful from tactical to strategic levels (how to sell what cyberspace can offer). The graduate also has experience that includes a technical acumen and understanding of how the human element relates to the cyberspace fight (cyberspace capabilities are more than ones and zeroes).

Conclusion

As I look back at my time as an AIDP-C intern and MI officer, I am amazed at the opportunities afforded to me during and after the program. I believe I received a state-of-the-art education and a set of experiences I never would have achieved otherwise. I grew to love the cyberspace field over the 2 years in the program and chose to make the leap from MI blue to Cyber gray. While my officer record brief reads "CY" today, I have not let go of all that the MI Branch offered me in the first 10 years of my career. Each day, I use skills I learned and honed as an MI officer, which I believe provide a depth and breadth to my cyber organization's needs.

The development of any new workforce is challenging and often takes many years to "get right." The military has a number of similar examples—creating the U.S. Army Air Corps and then the Air Force, and cracking the Enigma machine, to name a few. What I think can be learned from these examples, and applied to the continued development of the cyber workforce, is that it takes more than a technical background to make the organization "right." I believe inclusion of a highly technical core of cyber leaders is essential, but senior leaders should also look beyond the technical requirements of the workforce and consider the cyber ugly ducklings and cyber frogs princes(ses). The ugly ducklings and frog princes(ses), perhaps like the MI officers just beginning the AIDP-C program, may very well turn out to be the cyber swans and princes and princesses needed to defend U.S. interests in cyberspace.

If you are interested in your slice of the cyberspace pie and think you can make a difference on the battlefields within cyberspace, I challenge you to research and consider the AIDP-C program. The world is only going to become more technically connected, and the passing of ones and zeroes may ultimately mean the difference between a country's financial survival or demise, as an example, or in another more dangerous example, life or death. Some people believe future wars will be fought and won in cyberspace or, at the very least, will occur in large part in cyberspace. I chose AIDP-C because I felt called to continue my service in the newest domain, and I knew each day in the cyberspace arena would demand change, innovation, and talent—traits that I know reside in the MI Corps.

Endnotes

1. U.S. Army Human Resources Command (AHRC-OPL-R) Milper Message 14-298, "Initial 17A Cyber Branch Voluntary Transfer Incentive Program (VTIP)," 8 October 2014, para J(3).

2. *The Ugly Duckling* is a well-known children's fairytale by Hans Christian Andersen first published in 1843. A baby bird, hatched from a small group of eggs, suffers verbal and physical abuse by others on the farm because he is different. However, one day, he discovers he is actually a beautiful swan. *The Frog Prince* is an ancient story, best known through the Brothers Grimm's version. It is about a frog who just wants love, and if allowed to eat off the princess's plate and sleep on her pillow for 3 days, he will transform into a prince and deliver just the thing the princess was looking for. In much the same way, the less-technical individuals who may have been ill considered for a position in the cyber workforce may actually be the very people the cyber workforce needs to maximize its effectiveness.

3. Drew Boyd, "Thinking Outside the Box: A Misguided Approach," *Psychology Today*, February 6, 2014, https://www.psychologytoday.com/blog/inside-the-box/201402/thinking-outside-the-box-misguided-idea.

4. Spencer Ackerman, "US government responds to latest hack: give us more power over data collection," *The Guardian*, 5 June 2015, http://www.theguardian.com/technology/2015/jun/05/us-government-opm-hack-data-collection-powers.

5. Enjoli Francis, "Hackers, Possibly From Middle East, Block U.S. Bank's Websites," *ABC News*, September 27, 2012, http://abcnews.go.com/US/hackers-block-us-banks-online-service-bank-america/story?id=17343055.

6. "Hiring from Outside the Company: How New People Can Bring Unexpected Problems," *Knowledge@Wharton*, September 3, 2008, http://knowledge.wharton.upenn.edu/article/hiring-from-outside-the-company-how-new-people-can-bring-unexpected-problems/.

7. Ibid.

8. Malcolm Gadwell, "The Tipping Point," Gladwell.com, accessed 13 February 2016, http://gladwell.com/the-tipping-point/.

9. Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington DC: U.S. Government Publishing Office, 5 February 2003), I-2.

10. David Mayer and Herbert M. Greenberg, "What Makes a Good Salesman," *Harvard Business Review*, July–August 2006, https://hbr.org/2006/07/what-makes-a-good-salesman.

11. JP 3-12(R), *Cyberspace Operations,* I-2 to I-4.

12. "Joint Targeting School," *Joint Electronic Library,* last updated 18 October 2017, http://www.dtic.mil/doctrine/jfs/jts.htm.

13. "Careers and Internships–Targeting Analyst," *Central Intelligence Agency,* last updated July 11, 2017, https://www.cia.gov/careers/opportunities/analytical/targeting-analyst.html.

I had a discussion with a classmate on my topic, and it was in that conversation that he used the reference of cyber ugly duckling. I want to acknowledge that although* The Ugly Duckling *is a well-known children's story, and I generated the article topic myself, it was my classmate's comments that gave me the idea for the title. Thank you, LCDR Joel Yates!

MAJ Danielle Gonzalez serves as a national mission team lead in the Cyber National Mission Force at Fort Meade, MD. She was previously an intern at the Army Intelligence Development Program–Cyber and the Future Readiness Officer at U.S. Army Human Resources Command. She also served in both command and staff positions with 7th Special Force Group (Airborne), 111th Military Intelligence Brigade, and 10th Mountain Division (Light Infantry).

Contact and Article
Submission Information

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

When writing an article, select a topic relevant to the Military Intelligence and Intelligence Communities.

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

When submitting articles to MIPB, please take the following into consideration:

- Feature articles, in most cases, should be under 3,000 words, double-spaced with normal margins without embedded graphics.
- We cannot guarantee we will publish all submitted articles and it may take up to a year to publish some articles.
- Although MIPB targets themes, you do not need to "write" to a theme.
- Please note that submissions become property of MIPB and may be released to other government agencies or nonprofit organizations for republication upon request.

What we need from you:

- A release signed by your unit or organization's information security officer/operations security officer/SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain (IAW AR 380-5 DA Information Security Program). A sample security release format can be accessed at our website at https://www.ikn.army.mil/apps/MIPBW.
- A cover letter (either hard copy or electronic) with your work or home email addresses, telephone number, and a comment stating your desire to have your article published.
- Your article in Word. Do not use special document templates.
- Any pictures, graphics, crests, or logos which are relevant to your topic. We need complete captions (the Who, What, Where, When), photographer credits, and the author's name on photos. Do not embed graphics or photos within the article. Send them as separate files such as .tif or .jpg and note where they should appear in the article. PowerPoint (not in .tif or .jpg format) is acceptable for graphs, etc. Photos should be at 300 dpi.
- The full name of each author in the byline and a short biography for each. The biography should include the author's current duty assignment, related assignments, relevant civilian education and degrees, and any other special qualifications.

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

Submit articles, graphics, or questions to the Editor at usarmy.huachuca.icoe.mbx.mipb@mail.mil.

Our contact information:
Contact phone numbers: Commercial 520.533.7836
DSN 821.7836

Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance: Critical to an Army Corps

by Major Camero Song

What is the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance?

This article highlights the Military Intelligence (MI) Branch's initiative to develop MI professionals in the collection realm through a program called the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance (AIDP–ISR). It is important to note that this program is not the all-inclusive answer to collections training for the Army but is a catalyst to advance the intelligence warfighting function.

AIDP–ISR is the Army's effort to train and develop certified collection managers who can operate at the tactical, operational, and strategic levels. Based at the 704th MI Brigade at Fort Meade, Maryland, the program exposes students to, arguably, the best collections training the Department of Defense has to offer. Students train in the Washington, DC; Maryland; Virginia region. They have access to all the resident intelligence courses offered by organizations such as the National Security Agency, National Geospatial-Intelligence Agency, and Defense Intelligence Agency. Managers of the program have built key relationships with joint trainers and "enablers," allowing access to programs and classes that would be difficult to attend outside the program. Such classes include the Air Force ISR Operations Course, the Document and Media Exploitation Course, and the Joint Network Attack Course.

Each year, the program accepts up to 10 senior captains or junior majors. This is a remarkable program because, besides the handful of baseline core collection courses, students have the freedom and latitude to tailor their own collections training curriculum to the focus area of their choosing. This is one of the few programs that allow students to personally design their education by selecting building-block electives (known as core-enhancing courses and reinforcing visits). The student can pick as many courses and site visits as desired. Toward the end of the program, AIDP–ISR offers students the opportunity to participate in a capstone event. During this event, students apply their collection knowledge to an available unit or exercise that aligns with their future assignment.

AIDP–ISR Critical to an Army Corps

Knowledge gained in the AIDP–ISR program plays a critical role in supporting the force, and graduates use it to the fullest, especially at the Army corps level. At I Corps, an AIDP–ISR graduate currently fills the corps' collection manager position. Although it is a U.S. Army Forces Command unit, I Corps aligns with the U.S. Pacific Command (PACOM), which means the collection team has exposure to countless real-world and joint exercise opportunities. Like most units, I Corps operates with a very high operating tempo. I Corps headquarters actively trains and certifies at varying levels, including a tactical Army corps headquarters, a combined/joint force land component command, and a joint task force (JTF) with various allied and partner countries. Due to the fast pace of the unit, there is little time to train incoming collection managers to operate at the level the G-2 and commander require of their collection management team. One such example is Exercise Talisman Saber during which I Corps will operate and certify as a JTF headquarters while working alongside partners from Australia, New Zealand, and Canada. Without the institutional knowledge gained from AIDP–ISR, developing a collection branch to support this level of headquarters would be a complicated feat. A collection manager at this level needs to synchronize allocated theater assets while prioritizing major subordinate commands' collection requirements. The collection manager works alongside PACOM's collection branch to ensure the JTF's component prioritized collection list is tasked appropriately for the joint operating area. The collection team will also develop a collection strategy with more robust capabilities that feed the JTF's indicators and warnings and the joint targeting process. A strong officer could definitely do the job, but it would be a challenging situation.

In addition to training on direct action, the I Corps collection team focuses on collection support to steady-state operations. Since I Corps aligns with PACOM, the G-2 conducts intelligence support to PACOM phase 0 (shape) operations while in garrison. Their collection team properly builds a collection strategy, effectively researches and leverages existing collection requirements, and disseminates the information to relevant parties. The knowledge gained in the

program allows the collection manager to train a collection team that could effectively operate in a dynamic phase III (dominate) scenario during joint exercise life-cycle training opportunities and steady-state phase 0/I (shape/deter) operations. Another important aspect of the I Corps collection manager's duties is the role of collection manager for the installation's senior intelligence officer. The collection manager is the de facto collection trainer for all the major subordinate commands on the installation. Luckily, for AIDP–ISR graduates, the course qualifies them to fulfill this role.

Graduates of the AIDP–ISR program can immediately execute the duties of a collection manager. In some cases, when the Army assigns officers to a new position, they spend 1 to 3 months learning the job. With the robust and intense training AIDP–ISR offers to its students, graduates receive the foundational knowledge to advance their section and collection strategy for the G-2 and commander immediately upon assuming the new assignment.

Beneficial for Key Development Time

Upon completion of the program, students take a test to obtain their Certified Collection Management Professional-Fundamentals Department of Defense certification, and they receive award of the skill identifier "3F." Besides the numerous qualifications and excellent training they receive, ADP–ISR postures students perfectly for their career as a major in the Army. Immediately after completing the AIDP–ISR program, graduates or "AIDPers" are ready to attend the Command and General Staff College. AIDPers arrive at their next duty assignment as a major, intermediate-level education complete, and are likely to fill a collection management key development (KD) billet for 12 to 24 months. AIDP–ISR graduates are also more likely than junior majors to complete 24 months of KD within the first 2 to 3 years of their promotion to major (or within their first permanent assignment as a major). This is a huge advantage because many officers need time to build credibility in order to earn a KD position when arriving at a new unit or new installation. An additional benefit is that completing 12 to 24 months of KD so early in the process allows graduates to retain the flexibility to apply for more KD, conduct a broadening assignment, or apply for another Army special program for further development.

AIDP–ISR is a great opportunity for young MI professionals; however, there are some areas for improvement. Even though students become trained collection managers and work with the MI Branch for assignment as a division or corps collection manager, the assignment is not guaranteed when they arrive at a unit. The senior intelligence officer or the commander may have different plans for the graduate. It is important for graduates to keep this in mind and understand there is no guarantee for becoming a collection manager. Fortunately, graduates are equipped to do well in any position to which the command assigns them because of knowledge gained from the program.

Collection Training Areas for Improvement

AIDP–ISR is a great initiative to train collection managers, but it should not be the Army's only answer to developing collection capabilities for commanders. There are some areas for improvement. One thing to consider is that AIDP–ISR focuses more on the operational and strategic levels of collection operations. Therefore, graduates understand a great deal of the collection process at the JTF, the joint force command, and the national level, rather than at the tactical level. The vast majority of courses focus on theater and national collection procedures. Integrating AIDP–ISR interns into Combat Training Center rotations (such as the Joint Readiness Training Center and the National Training Center) and division- and corps-level warfighter exercises, as guest observers or controller trainers, could help bridge this gap and serve as the capstone event for AIDP–ISR.

Another issue with the program is that there are not enough AIDP–ISR billets to adequately source all collection manager positions in the Army. Although the Army designed AIDP–ISR to produce division collection managers, the Army's three corps, five battlefield coordination detachments, and three expeditionary MI brigades could benefit from AIDP–ISR trained personnel. This year, AIDP–ISR will have its first warrant officer intern, which along with further expansion of AIDP–ISR to MI noncommissioned officers above the rank of staff sergeant will provide substantial benefit to the unit if assigned as a collection management deputy or noncommissioned officer in charge. Allowing the deputy and/or noncommissioned officer in charge to be AIDP–ISR trained would provide substantial benefit to the unit.

The final recommendation for improvement is not focused on AIDP–ISR but on collection training for Army intelligence overall. Company-level professional military education should incorporate more in-depth collection training. Collection training at the Advanced Leader Course, Warrant Officer's Advanced Course, and Military Intelligence Captain's Career Course should not just focus on the capabilities each intelligence discipline provides or the capabilities of collection assets. Every senior noncommissioned officer, junior warrant officer, lieutenant, and captain should know the fundamentals of collection management. Not only should they be proficient at collection

requirements management but also at collection operations management, ISR operations, and ISR planning. The MI professional should be able to fully leverage collections to support the commander's decision support matrix, manage organic assets, effectively request for higher collect, and manage subordinate collection managers.

There is a delta in training the force on collection management. With the growing emphasis on ISR to support operations, trained and effective collection managers are in high demand. AIDP–ISR is a great initiative to fill this gap; however, like every program and process, there is always room for improvement.

MAJ Camero Song is a graduate of the Army Intelligence Development Program-Intelligence, Surveillance, and Reconnaissance program and is currently the I Corps collection manager. He stood up the collections framework and strategy for I Corps' intelligence support to phase 0 (shape) operations and served as the collection manager for numerous joint exercise life-cycle events, including Ulchi Freedom Guardian, Yama Sakura, Key Resolve, and other warfighter exercises.

Effect Positive Change

During a presentation of recent lessons and best practices to a room full of Military Intelligence Captain's Career Course (MICCC) students, one captain pointedly asked, "Instead of telling us what we're doing wrong, why don't you tell us what we're doing right?" The student further commented that most of the lessons learned information often emphasized the challenges and enduring patterns or trends of less than optimal performance. In the student's words, "Things they're being told they are doing wrong." Another student shared the statement of an evaluator made immediately before beginning a collective, home-station training exercise at a prior assignment: "I already know you're going to have problems in topics A, B, and C." The evaluator's assessment in advance of the training event served as a disincentive to even attempt achieving success. The officer explained that the unit's Soldiers saw no value in exerting more than minimal effort on a task for which they would not be successful, as evidenced by the evaluator's prejudiced assessment.

I responded by declaring that the Army's Lessons Learned enterprise shared their concerns and is already taking steps to increase the identification and dissemination of best practices. The intent of highlighting best practices is to help commanders, leaders, and Soldiers integrate the most successful techniques and procedures into unit planning, preparation, operations, and assessment strategies. The Lessons Learned column appearing in the July-September 2016 issue of Military Intelligence Professional Bulletin described the Army Lessons Learned enterprise's version of emphasizing best practices—the Before Action Report. The U.S. Army Intelligence Center of Excellence (USAICoE) expanded upon the Before Action Report effort and evolved it into another technique—the Before Action Report Relevant Exchange of Lessons (BARREL). This new technique and name haven't quite caught on as well as we had hoped; but the requests from units for information contained in the BARREL continue to increase over time. The BARREL is simply a mechanism through which the USAICoE Lessons Learned Team provides best practice information to unit leaders. The key to a successful BARREL is to establish a dialogue with unit leaders far enough in advance of an operation or training event to positively impact unit planning.

I cannot fault the MICCC students for voicing their expectation that the lessons and best practices brief would focus only on poor performance. They may not have been aware that the driving force of the Army Lessons Learned enterprise is to effect positive change—not criticize performance. It is inherent in every adaptive learning organization to conduct critical self-assessment. Sometimes this can lead to unanticipated consequences such as those voiced by the two students. The repetitive reporting of the same (or similar) lessons is sure to induce a conditioned (Pavlovian) response. This type of attitude was conveyed in another student's statement, "Why (should we) even bother to try?" Several immediate responses came to mind, none of which would have resulted in an effective learning outcome. The question had merit; but it also became the catalyst for action when combined with another student's request of, "Show me what right looks like."

Best Practice Library

The USAICoE Lessons Learned Team is determining the best way to implement a new feature of our program—an online best practices library. We intend to create a place where Soldiers and leaders can access and share best practice examples.

The idea of creating a library of best practice products began earlier this year as USAICoE's Directorate of Training personnel engaged with the brigade combat team S-2 course instructors and students at Fort Leavenworth, Kansas. We thought by presenting best practice examples from personnel in the field, we could demonstrate how others implemented fundamental military intelligence (MI) doctrinal techniques and processes in accordance with the operational and mission variables. While our MI Lessons Learned Repository contains an abundance of best practices, none are highlighted or consolidated in a single location.

Thinking over the opinions offered by the MICCC students, two things became clear for the USAICoE Lessons Learned Team:

- We were not meeting the needs of USAICoE students soon to serve as battalion S-2s or MI company commanders.
- We needed to immediately implement the program improvements we had developed.

Revised Collection Reports

Fortunately, complementary improvements recently made to the USAICoE Lessons Learned program made it much easier for us to highlight examples of "what right looks like" for some topics. The first change is evident in the revised format of USAICoE's Lessons Learned collection reports. These reports are comprised of separate observations grouped under a common topic. The first part of the lessons learned report lists the topics and the titles of the supporting separate observations. The list serves as a table of contents for the report. Topics and observations, which the report presents as an actual or potential best practice, are labeled "A Best Practice."

The second part of the report presents the observations (lessons and best practices) in detail using the familiar observation, discussion, and recommendation format. Separate best practice observations are also marked "A Best Practice" in this part of the report. Additionally, the topics and observations listed in the first part of the report are hypertext linked to the supporting observation. The hyperlinks make it easier to access information of interest.

The two parts of the report are consolidated into one document when disseminated to members of the MI Lessons Learned enterprise (email distribution) or when uploaded to the Joint Lessons Learned Information System (JLLIS) and the USAICoE Lessons Learned Portal.

Another recent change we've made to our reports is to include actual examples of best practice products. We embed small (file size) products as figures and provide attachments for larger products. Products too large to send as email attachments, we identify in the reports and include a web address link to the product. Revising the format and contents of reports still requires one to open each report and then each best practice separately. Additionally, by the time of this publication we will have instituted another improvement to the USAICoE Lessons Learned program—a best practices repository on the MI Lessons Learned homepage.

Best Practices Repository

A section of the USAICoE Lessons Learned Portal will be devoted exclusively to best practices. We struggled with identifying the best way of organizing the Best Practices Repository. The Lessons Learned Portal already has an overabundance of separate folders and sub-folders in which products are stored. We want to make it easier for you to find the best practices relevant to your requirements; not make it more difficult. The MICCC student's original question makes it painfully obvious we need to eliminate any further delay. We have started placing examples (lessons learned observations and products from various sources) identified as best practices into the repository. To avoid suffering paralysis due to (over) analysis, we chose to let the contents of the Best Practices Repository indicate a suitable categorization scheme over time. We will periodically review the Best Practice holdings to ensure the examples we posted are still of value to current operations. We will also ensure the contents are timely, accurate, and pertinent. Items removed from the Best Practices Repository will remain part of the original product(s) already stored in other file locations on our site and on JLLIS.

Conclusion

We are dependent upon your feedback to make the Best Practices Repository effective. We are already dependent upon your allowing us to discover best practices from observing your operations and training. Another challenge we face, in which we seek your assistance, is learning of MI best practices publicized in other venues. Keep us in mind as you come across MI best practices in your professional and personal experiences. Armor, Infantry, Fires, MI, and other professional bulletins along with other publications, such as *Small Wars Journal*, frequently contain MI best practice information. Sometimes we miss an article or two, so we encourage you to contact us regarding items you think we should know about.

Though we are concentrating our focus on best practices, we continue to collect and report lessons (problems, challenges, issues) from the field. As a member of the Army's Lessons Learned enterprise, the USAICoE Lessons Learned Team is required to identify problems, help develop solutions, and drive positive changes in training, equipping, and leading the force. Both the Center for Army Lessons Learned and USAICoE are emphasizing the transition from reporting lessons learned to integrating lessons and best practices "…to improve performance and efficiency and to save lives across the force."[1]

We look forward to receiving your lessons and best practices. To learn more, visit the Center for Army Lessons Learned https://call2.army.mil/or USACICoE MI Lessons Learned Portal https://army.deps.mil/Army/CMDS/USAICoE_Other/LL/SitePages/Home.aspx.

Endnote

1. U.S. Army Regulation 11-33, *Army Lessons Learned Program* (Washington DC: Government Publishing Office, 2017), 3.

Human Intelligence Trainees and the Struggle to Acculturate

by Mr. Mounir Bouchareb

Introduction

Human intelligence (HUMINT) plays a critical role within the intelligence arena, helping outline foreign policy outcomes and protecting U.S. interests around the globe. This type of intelligence activity, conducted by trained HUMINT collectors, requires actual contact with humans and demands mental strength, resilience, and adaptability. As part of their job, HUMINT collectors are in frequent contact with other cultures, increasing the probability that an exchange will take place in which the two sides may or may not adapt behavior, language, values, and beliefs. HUMINT collectors are among the most rigorously trained military personnel. Our national security's critical dependence on HUMINT to deliver results demands that we identify tools and strategies to help HUMINT collectors manage cultural stressors and maintain their psychological health. This will result in maximized HUMINT collection efforts.[1]

What is Human Intelligence and Why is it so Central?

Tasks of the HUMINT collector can include:

- Interrogations.
- Source operations.
- Debriefings.
- Liaison with allied counterparts.

These tasks can take the HUMINT collector to a multitude of areas of operation around the globe. HUMINT collectors are well prepared to answer intelligence and information requirements through long and rigorous hours of training. They have strict guidelines to follow and consistently sharpen their skills through planning and preparation, research, and hands-on experience. Understanding cultural influence, such as history, politics, economics, religion, and geography, is a big part of their job as they develop language and interpersonal skills and sharpen critical character traits. Overall, HUMINT collectors are well-rounded, motivated, and intelligent individuals who require the utmost attention and support to accomplish a very challenging and complex mission.[2]

As HUMINT collectors encounter other cultures, the goal, generally, is to pursue a mutual understanding and negotiate a compromise, with an end goal in mind. According to John Berry, a renowned professor of psychology, this encounter results in acculturation, which is "the process of cultural change and psychological change that results following meeting between cultures."[3] In other words, acculturation is what happens when you live with French people for a while and start saying "ooh la la" and eating snails. On a more serious note, however, "As enculturation is used to describe the process of first-culture learning, acculturation can be thought of as second-culture learning."[4] HUMINT

collectors may experience a less lasting and potent form called individual-level acculturation, especially if the mission is a short-term assignment.[5]

Cross-cultural psychology has been central in the study of this change in human behavior stemming from cultural contact between people. Much of the research findings concluded that there are large variations in how individuals acculturate and acclimate to this process. Research on inter-cultural contact has discovered that "there are relationships between how individuals acculturate and how well they adapt."[6] Stress is experienced during the acculturation process, and there are variations in psychological and sociocultural adaptation.[7] Therefore, having an acculturation strategy can be critical in reducing culture shock; but we should also take into consideration the fact that individuals are unique in their ability to cope.

When I was an instructor at the U.S. Army HUMINT collector course, I understood that each individual was unique in their ability to cope. I always tailored the one-on-one practice sessions to meet the needs of each student . The key, in my experience, was to portray and maintain a realistic role that would naturally trigger stressors necessary to create a beneficial encounter that ultimately resulted in self-awareness and personal growth.

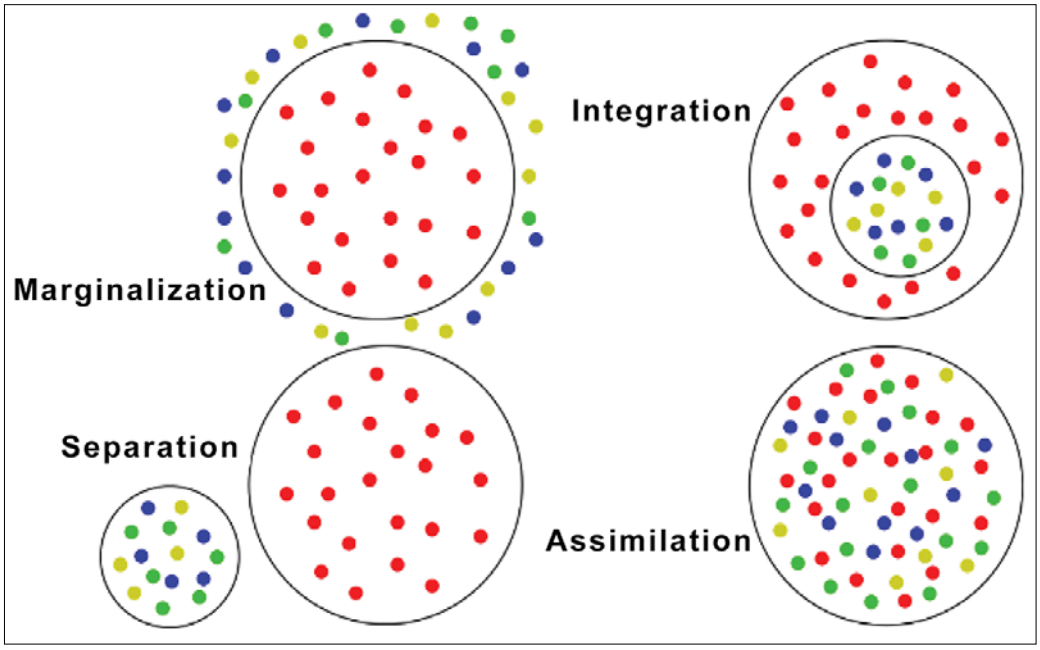
Acculturation Explained

As we seek to adapt through acculturation, our ultimate goal is to find physical and psychological well-being and sociocultural balance when managing daily activity within this new reality.[8] Berry states, "Good psychological adaptation is predicted by personality variables, life changing events, and social support, whereas good sociocultural adaptation is predicted by cultural knowledge, degree of contact, and positive intergroup attitudes."[9]

The HUMINT instructor nurtures psychological adaptation by establishing a 5-month-long professional relationship based on trust and social support, thus helping to ease the arduous process of adaptation. On the other hand, every encounter or iteration triggers the sociocultural adaptation, transporting the student into a realistic scenario encompassing complex human interactions and stressful encounters. These repetitive but unique iterations allow students to develop a type of muscle memory, becoming more at ease with every encounter. This frees the mind to develop other areas of interest such as communication skills, rapport building skills, and approach strategies.

"The most widely researched…approach to acculturation has been John Berry's acculturation framework,"[10] which has shown that two critical issues are debated before the acculturation process begins: Do we want to preserve our cultural heritage, and how willing are we to interact with this new culture?[11] People do not experience acculturation in the same way and usually seek out an acculturation strategy based on their attitudes and behaviors.[12] For a HUMINT collector, certain factors will be critical when answering the above questions, such as:

- Skill level.
- Age.
- Prior cultural exposure.
- Practical Life experience.
- Multilingual ability.
- Personality type.
- Motivation.
- Sincerity.
- Stress management skills.
- Self-understanding.[13]



Acculturation Strategies.

Once we answer the acculturation framework questions, the next step is to decide on an acculturation strategy by choosing from one of the following four strategies:

Assimilation. The assimilation strategy is when one does not want to maintain a cultural identity but does want close contact

with another culture, in essence adopting the cultural values and norms of the other.[14]

Separation. The separation strategy is when one wants to maintain a cultural identity but does not want close contact with another culture.[15]

Integration. The integration strategy is when one wants to maintain a cultural identity but also wants close contact with another culture, essentially seeking a middle ground.[16]

Marginalization. Finally, the marginalization strategy is when one does not want to maintain a cultural identity and does not want close contact with another culture.[17]

Each individual's unique culture and how they perceive it creates an imprint; therefore, "acculturation involves alterations in the individual's sense of self"[18] and "changes in a person's behavioral repertoire."[19]

As an instructor, I found it was important to identify each student's unique acculturation strategy early on in order to help nurture it. If an individual favors, for example, an assimilation strategy, instructors would tailor the training and provide the skills necessary. Ultimately, as students progressed, the ideal is to have HUMINT collectors who can adapt to all four acculturation strategies and are able to morph when necessary. A HUMINT collector who can adapt to any situation has a higher rate of return when it comes to collection efforts.

Strategies

We need to ask ourselves what changes take place during acculturation. We should question the nature of this relationship, and question whether control or common respect is its foundation. As a result of these inquiries, what observable changes have occurred as a result of these two-way interactions? Who am I and where do I belong?

As previously mentioned, an acculturation strategy is unique to each individual, with variation across the spectrum, depending on personal beliefs and perceptions of the host culture.[20] Because of that, one may choose, for example, to acculturate values or beliefs but not necessarily political ideology and vice versa. The compatibility of the two cultures' values, beliefs, behaviors, and norms requires analysis, as it is a critical component of the process of selecting a strategy.[21] Other changes that occur during acculturation are affective (stress/emotions), behavioral (social coping mechanisms), and cognitive (self-perception).[22]

Socrates said, "To know thyself is the beginning of wisdom." Self-knowledge is also a stepping-stone to acculturation. Students at the HUMINT course are confronted with their innermost fears during every iteration or practical exercise, allowing them to discover strengths and weaknesses and the opportunity to modify behavior before they actually face it on the battlefield.

One hurdle mentioned by George Kelly discusses personal constructs, such as stereotypes and prejudices, which have a tendency to manipulate our thinking and actions.[23] Niklas Luhmann debates the importance of what he calls double contingency, or personal expectations, as critical to creating mutual understanding through communication, openness, and sharing. The less we know about each other, the more arduous the road to inter-connectedness.[24] For this reason, a rigorous and constant barrage of cultural training and development has been at the core of all the HUMINT training.

Best Acculturation Strategy, Why Integration?

Researchers have found that selecting the right acculturation strategy will determine how well one adapts. The

Photo by U.S. Air Force SSgt. Benjamin Raughton

U.S. Army Reserve Officer Training Corps cadets watch as a Djiboutian Army weapons instructor teaches them how to safely field strip an AK-47 at the Djiboutian Army Academy in Arta, Djibouti, July 25, 2016. After the cadets learned the fundamentals, they competed with each other to see who was the quickest at field stripping the weapon.

majority of research has discovered that *integration* results in the best psychological and sociocultural outcomes, while *marginalization* results in the least adaptability and is least favorable.[25] So how well do people acculturate? To answer this question, we need to look at long-term psychological and physical health, communication proficiency, self-awareness, stress management, emotional acceptance, and cultural awareness skills.[26] Adaptation is not tantamount to acculturation, but it can manifest itself as a result of change.[27]

As the debate continues, there has been a split in acculturation research between the unidimensional and the bidimensional views on acculturation. The major difference between the two models is "how they treat the relationship between the culture of birth or upbringing, referred to here as the *heritage culture*, and the predominant cultural environment, or *mainstream culture.*"[28] The *unidimensional* approach theorizes that a shedding of attitudes, values, and behaviors takes place as the person acquires new ones from the mainstream culture.[29] The *bidimensional* approach is convinced that the heritage and mainstream cultures have equal share in reshaping attitudes, values, and behaviors, giving the individual a choice in adopting parts or wholes.[30] My personal observation is that both unidimensional and bidimensional approaches have been used successfully by students. The circumstances, personality traits, individuals involved, and selected approach strategy are the factors that determine the success rate. The students control the choice of acculturation strategy that fits the scenario, and they are encouraged to remain flexible throughout the process.

Regardless of how the process of acculturation takes place, there are factors that play a crucial role in the rate at which an individual begins to adapt. These components include but are not limited to "premigration exposure to the mainstream culture, residence in an ethnic neighborhood, willingness to seek language education, and frequency of contact with individuals from the mainstream culture."[31]

Acculturative Stress

When exposed to a new culture, people meet many obstacles such as language, values, beliefs, behaviors, and norms, resulting in a tremendous amount of trauma, also referred to as acculturative stress. Acculturative stress is a critical factor in mental health stability and a predictor of future psychological problems. Variables that have a tendency to affect the stress level include the extent to which the two cultures differ, the reason for contact between the two, and the degree of acceptance of the host culture.[32] Acculturative integration is least stressful, while marginalization is the most stressful. On the other hand, assimilation and separation approaches tend to alternate in the stress level, depending on the circumstances.[33.]

When exposed to acculturative stress, individuals can undergo psychological changes such as behavioral alterations in speaking, dressing, and eating, accompanied by indecision, anxiety, and depression.[34] This type of major change is comparable to the stresses brought on by a major life event or events, which are usually accompanied by serious challenges. Examples of manifestation of acculturative stress in HUMINT collector trainees include complete shutdown, refusal to communicate, defensive posture, argumentative attitude, surrender to the other culture, focus on intelligence collection, and attempt to convert the host culture to their own worldview. When skilled HUMINT instructors notice these behaviors in students, the first step is to maintain the authenticity of the training by remaining in role. This guarantees that the stresses remain active; otherwise, the learning value is lost. The second step is to identify the behavior caused by stress and channel it through constructive means such as subtle in-role leads. The instructor should provide just enough assistance to prevent drowning, but the rest has to come from the student's own willingness to change course. For example, if a student takes a defensive posture, the instructor should intervene and mention, in role, that in their culture, a lack of eye contact is considered rude and offensive. Depending on the circumstance, the subtlety of the message will depend on the skill level of the student and severity of the problem. This quickly helps the student regain their composure and resume training, having now developed a strategy to help reduce stress in a future encounter of similar circumstances.

Conclusion

Acculturation theory is a revelation. It not only reveals the range of possible acculturation strategies, but it also provides an insight into possibilities that we might not have considered. For example, HUMINT collectors can acculturate to cultures that they may not necessarily like or that exist in a bicultural state, finding marginality to be a positive trait. The integrationist strategy of acculturation is the path of least resistance for a HUMINT collector. Berry said, "This may be an example of reciprocity in mutual attitudes: If immigrants experience rejection from the society of settlement, then they are more likely to reject them in return."[35] For a HUMINT collector, it especially rings true that showing humility and sincerity while extending an olive branch will most likely open doors and is a sign of strength and courage. On the other hand, Berry stresses, "discrimination is often the most powerful predictor of poor psychological and

sociocultural adaptation."[36] Discrimination, as it applies to HUMINT, is the action of rejecting the other culture or lacking in motivation to acculturate.

As instructors, we also concluded that a link existed between acculturation strategies and adaptation. We now know, after much research, that acculturation is survivable. Acculturation does not weaken the individual, by any means; it is instead a rather empowering and enriching experience. This is especially relevant in our multicultural society where acculturation will become inevitable and essential not only for its inherent value but also in the benefit received from bridging the gap and maintaining a steady stream of diversity into the world. It is critical for HUMINT collectors to develop the skills to transition in and out of cultures with ease and simplicity in order to surmount stress and achieve success in their mission endeavors.

Endnotes

1. "Intelligence: Human Intelligence," *Central Intelligence Agency*, April 30, 2013, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html.

2. U.S. Army Field Manual (FM) 2-22.3, *Human Intelligence Collector Operations* (Washington DC: Government Publishing Office, 2006), 1-12, 1-13.

3. David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 472, doi: 10.1177/1745691610373075.

4. Joseph Adebayo Awoyemi, *Pre-Marital Counselling In a Multicultural Society* (Morrisville, NC: Lulu Press, 2014), 213.

5. Ibid.

6. David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 472, doi: 10.1177/1745691610373075.

7. Ibid., 475.

8. Ibid., 476.

9. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 709.

10. Andrew G. Ryder, Lynn E. Alden, and Delroy L. Paulhus, "Is Acculturation Unidimensional or Bidimensional? A Head-to-Head Comparison in the Prediction of Personality, Self-Identity, and Adjustment," *Journal of Personality and Social Psychology* 79, no. 1 (2000): 50.

11. David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 476, doi: 10.1177/1745691610373075.

12. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 702.

13. Magid Al-Araki, "Models of Intercultural Communication: Identities, Styles of Acculturation, and Premises for Enjoying the Company of One Another—Empirical Data From the Public Sector in Norway," *SAGE Open* 5, no. 2 (August 2015): 1, doi: 10.1177/2158244015577795.

14. David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 476, doi: 10.1177/1745691610373075.

15. Ibid.

16. Ibid.

17. Ibid.

18. Andrew G. Ryder, Lynn E. Alden, and Delroy L. Paulhus, "Is Acculturation Unidimensional or Bidimensional? A Head-to-Head Comparison in the Prediction of Personality, Self-Identity, and Adjustment," *Journal of Personality and Social Psychology* 79, no. 1 (2000): 49.

19. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 707.

20. Joseph Adebayo Awoyemi, *Pre-Marital Counselling In a Multicultural Society* (Morrisville, NC: Lulu Press, 2014), 213.

21. David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 473, doi: 10.1177/1745691610373075.

22. Ibid., 474-475.

23. Magid Al-Araki, "Models of Intercultural Communication: Identities, Styles of Acculturation, and Premises for Enjoying the Company of One Another—Empirical Data From the Public Sector in Norway," *SAGE Open* 5, no. 2 (August 2015): 2, doi: 10.1177/2158244015577795.

24. Ibid., 3.

25. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 708-709; Andrew G. Ryder, Lynn E. Alden, and Delroy L. Paulhus, "Is Acculturation Unidimensional or Bidimensional? A Head-to-Head Comparison in the Prediction of Personality, Self-Identity, and Adjustment," *Journal of Personality and Social Psychology* 79, no. 1 (2000): 53; David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 477, doi: 10.1177/1745691610373075.

26. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 709.

27. Ibid., 699, 706.

28. Andrew G. Ryder, Lynn E. Alden, and Delroy L. Paulhus, "Is Acculturation Unidimensional or Bidimensional? A Head-to-Head Comparison in the Prediction of Personality, Self-Identity, and Adjustment," *Journal of Personality and Social Psychology* 79, no. 1 (2000): 49.

29. Ibid., 49-50.

30. Ibid., 49-50.

31. Ibid., 50.

32. "John Wesley Powell," New World Encyclopedia, 9 September 2016, http://www.newworldencyclopedia.org/p/index.php?title=John_Wesley_Powell&oldid=999195.

33. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 708; David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 474, doi: 10.1177/1745691610373075.

34. John W. Berry, "Acculturation: Living Successfully in Two Cultures," *International Journal of Intercultural Relations* 29, no. 6 (2005): 702.

35. David L. Sam and John W. Berry, "Acculturation: When Individuals and Groups of Different Cultural Backgrounds Meet," *Perspectives on Psychological Science* 5, no. 4 (2010): 479, doi: 10.1177/1745691610373075.

36. Ibid.

References

New World Encyclopedia contributors. "Acculturation." New World Encyclopedia. http://www.newworldencyclopedia.org/p/index.php?title=Acculturation&oldid=993879.

Trimble, Joseph, E. "Introduction: Social Change and Acculturation." In Acculturation: Advances in Theory, Measurement, and Applied Research. Edited by Kevin M. Chun, Pamela Balls Organista, and Geranrdo Marin. Washington, DC: American Psychology Association, 2003, https://www.researchgate.net/profile/Joseph_Trimble/publication/236844501_Introduction_Social_change_and_acculturation/links/54b6f1150cf2e68eb28002db/Introduction-Social-change-and-acculturation.pdf.

U.S. Army. FM 3-24, "Culture" Chap. 3 in *Insurgencies and Countering Insurgencies.* Washington DC: GPO, 2014.

U.S. Army. FM 3-24.2, *Tactics in Counterinsurgency*. Washington DC: GPO, 2009.

Van Dyne, L., Ang, S., and Livermore, D. "Cultural Intelligence: A Pathway for Leading in a Rapidly Globalizing World." In K.M. Hannum. B. McFeeters, and L. Booysen (Eds.), Leading Across Differences: Casebook. San Francisco, CA: Pfeiffer.

Mr. Mounir Bouchareb is a senior training development specialist and a master instructor at the U.S. Army Training and Doctrine Command Culture Center at Fort Huachuca, AZ. He completed a bachelor of arts in education in 2002 and a master of arts in political science in 2010. His interests have been in education and the study of foreign languages. Before joining the Culture Center, Mounir served multiple tours as a senior interrogator during Operation Iraqi Freedom and later as a training instructor at the human intelligence collector course, spanning a 16-year career in military intelligence.

by Ms. Lori S. Tagg, USAICoE Command Historian

In the latter half of the 19th century, military organizations around the world began experimenting with aerial technologies. By the early part of the 20th century, advances in airplanes and cameras inevitably linked these two technologies for military intelligence purposes. By the time the United States entered World War I, aerial visual and photographic reconnaissance had become principal sources of intelligence used by the British and French for planning and executing battles. Following the lead of the Allies, the fledgling U.S. Air Service deployed 18 Aero Squadrons (Observation) to France in 1917 and 1918. Of these, 14 served with 1st, 3rd, 4th, 5th, and 6th Corps. The first corps-level observation group was established in 1st Corps.

In April 1918, the 1st Corps Observation Group was assigned to the Toul Sector in support of the 26th Division. The Group consisted of the 1st Aero Squadron, responsible for long-range visual observation and aerial photographic missions and adjustment of divisional heavy artillery fire, and the 12th Aero Squadron, which conducted short-range visual and photographic missions, light artillery spotting missions, and infantry contact patrols. During its 8 months of operations, the Group also temporarily included the 50th and 88th Aero Squadrons.

Each squadron consisted of 18 pilots and 18 observers; all officers. The Group also had a Photographic Officer, responsible for installing cameras on the aircraft and overseeing development of photographs after the missions, and a Branch Intelligence Officer (BIO). The BIO, assigned by the American Expeditionary Forces (AEF) G-2, studied and interpreted the photographs and distributed all relevant information to higher commands. The Group also included a motorcycle courier who sped the photo plates from the aircraft to the lab. Once there, 30 enlisted technicians and specialists printed and enlarged the photos and got them in the hands of the BIO within 6 hours.

In the early days of aerial operations, weather and mechanical problems cancelled more missions than were actually flown, and many of the initial photographs had little intelligence value. Squadron personnel used their time in the relatively quiet sector to complete their training in preparation for more active operations. In addition to providing valuable training, the constant overwatch in the sector made it difficult for the enemy to prepare for large-scale attacks without the Allies' knowledge.

These quiet days in Toul ended in early July 1918 when the United States began large-scale military operations against the German lines. The 1st Corps Observation Group actively participated in the Aisne-Marne, St. Mihiel, and Meuse-Argonne offensives. Commanders who initially expressed skepticism about the value of aerial reconnaissance were now relying heavily on the discipline when planning operations. Weather permitting, aero squadrons flew daily dawn and twilight patrol missions and other missions as the tactical situation dictated. The BIO compared photographs from successive missions to identify changes in enemy battery positions, movement on roads and railways, and evidence of new works and troop concentrations. As the squadrons gained experience in actual combat conditions, they became more responsive to the needs of corps and division G-2s, and air-delivered timely "First Needs" packets of photographs directly to command posts.

As the war moved out of the trenches becoming more mobile, photographic reconnaissance became less important than artillery adjustment and infantry contact patrols. Because most of the observers were field artillery officers, they were attuned to and focused on meeting the requirements for artillery targeting. During contact patrols, aircrews kept the command informed of the location of its front line by flying low enough to mitigate issues of unfavorable weather while braving the dangers of both friendly

and enemy ground fire. Intensive collective training partially overcame communication issues between aircrews and infantry units, although the rapidly changing battlefield challenged even the best efforts at liaison.

In reviewing its efforts, the U.S. Air Service identified issues related to weather, air-to-ground communication, timeliness of photographic processing, and inadequate training that would need to be addressed in post-war developments. Still, the success of the Aero Squadrons cannot be overlooked. The Air Service understated the value of aerial visual and photographic reconnaissance as "satisfactory," while historians noted that it had become the primary information source influencing decision-making by the end of the war. General John J. Pershing, Commander of the AEF, concurred, stating, "No army ever went out with such information as to what was in front of it as the American Army did in St. Mihiel and in the Argonne." Clearly, aerial reconnaissance would continue to be a critical component of Army Intelligence operations.

Courier CPL Roland McFall receives plates from Observer, 1LT James B Harvey. At the end of the aerial photo mission, the motorcyclist waits to retrieve the glass photographic plates for speedy delivery to the photo lab for processing.

2018 Military Intelligence Corps Awards Nomination Period Announcement

LTG SIDNEY T. WEINSTEIN AWARD FOR EXCELLENCE IN MILITARY INTELLIGENCE

Nominations are being accepted for the 2018 Weinstein Award through 2 March 2018. To be eligible, a candidate must be a military intelligence officer of the rank of Captain (CPT/O-3) in the Active Army, Army Reserve, or Army National Guard. He/she must have performed actions, which positively promote, impact, advance, and bring honor to the MI profession during the period 1 January–31 December 2017. The candidate must possess either an MI Officer Area of Concentration (AOC) or a 15C/35 AOC, be fully eligible for continued service for at least one year after award presentation (i.e. through June 2019), and not be in a promotable status at the time of nomination submission. No posthumous awards will be presented. Candidates also must meet the height and weight standards specified in AR 600-9, maintain a current passing grade on the Army Physical Fitness Test (waived for deployed nominees unable to take the APFT), and must not be under an unfavorable personnel or UCMJ action.

CW5 REX A. WILLIAMS AWARD FOR EXCELLENCE IN MILITARY INTELLIGENCE

Nominations are being accepted for the 2018 Williams Award through 2 March 2018. To be eligible, a candidate must be a military intelligence company grade Warrant Officer (WO1-CW2) in the Active Army, Army Reserve, or Army National Guard. The candidate must have performed actions during his/her career, which positively promotes, impacts, advances, and brings honor to the MI profession. The candidate must possess an MI Warrant Officer MOS and be fully eligible for continued service for at least one year after award presentation (i.e. through June 2019). No posthumous awards will be presented. Candidates also must meet the height and weight standards specified in AR 600-9, maintain a current passing grade on the Army Physical Fitness Test (waived for deployed nominees unable to take the APFT), and must not be under an unfavorable personnel or UCMJ action.

CSM DOUG RUSSELL AWARD FOR EXCELLENCE IN MILITARY INTELLIGENCE

Nominations are being accepted for the 2018 Russell Award through 2 March 2018. To be eligible, a candidate must be a Soldier in the grade of Sergeant (E5) or below in the Active Army, Army Reserve, or Army National Guard. He/she must have performed actions, which directly contributed to the success of the MI Corps during the period 1 January–31 December 2017. The candidate must be fully eligible for continued service for at least one year after award presentation (i.e. through June 2019). No posthumous awards will be presented. Candidates also must meet the height and weight standards specified in AR 600-9, maintain a current passing grade on the Army Physical Fitness Test (waived for deployed nominees unable to take the APFT), and must not be under an unfavorable personnel or UCMJ action.

Recipients of these three awards are recognized annually at a luncheon during the MI Corps Hall of Fame Week in June at Fort Huachuca, Arizona.

Nominations for the awards must be received no later than 2 March 2018. Nominations should be emailed to lori.s.tagg.civ@mail.mil. You can also physically mail complete nomination packets to Command Historian, U.S. Army Intelligence Center of Excellence, 1889 Hatfield Street, Building 62723, Fort Huachuca, Arizona 85613-7000. For questions/assistance, or to obtain full nomination procedures, please contact Ms. Lori Tagg at (520) 533-4113/DSN 821-4113 or at the email above. You can also obtain the nomination procedures on the MI Corps Hall of Fame website: https://www.ikn.army.mil/apps/MIHOF/Home.

ATTN: MIPB (ATZS-CDI-DM)
BOX 2001
BLDG 51005
FORT HUACHUCA AZ 85613-7002

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

PIN: 202743-000