MI Professional Bulletin

July - September 2017
PB 34-17-3

Military Intelligence
Programs
United States Army
Intelligence Center of Excellence
National Intelligence University
1962
Command & Control ★ Sensors ★ Communications
CERDEC
Research • Development • Engineering Command
Intelligence & Information Warfare
National Geospatial-Intelligence Agency
National Security Agency
United States of America
United States Army
Intelligence and Security Command

Subscriptions: We have recently updated our distribution database. All organizations that were receiving copies of the publication should still be receiving at least one copy. If your organization has stopped receiving copies, please contact us so we can resolve the issue.

Free unit subscriptions are available by emailing MIPB at usarmy.huachuca.icoe.mbx.mipb@mail.mil
Include a complete mailing address.

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

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

Our mailing address: MIPB, USAICoE, Box 2001, Bldg. 51005, Ft. Huachuca, AZ, 85613.

Commanding General
MG Scott D. Berrier

Chief of Staff
COL Douglas R. Woodall

Chief Warrant Officer, MI Corps
CW5 Matthew R. Martin

Command Sergeant Major, MI Corps
CSM Thomas J. Latter

STAFF:

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

Associate Editor
Regina R. Pierre

Graphics and Layout Design
Gary V. Morris

Military Staff
CPT Robert D. Wickham
CW4 Julio A. Ovalle-Medellin

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
1712901

From the Editor

We would like to take this opportunity to sincerely thank our key advisors/contributors, LTC Andrew Pekala, MI Branch Chief, U.S. Army Human Resource Command and CPT Craig Porte, MI Branch Future Readiness Officer, U.S. Army Human Resource Command. Without their planning, identification of articles and authors, committed support, and other key contributions, this highly informative issue would not have been possible.

The following themes and deadlines are established for:

January–March 2018, Military Intelligence Capability Development, the focus for this issue will be on future systems and their fielding. Deadline for submissions is 28 September 2017.

April–June 2018, Leader Development, this issue will focus on developing leaders at all levels within the operational and institutional force. Deadline for submissions is 18 December 2017. This is a change from the previously published deadline of 3 December 2017.

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. This is a change from the previously published deadline of 4 March 2018.

As always, articles from you, our reader, remain important to the success of MIPB as a professional bulletin. Please continue to submit them, even if the topic of your article may differ from an issue's theme, do not hesitate to submit it. 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

Tracey Remus
Editor

MI Professional Bulletin

July - September 2017
PB 34-17-3
Volume 43 Number 3

34

50

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.

DEPARTMENTS

Always Out Front

by Major General Scott D. Berrier
Commanding General
U.S. Army Intelligence Center of Excellence

Part of what it takes to become a successful military intelligence (MI) leader is a strong desire to learn and technical background combined with challenging leadership, staff, and intelligence experience. It is essential for Army leaders to be diversified in their fields, have distinct specialties and skills, and have a strong work ethic to support the Army's number one priority—readiness. MI programs exist to support readiness by creating a cadre of talented, driven, and intellectually curious MI leaders who possess an enhanced understanding of the intelligence community to better answer commanders' intelligence requirements.

MI programs are a great way for officers, warrant officers, and noncommissioned officers (NCOs) to "broaden within MI." Broadening within MI means shifting participants off the more standardized MI training and assignment pipeline for a few years in order to concentrate in a unique and specialized sector of the intelligence community. These specialized focus areas allow them to receive unique training and gain incomparable experience from an array of different units and agencies across the Department of Defense.

This edition of MIPB provides MI professionals across the Army with the history of existing programs, a breakdown of each program, and discussion of the type of applicant who would be ideal for each. The U.S. Army Intelligence and Security Command, U.S. Army Human Resources Command, and the U.S. Army Intelligence Center of Excellence have done an excellent job over the years advertising and publicizing these programs, but unfortunately, there remains a bit of mystery and uncertainty regarding them. This quarter's MIPB unpacks each program, fully highlighting everything a potential candidate needs to know before applying.

From my experience as a "2" and an MI formation commander, I have found the most capable and competent MI officers and NCOs are those who have diversified their careers by serving in the most challenging positions, in different major commands, and supporting unique missions. The broader experiences of these leaders gives them a distinct advantage to peer through different lenses when problem solving, analyzing, and providing recommendations to decision makers. They have a strong grasp of friendly and enemy capabilities, and MI and maneuver doctrine. They have a concrete understanding of how the intelligence community, its agencies, assets, and people can help create a fully developed common operating picture. For these reasons and more, I am a strong believer in the merit and potential of our current MI programs. MI programs not only facilitate high-quality MI leaders becoming the master "sense makers" for their unit or agency leadership, but they challenge the participants to think more critically in real-world environments, ultimately making them better leaders and intelligence professionals.

In the civilian world, post-graduate degrees educate students as true experts in a given field. A master's degree in accounting or a juris doctorate prepares someone to become a certified public accountant or attorney, respectively. MI programs are designed to perform a similar function for Army intelligence. For example, the Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance Program is designed to be similar to a master's degree program for 35D, All-Source Intelligence Officers. The program sends officers to numerous ISR courses for approximately one year. The program participant then interns at various national-level ISR agencies and takes the tools and skills they've acquired to perform better as a 35D. The Junior Officer Cryptologic Career Program (JOCCP) and Warrant Officer Cryptologic Career Program (WOCCP) give officers advanced degree-level training and experience in signals intelligence. For NCOs, military occupational specialty 35G, Geospatial Intelligence Imagery Analysts, can participate in the GEOINT Career Advancement Program to receive advanced academic and on-the-job training in an internship, then PCS to a combatant command to work as a National Geospatial-Intelligence Agency liaison. The experience of NCOs, warrant officers, and officers before they start the programs coupled with the scope and real-world application of the programs, truly sets the individual up for success in the future.

The academic coursework and on-the-job training internships associated with each program are distinctly designed to make you a more technically proficient MI leader and professional. Additionally, MI program selectees are among the most competitive for promotion and selection for positions of higher authority. For example, 72 percent of eligible officer program graduates from year groups 1987 through 2000 were selected on the Central Selection List. These programs are, and will continue to be, successful as long as we have highly qualified officers and NCOs participating in them, who then take their experience and skills to improve intelligence operations within their future units. The application and selection process is further explained inside this issue.

The programs truly are "Win—Win—Win" for the Army, Army intelligence, and the individual. The Army and intelligence community receive high-caliber MI professionals and turn them into technically enhanced MI leaders who are ready to increase the proficiency of units and the readiness of the Army and MI Corps. For the individuals, these programs permit them to select an area that interests them greatly and provides them with an expertise and knowledge base they can leverage in future assignments.

Always Out Front – Army Strong!

CSM FORUM

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

Our Military Intelligence Creed states: "I am a Soldier first, but an intelligence professional second to none." The question is, How do you become that superior intelligence professional? Professionalization within intelligence requires more than "sets and reps" on what you already know, it requires deepening in your discipline, and broadening in the profession. To be a true professional you need to be a subject matter expert in your discipline, and yet fully understand all of the intelligence disciplines, how they support each other, and how to leverage them to "find, know, and never lose the enemy."

Many career-enhancing programs have been developed to support the depth and breadth needed to prepare intelligence professionals. Some of these provide a combination of training and work role assignments that occur over several years like the internships we have with national level agencies such as the National Security Agency (NSA) and the National Geospatial-Intelligence Agency. Others are degree producing like the bachelor's and master's programs at the National Intelligence University. So, when during your career should you apply for these programs?

In general, I recommend you attend the more technical programs earlier in your career—sergeant to staff sergeant. These career-enhancing programs provide the technical depth and broadening within the intelligence disciplines to become a subject matter expert. Attending them, as a junior noncommissioned officer (NCO), provides you the greatest opportunity to utilize the new skills you have developed throughout the rest of your career. In addition, for those contemplating becoming a warrant officer, these programs can make you more competitive for selection against your peers.

For the degree producing broadening education opportunities, I recommend you apply for the bachelor's programs as a staff sergeant, and the master's level opportunities as a sergeant first class or master sergeant. The education you receive, as well as, the joint learning environment, which encompasses expert faculty and diverse students from all intelligence disciplines, makes these programs excellent career-broadening experiences within intelligence. As you become a more senior NCO, understanding all of the intelligence disciplines and the entire intelligence community will help you not only as an intelligence professional, but also as a leader in Army and joint organizations.

Unfortunately, every year slots go unfilled in these special programs simply because no one applies for them. For instance, military occupational specialty 35Q, Cryptologic Network Warfare Specialist, has valid billets set aside in the Middle Enlisted Cryptologic Career Advancement Program at NSA that have gone unfilled for the past two years. You may have doubts whether you are the right individual for the Army to put into these programs. I recommend you put in your packet and allow someone with more experience determine if you are qualified for the program or at the right point in your career to participate or not. Additionally, leaders need to be identifying more junior NCOs in their formations who should attend these programs, and encourage and assist the ones with the most potential to apply.

Never stop learning in life. As an intelligence professional, take advantage of the career enhancing programs that are available to increase your subject matter expertise within your intelligence discipline and the broader intelligence community. Throughout this issue of MIPB, you will read articles about current programs. If you do not see a program mentioned that you think exists, contact your branch manager at the U.S. Army Human Resources Command or your Office of the Chief, Military Intelligence career manager and ask them about it.

Always Out Front!

Technical Perspective

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

The expectations of military intelligence (MI) warrant officers have never been greater than they are today. Our Army demands that we continue to be masters of our individual technical competencies. To complement those demands, senior leaders stress that our cohort develop capabilities to perform a wide variety of leadership, technical, and warfighting skills that transcend individual military occupational specialties. This requires warrant officers that are committed to maintaining high-level technical competence and are willing to take advantage of available learning opportunities to expand their skills and knowledge beyond the institutional training domain.

The current operating environment is replete with examples of why MI warrant officers must be more than technical experts. Today's warrant officers have the mental agility, physical toughness, and depth of knowledge to integrate across multiple echelons and organizations in a joint, interagency, intergovernmental, and multinational environment. Advanced technical and educational opportunities that increase individual understanding and provide a path towards expert knowledge to ensure success within complex and dynamic environments, are central to that goal.

Today's MI warrant officers are eligible for a wide range of educational opportunities that deepen and expand their knowledge while complimenting existing institutional education. These programs give select individuals the opportunity to explore unique challenges, learn advanced technical skills, and apply critical thinking and problem-solving within areas of concentration that expand warrant officer technical capabilities. Opportunities abound for those warrant officers who have proven themselves masters of their craft; ranging from strategic and national level intelligence support, advanced civil schooling, to working with White House officials and cabinet members. Our MI programs and educational opportunities represent a long-term investment in our very best technicians so they are well prepared to serve in the most demanding positions throughout the Army.

We must strive to go beyond what is learned through institutional training or on-the-job training and seek out unique and challenging programs that can provide the tools to solve some of the Army's most complex intelligence problems. MI programs provide an azimuth for our most highly qualified warrant officers to improve their technical and educational skillsets to support the Army and Department of Defense partners. The selection process for our professional development programs is extremely competitive, ensuring the participation of only the most highly qualified warrant officers. I would highly encourage each of you to take advantage of our MI programs with the intent of expanding professionally and personally.

Thanks for your enduring support and if you are interested in pursuing one of our existing MI programs please reach out to the U.S. Army Human Resource Command MI warrant officer assignment officers. Their contact information is available at https://www.hrc.army.mil/.

Always Out Front!

Army Intelligence 2017–2025:
Intelligence at the Speed of Mission Command

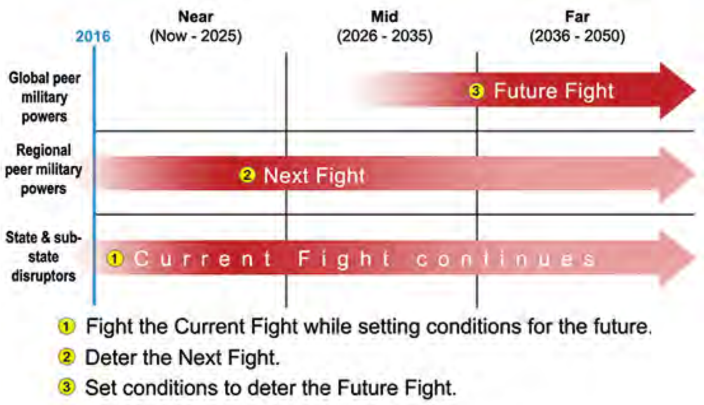
Editor's Note: The following article is an excerpt from a strategy booklet produced by LTG Robert P. Ashley, Jr., Department of the Army, Deputy Chief of Staff, G-2. For further information about this publication or other DA G-2 initiatives, please contact the G-2 Initiatives Group via email at usarmy.pentagon.hqda-dcs-g-2.dami-zxg@mail.mil.

A complete version of this strategy booklet can be downloaded from MIPB's IKN welcome page at https://www.ikn.army.mil/apps/MIPBW.

Introduction

Now more than ever, our Nation needs an Army Intelligence Corps that can enable mission command in an expeditionary, dispersed, and decentralized force operating in multiple domains. Central to meeting this challenge on both current and future battlefields is our ability to "integrate the national to tactical intelligence enterprise with multi-domain operations to provide a high degree of situational understanding across the range of military operations, while operating in complex environments against determined, adaptive enemy organizations." [1] We must see first, understand first, and report first, enabling timely and informed decision making and providing **intelligence at the speed of mission command.** This vision demands excellence in our core competencies—intelligence synchronization; intelligence operations; intelligence analysis; and intelligence processing, exploitation, and dissemination (PED).[2] We must synchronize our information collection and analysis efforts to generate situational understanding of our adversaries' intentions, discern key trends emerging within the operational environment, and enable our commanders with the decision space to place the enemy in a position of disadvantage for maximum effect.

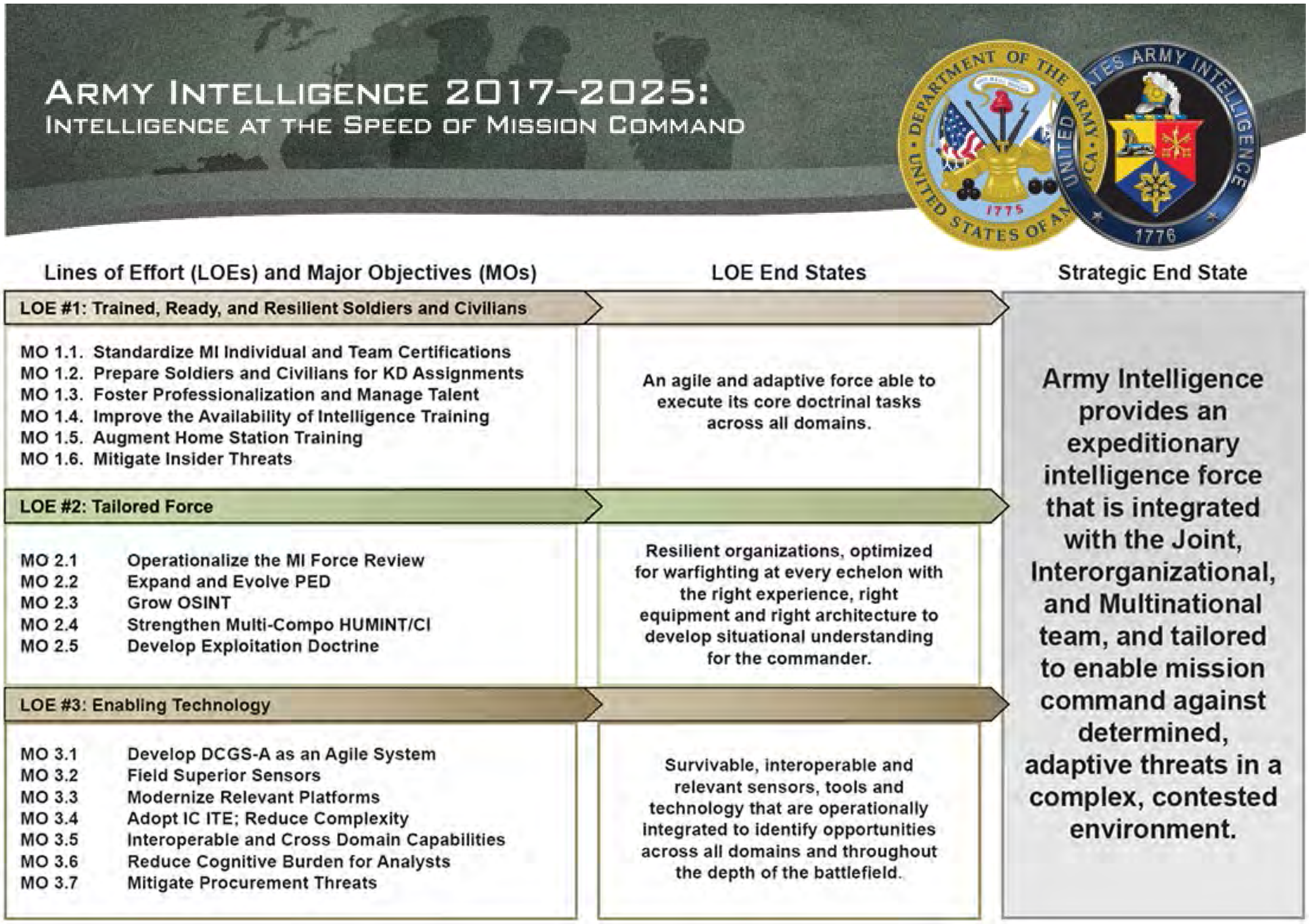
Success in these tasks has become increasingly difficult amid the global instability introduced by revisionist powers aggressively stretching the thresholds demarcating the boundary between measures short of war and high-order conflict. [3] Non-state actors further weaken the international system by leveraging technology and exploiting ineffective governance to attack and erode the authority of the state.


2016
Near
(Now - 2025)
Mid
(2026 - 2035)
Far
(2036 - 2050)
Global peer military powers
Regional peer military powers
State & sub-state disruptors
3 Future Fight
2 Next Fight
1 Current Fight continues
1 Fight the Current Fight while setting conditions for the future.
2 Deter the Next Fight.
3 Set conditions to deter the Future Fight.

Reference: The Army Strategic Plan

The simultaneous deterioration of U.S. Forces' comparative military advantage has notably exacerbated these conditions. We can no longer presume continuous superiority in any domain; our adversaries now possess the tactics and technologies necessary to contest our operations on land and in the air, sea, space, cyberspace domains, electromagnetic spectrum, information environment, and cognitive dimensions of warfare. Our Army must be able to fight state and sub-state disruptors in the *Current Fight* without mortgaging future force development, prepare to fight regional peer military powers in the *Next Fight*, and build options to counter the possible emergence of global peer military powers in the *Future Fight*.[4]

> *"Clearly, the next 25 years will not be like the last. The threats and missions we face today will endure well into the future, but they will be overshadowed by emerging great power competition. It seems likely that all forms of warfare will grow faster, deadlier, and more ambiguous while expanding into new physical and virtual domains."*
>
> – General Mark A. Milley, 39th Chief of Staff of the Army


Army Intelligence 2017–2025:
Intelligence at the Speed of Mission Command
Department of the Army
United States of America
1775
United States Army Intelligence
1776

Lines of Effort (LOEs) and Major Objectives (MOs)	LOE End States	Strategic End State
LOE #1: Trained, Ready, and Resilient Soldiers and Civilians		Army Intelligence provides an expeditionary intelligence force that is integrated with the Joint, Interorganizational, and Multinational team, and tailored to enable mission command against determined, adaptive threats in a complex, contested environment.
MO 1.1. Standardize MI Individual and Team Certifications MO 1.2. Prepare Soldiers and Civilians for KD Assignments MO 1.3. Foster Professionalization and Manage Talent MO 1.4. Improve the Availability of Intelligence Training MO 1.5. Augment Home Station Training MO 1.6. Mitigate Insider Threats	An agile and adaptive force able to execute its core doctrinal tasks across all domains.	
LOE #2: Tailored Force		
MO 2.1 Operationalize the MI Force Review MO 2.2 Expand and Evolve PED MO 2.3 Grow OSINT MO 2.4 Strengthen Multi-Compo HUMINT/CI MO 2.5 Develop Exploitation Doctrine	Resilient organizations, optimized for warfighting at every echelon with the right experience, right equipment and right architecture to develop situational understanding for the commander.	
LOE #3: Enabling Technology		
MO 3.1 Develop DCGS-A as an Agile System MO 3.2 Field Superior Sensors MO 3.3 Modernize Relevant Platforms MO 3.4 Adopt IC ITE; Reduce Complexity MO 3.5 Interoperable and Cross Domain Capabilities MO 3.6 Reduce Cognitive Burden for Analysts MO 3.7 Mitigate Procurement Threats	Survivable, interoperable and relevant sensors, tools and technology that are operationally integrated to identify opportunities across all domains and throughout the depth of the battlefield.	

In his initial message to the force, the 39th Chief of Staff of the Army (CSA) identified Readiness; the Future Army; and Taking Care of Soldiers, Civilians, and their Families as his framework for preparing the Army to meet these challenges. [5] These tenets serve as the foundation from which the Army will "fight and win the Nation's wars through prompt and sustained land combat, as part of the joint force." [6] Army Intelligence contributes to accomplishment of this mission by providing an **expeditionary intelligence force** that is **integrated with the Joint, Interorganizational, and Multinational (JIM) team,** and **tailored to enable mission command against determined, adaptive threats in a complex, contested environment.**

To that strategic end, this document orients the Total Army Intelligence Force (Active, National Guard, and Reserve Forces) along three Lines of Effort (LOE):

LOE #1: Trained, Ready, and Resilient Soldiers and Civilians

LOE #2: Tailored Force

LOE #3: Enabling Technology

Subordinate to these LOEs are a number of Major Objectives (MOs), focused on how we fight; how we organize to fight; what we fight with; how we build readiness; and how we recruit, develop, and train people for the fight. Each MO clearly defines the decisive effects needed to achieve the LOE end state. Given their enduring nature, MOs are included here and reviewed every 2 years. Subordinate to each MO are a number of specific, prescriptive, and organizationally assigned tasks that directly contribute to the accomplishment of the MO. These tasks are inherently temporal and therefore must be assessed frequently. They can be found in the Total Army Intelligence Campaign Plan, which supports the Army Campaign Plan and undergoes assessment and validation annually.

It is important to note that our Army will always operate under resource constraints. As senior Army leaders contend with fiscal uncertainty in the planning, programming, and budgeting system, we must assume that Army Intelligence will not be given all of the resources required to fulfill every aspect of this strategy. We will manage this risk by both prioritizing and synchronizing the pursuit of our objectives, starting with the three LOE. These LOEs nest

with the CSA's priorities and, along with their subordinate MOs, are purposely identified in priority order. First, our most critical mission is generating readiness for the current fight; we must build trained and ready Soldiers and Civilians that are prepared to fight and win. Second, we must organize for the next fight by evolving existing intelligence force structure and platforms to best counter the threats of 2025 and beyond. Third, we must prepare for the future fight by innovating technical and tactical solutions that will ensure U.S. superiority in a multi-domain battle. This strategy provides the lens through which we examine requirements, allocate effort and investments, and assess progress. Diligent, disciplined adherence to this strategy will ensure that Army Intelligence is postured to support commanders today, tomorrow, and into the future.

"The Army must also anticipate changing conditions and focus readiness efforts on staffing, equipping, training, and developing Soldiers in advance of the day's fight. No American Soldier will ever go to combat unready for the brutal and unforgiving environment that is ground warfare. We must guarantee the American public that our Soldiers and our Army remain ready to answer the Nation's call."

– Sergeant Major of the Army Daniel A. Dailey, 15th Sergeant Major of the *Army*

Army Green Book 2016-17, October 2016

Endnotes

[1] U.S. Department of the Army Training and Doctrinal Command (TRADOC), TRADOC Pamphlet 525-2-1, The U.S. Army Functional Concept for Intelligence 2020-2040 (Fort Eustis, VA: U.S. Department of the Army, January 25, 2017)

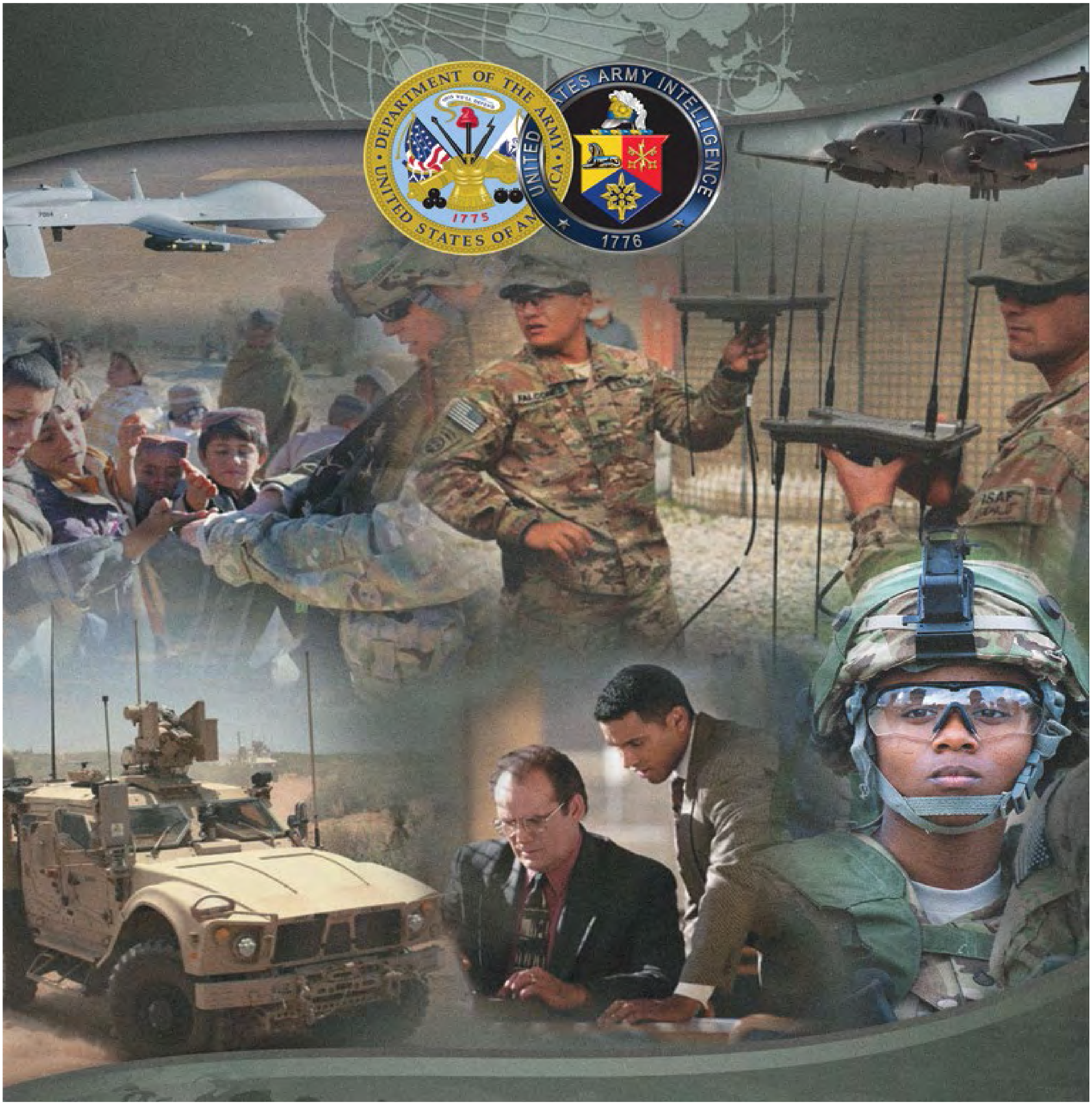
[2] U.S. Department of the Army, Army Doctrinal Publication 2-0, Intelligence (Washington DC: U.S. Department of the Army, August 31, 2012), 6.

[3] See Ben Connable, Jason H. Campbell, Dan Madden, Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War (Santa Monica, CA: RAND Corporation, 2016) for detailed discussion of measures short of war and high-order conflict. Examples of such behaviors include disinformation campaigns, proxy force operations, and illegal incursions violating national sovereignty.

[4] Headquarters, Department of the Army, The Army Campaign Plan 2017 (Washington, DC: U.S. Department of the Army, January 23, 2017), 5-7.

[5] 39th Chief of Staff of the Army, GEN Mark A. Milley, Initial Message to the Army, August 2015.

[6] U.S. Department of the Army, Army Doctrinal Publication 1, The Army (Washington, DC: U.S. Department of the Army, November 7, 2012), 1-8.



Human Resources Command: Military Intelligence Programs Overview

Military Intelligence Programs: Fashioning Technically Proficient Intelligence Leaders

by Captain Craig M. Porte

What are Military Intelligence Programs?

Military intelligence (MI) programs provide professional development opportunities to produce a cadre of intelligence leaders with the management skills and enhanced technical proficiency to harness the intelligence enterprise in future leadership positions within the intelligence community. MI programs are designed to select the MI Corps' most qualified officers and enlisted personnel and broaden their expertise through an MI internship and then utilize their freshly honed knowledge, skills, and abilities in a real world environment. MI programs are a critical component of the MI Corps' deliberate effort to prepare our best-qualified personnel to be future leaders of the MI Corps and support Army readiness by exposing them to resources and experiences they can harness throughout the rest of their careers.

There are many broadening opportunities available to MI officers; however, MI programs are distinct from other broadening opportunity programs as they broaden MI officers *within* MI—thus preparing them to serve as superior S-2s, G-2s, executive officers, S-3s, commanders, and in other key leadership positions. During the fiscal year 2016 Command Selection List (CSL) Board, MI program graduates were 28 percent more likely to be selected than nongraduates were. Additionally, 67 percent of MI lieutenant colonels who participated in MI programs were selected for promotion in the primary zone during the fiscal year 2016 Colonel Promotion Selection Board. This is primarily due to the quality of officers selected for MI programs, and these graduates' efforts to enhance aquired skills and maintain their high level of performance leading up to their boards and selection for command or colonel. MI programs directly support Army readiness, and participating in these programs enhances MI officers' careers and promotions. This article will examine what MI programs are, how to apply, and how the programs selection process works.

MI Programs Overview

There are currently ten MI programs. Last year the Junior Officer Geospatial Intelligence (GEOINT) Program was added and MI Branch anticipates continued growth of these programs with the inclusion of the National Intelligence University (NIU) this year.

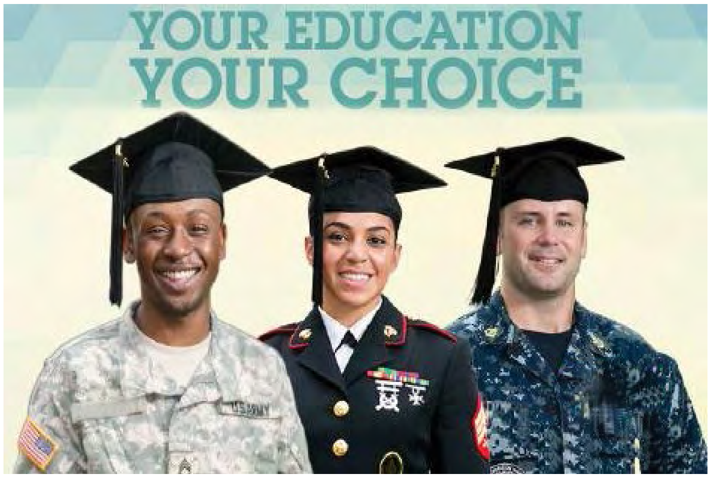
- ✦ Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance (AIDP-ISR) is a one-year internship followed by a two year utilization tour in U.S. Army Forces Command (FORSCOM). The program is designed to produce division and corps collection managers (key developmental for majors) who can leverage the intelligence community in support of unified land operations. Upon successful completion of this program, officers are awarded the additional skill identifier (ASI) 3F.
- ✦ Army Intelligence Development Program–Counterintelligence (AIDP-CI) is a two-year internship that develops an officer's counterintelligence management skills in preparation for leadership roles in counterintelligence assignments. Selected officers are assigned to the 902nd MI Group for their internship and are prepared to go on to serve in key developmental positions in U.S. Army Intelligence and Security Command (INSCOM), FORSCOM, and across the Army.

- Army Intelligence Development Program–Cyber (AIDP-Cyber) is a two-year program focused on a mix of military and industry-standard training with multiple opportunities to serve within the National Security Agency and U.S. Cyber Command. Selected officers are assigned to the 780th MI Brigade for their internship.
- Junior Officer Cryptologic Career Program (JOCCP) and Warrant Officer Cryptologic Career Program (WOCCP) are three-year internships formulated to increase leaders' knowledge of the signals intelligence (SIGINT) enterprise and develop experts who can leverage national SIGINT assets. Officers selected for JOCCP/WOCCP are assigned to the 704th MI Brigade for the duration of the program. Upon successful completion of this program, officers are awarded ASI 3W.
- Junior Officer GEOINT Program (JOGP) is a three-year internship to learn GEOINT and management skills through a combination of on-the-job work experience with National Geospatial-Intelligence Agency (NGA) analysts and mentors, and National GEOINT College course work. Officers selected for JOGP are assigned to the Army GEOINT Battalion at the NGA Campus East in Springfield, Virginia for the duration of the program.
- U.S. Army Intelligence Center of Excellence (USAICoE)–Communications-Electronics Research Development and Engineering Center (CERDEC) Program is a three-year program designed to educate and produce a cadre of MI professionals familiar with the Army's science and technology process, and capable of connecting those efforts into the Army's long range intelligence investment strategy. Selected officers are assigned to USAICoE at Fort Huachuca, Arizona, with duty at CERDEC, Aberdeen Proving Ground, Maryland, for the first year of the program and spend the second and third year at Fort Huachuca, Arizona.
- National Security Agency/Central Security Service (NSA/CSS) Director's Fellowship Program provides one MI lieutenant colonel, promotable major, or major with high-level exposure to current management, operations, and resource issues affecting NSA/CSS, and provides an opportunity to observe decision-making processes at the highest echelon. Officers who complete the NSA/CSS fellowship will serve a 12-24 month utilization assignment to apply their newly acquired skills within the SIGINT enterprise.
- The National Intelligence University is the intelligence community's sole accredited, federal degree-granting institution, and provides officers with an opportunity to spend one year in the national capital region earning a master of science in strategic intelligence or a master of science and technology in intelligence. NIU's primary role is to educate future intelligence and national security leaders in the intelligence profession. Officers, warrant officers, and enlisted personnel can apply to NIU. Further details can be found at http://ni-u.edu.
- Advanced Civil Schooling (ACS) consists of a fully-funded graduate program to provide Army officers academic education, prepare them to face unforeseen challenges, and groom the officers for positions where advanced civilian schooling is essential for optimum performance of their duties. While considered an Army broadening opportunity program, MI officers and warrant officers are selected for ACS by the MI programs panel and not the broadening opportunity program panel.

Applying for Military Intelligence Programs—A Simple Process

There is one panel and one process to applying for all of the MI programs. The MI programs military personnel (MILPER) message published annually by U.S. Army Human Resource Command (HRC) is the best resource to determine eligibility for a particular MI program. However, once eligibility is determined, the only document required for the board to consider selection is a DA Form 4187 endorsed by the first O-6 in the chain of command. Ensure you indicate to which program(s) you are applying. Additional guidance is available in the MILPER message. Additionally, officers may submit letters of recommendation with the DA Form 4187, but this is not required. Please do not include any medical or personally identifiable information in any letter of recommendation, since letters including any such information will not be submitted to the MI programs panel.

Who May Apply and When? The following are the programs for MI officers and warrant officers that have been included



in this year's MI programs MILPER message and which Active Component MI officer cohort year groups (CYG) may apply. All applicants must be deployable and must not be flagged or pending adverse action.

- **AIDP–ISR:** CYG 2008 and 2009.
- **AIDP–CI:** Open to CYG 2009. Previous counterintelligence experience or completion of the Counterintelligence Officer Course is desirable, but not required.
- **AIDP–Cyber:** Key developmental (KD) complete CYG 2009 officers.
- **JOCCP:** KD complete and professional military education (PME) complete CYG 2010 and 2011 officers.
- **WOCCP:** 352-Series CW2 or CW3s with less than one-year time in grade and are Warrant Officer Advanced Course (WOAC) complete at the beginning of the internship program.
- **JOGP:** Open to CYG 2009. Previous GEOINT experience or completion of the S1-ID course is desirable, but not required.
- **USAICoE—CERDEC Program:**
  - KD and PME complete CYG 2011 CPTs.
  - KD complete CYG 2003 MAJs.
  - Intermediate level education complete CW3s and Warrant Officer Senior Staff Course complete CW4s in military occupational specialties:
    - 350F, All-Source Intelligence Technician.
    - 350G, Geospatial Intelligence Imagery Technician.
    - 352N, Signals Intelligence Analysis Technician.
    - 352S, Signals Collection Technician.
    - 353T, MI Systems Maintenance/Integration Technician.
- **NSA/CSS Director's Fellowship Program:** Open to all MAJ, MAJ (P), and LTC that are KD complete and grade equivalent-PME complete.
- **NIU:** Open to grade-appropriate, PME complete—
  - CYG 2009 CPTs (Captains Career Course).
  - CYG 2004 MAJs (Intermediate Level Education).
  - CW2s (Warrant Officer Advanced Course).
  - CW3s (Warrant Officer Intermediate Level Education).
  - CW4s (Warrant Officer Senior Service College).

Also, desirable is excellent writing ability and use of grammar; superior Graduate Record Exam scores, a master's degree; potential for future, long-term service; and study in an academic discipline that will support the career field.

Photo by Daniela Vestal, U.S. Army Human Resources Command

- **Advanced Civil Schooling:** While ACS is not an MI program, the MI programs panel selects eligible officers for ACS alongside officers selected for MI programs. ACS is open to grade-appropriate, PME complete—
  - CYG 2009 CPTs (Captains Career Course).
  - CYG 2004 MAJs (Intermediate Level Education).
  - CW2s (Warrant Officer Advanced Course).
  - CW3s (Warrant Officer Intermediate Level Education).
  - CW4s (Warrant Officer Senior Service College).

Also, desirable is excellent writing ability and use of grammar; superior Graduate Record Exam scores; potential for future, long-term service; and study in an academic discipline that will support the career field. Officers who have already received a federally funded degree (such as GRADSO) or previous ACS, or seek a degree in a subject in which they already have a degree, will not be eligible for ACS.

JOCCP, WOCCP, JOGP, AIDP-Cyber, AIDP-CI, and USAICoE—CERDEC all have a six-year Active Duty service obligation (ADSO). AIDP-ISR and NSA/CSS Director's Fellowship Program have a three-year ADSO. Officers who attend ACS, acquire three days of ADSO for each day in school upon completion of schooling.

MI Programs Process Timeline

Each year, the MI programs process (Figure 1, next page) kicks off with the release of the MI programs' MILPER message, which typically occurs in April. This message provides everything needed to apply for MI programs during that specific year. The MILPER message does change from year to year and is the authority for MI programs. Completed applications may be submitted to your assignment officer at MI Branch no later than the deadline indicated in the MILPER message for consideration in that year's MI program panel. Typically, the deadline is the last day of July.

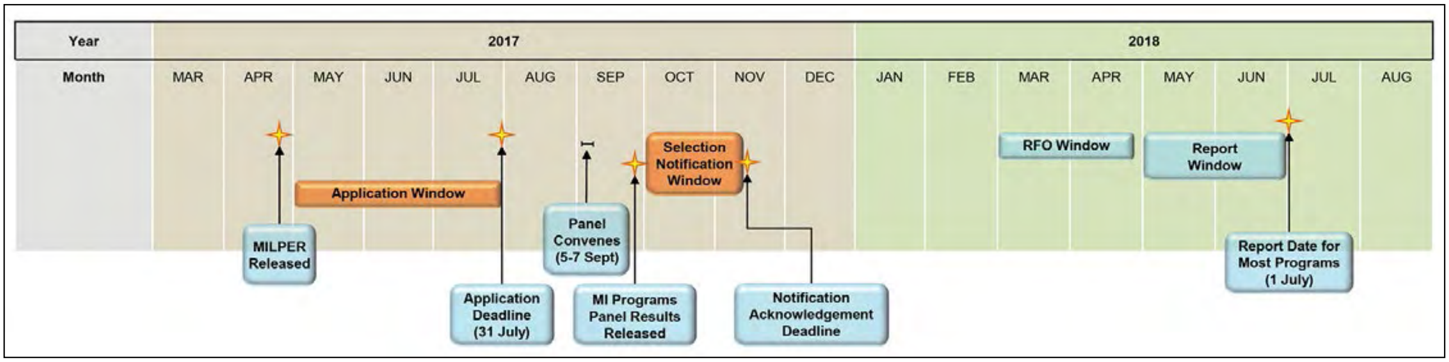

Year
2017
2018
Month
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
Application Window
Selection Notification Window
RFO Window
Report Window
MILPER Released
Panel Convenes (5-7 Sept)
Application Deadline (31 July)
MI Programs Panel Results Released
Notification Acknowledgement Deadline
Report Date for Most Programs (1 July)

Figure 1. MI Programs Application and Panel Timeline.

All applications are vetted to ensure they are correct, complete, and compliant with the guidance in the MILPER message, including performance and CYG eligibility. Applications meeting all criteria are consolidated and directed to Department of the Army Secretariat, which is the proponent for the conduct of all centralized selection boards, and the MI programs panel. DA Secretariat imports the files into an automated system that displays the considered officer's records (evaluation reports, awards, letters of recommendation, etc.) for the panel members to review and score the officers' files. See Figure 2 on the next page for an idea of what the entire panel process looks like. An important note to keep in mind is supporting documents seen by the panel are pulled from iPERMS the morning the panel convenes.

MI programs panel results will be released before the end of each fiscal year to enable units to project losses for the next summer's manning cycle. Individuals receive notification of their selection to a specific program and they must indicate whether they will accept selection before the deadline (typically, this is mid-November). Officers selected as alternates, should also respond to their selection so they can activate if primary selectees decline or can no longer attend programs. Officers who decline an MI program must re-apply to compete in future program panels.

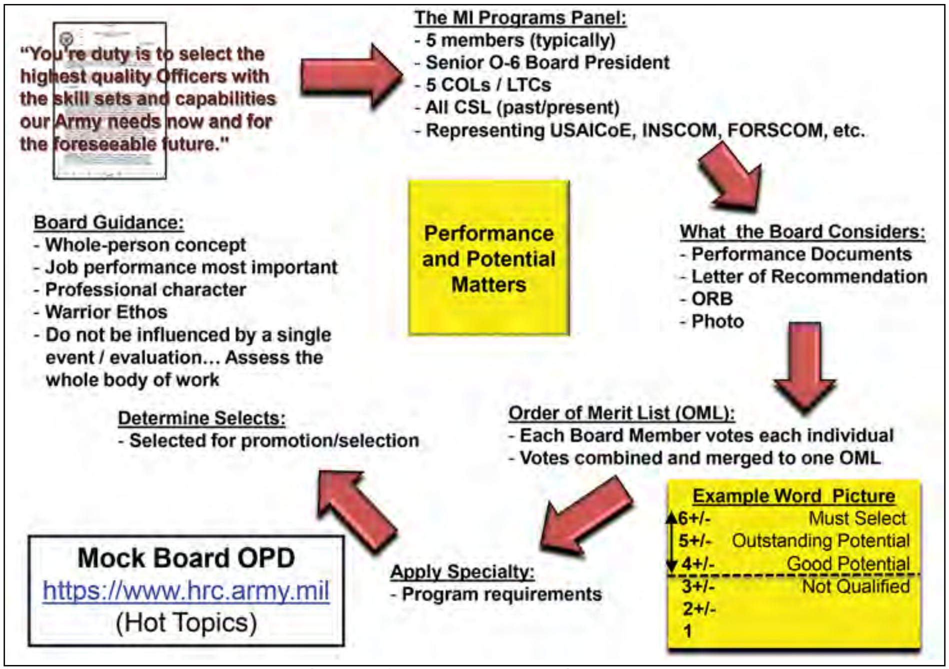
Upon consolidation of all selectee responses, officers will be enrolled in the next summer manning cycle and can expect to receive their request for orders beginning in March or about 90 to 120 days from their report dates. Most programs have a report date of 1 July of the following year and early report is generally authorized similar to most other permanent change of station moves.

How the Military Intelligence Programs Panel Selects Candidates

The MI programs selection panel utilizes senior Army leaders to nominate and then select officers for the programs. Although the panel does have the ability to review classified documents, this process is not secretive. Rather the panel conducts processes in the same manner as promotion selection boards or separation boards. A mock board that demonstrates the board process can be viewed at the following website address: https://www.youtube.com/watch?v=A4uJuwh40A0.[1] *The key factor in selection of candidates for MI programs is the collective performance and potential of the officer as described in the senior rater comments.*

Senior leaders from USAICoE, INSCOM, FORSCOM, and other organizations serve on a special duty assignment as a panel member. They travel to Fort Knox, Kentucky, for the selection panel, located at HRC. Panel members receive guidance through a memorandum of instruction and a mission to select officers to meet the needs of the Army and MI Corps. At least five panel members are required; however, depending on the panel's mission (i.e., number of applicants considered) there can be up to 22 members. However, most panels consist of five members. This is due to the small number of candidates who are eligible and competitive for MI programs.

Over the past five years, MI programs have averaged about 80 candidates each year, and of those, an average of 24 are selected—a 30 percent selection rate. Last year, there were 77 applicants and 29 were selected for a program—a 37.6 percent selection rate. Last year's panel did not fill all of the programs authorization—29 of 32 filled. This was quite simply due to a lack of file competitiveness. Many candidates were eliminated because they did not possess files strong enough for any MI program. Other officers had strong files, but they did not apply to all programs that they were eligible for, so more qualified officers in programs they applied for overshadowed their files. They would have been competitive for those other programs had they applied for them. Strong applicants were passed over because of their file competitiveness relative to the smaller pool they elected to compete in. Historical analysis does not reveal any one program consistently more popular than any other (although, generally, the older a program is the more applicants tend to know about it). Rather, program



"You're duty is to select the highest quality Officers with the skill sets and capabilities our Army needs now and for the foreseeable future."

The MI Programs Panel:
- 5 members (typically)
- Senior O-6 Board President
- 5 COLs / LTCs
- All CSL (past/present)
- Representing USAICoE, INSCOM, FORSCOM, etc.

Performance and Potential Matters

What the Board Considers:
- Performance Documents
- Letter of Recommendation
- ORB
- Photo

Board Guidance:
- Whole-person concept
- Job performance most important
- Professional character
- Warrior Ethos
- Do not be influenced by a single event / evaluation... Assess the whole body of work

Order of Merit List (OML):
- Each Board Member votes each individual
- Votes combined and merged to one OML

Determine Selects:
- Selected for promotion/selection

Example Word Picture

6+/-	Must Select
5+/-	Outstanding Potential
4+/-	Good Potential
3+/-	Not Qualified
2+/-	
1	

Apply Specialty:
- Program requirements

Mock Board OPD
https://www.hrc.army.mil
(Hot Topics)

Figure 2. The MI Programs Panel Process.

competitiveness fluctuates from year to year as dictated by the preferences of those who applied that year. Therefore, we recommend applying to all programs for which one is eligible and rank ordering them in your application. The key factor in section of candidates for programs remains performance and potential, but you can increase your odds of selection.

Panel members do not discuss files or share their individual voter philosophies. They must decide for themselves how to score each officer. However, feedback from panel members consistently indicates that performance, especially in multiple key development positions, and potential are considered first, and then panel members consider the guidance provided in the memorandum of instruction—including the applicant's civilian academic performance, degree concentration, Graduate Record Exam scores (if applicable), and letters of recommendations.

The important thing to take away from this is that everyone in the considered population is represented, panel members are prohibited from communicating about officers' files, and MI Branch has no direct input into the panel's selection process.

Appeals Process

The Army Board for Correction of Military Records, DA Pam 623-3, *Evaluation Reporting System*, and AR Regulation 623-3, *Evaluation Reporting System* outline appeals to correct material error in an individual's military record. The MI programs panel mirrors selection and separation boards in that appeals are limited to newly discovered evidence, the subsequent removal of documents from the Soldier's Army Military Human Resources Record (AMHRR), or material error in the AMHRR when reviewed by the panel. Appeals that do not meet these criteria receive disapproval by HRC and the panel's selection will stand. Appeals that meet these criteria will be forwarded to the next panel for review.

The Way Ahead

The MI programs discussed here have grown over the years. Programs that enhance technical proficiency and management skills, prepare participants to excel in future leadership positions within the MI Corps, and require the selection of the highest quality officers and enlisted are some of the key criteria of what constitutes MI programs. MI Branch continuously evaluates existing programs and makes recommendations to the Office of the Chief, MI (OCMI) for inclusions into MI programs, to ensure support to the MI Corps and Army readiness. If you are the proponent of a program you believe meets this criteria, we encourage you to reach out to MI Branch or OCMI to have your program considered for addition to the Army's official MI programs.

Military Intelligence Enlisted Branch Programs Process and Considerations

by Lieutenant Colonel Daniel D. Jones

The MI Corps has numerous opportunities for professional development in a variety of Army programs to enhance a Soldiers career. For most programs, there is an associated military personnel message that details prerequisites for each course including items such as prescribed civilian education, professional experience, and overall performance record. The Enlisted MI Branch at HRC reviews all submitted packets for each of the individual programs. Records are scrutinized to ensure that all criteria is met, in accordance with each separate program requirements, and to ensure that the Service Member is fully eligible to move on a permanent change of station. Each program has a limited number of authorized billets, which makes selection to attend very competitive. Soldiers that meet the prerequisites and have the strongest quality of file are prioritized against available training/program seats. Overall manner of performance is assessed based on historical evaluations—both performance and academic. Packets are reviewed, prioritized, and provided to internal branch leadership for concurrence. Once the list is finalized, the packets are provided to the program managers and Soldiers are placed on assignment requisitions. Key factors that Soldiers must consider are—

- ✦ Do they meet the MOS/Skill Level requirement as prescribed for the program?
- ✦ Have they served (or will they) 24 months' time on station at their current duty station by the projected program start date?
- ✦ Have they met their gates for promotion in their current rank by fulfilling commensurate leadership positions as prescribed by DA Pam 600-25, *U.S. Army Noncommissioned Officer Professional Development Guide* (e.g., section sergeant, squad leader, platoon sergeant)?
- ✦ Do recent performance and academic evaluation reports demonstrate a consistent strong manner of performance?
- ✦ Does the current command support the application?
- ✦ Are there any administrative issues for clearance (e.g., Exceptional Family Member Program, Married Army Couples Program)?

This process works to ensure that we provide the best available candidates to participate in approved Army programs.

Endnote

[1] *Exportable Mock Board*. U.S. Army Human Resource Command. YouTube. April 28, 2015. This video is a mock board on the Department of the Army Centralized Selection Board process.

CPT(P) Porte is the U.S. Army Human Resources Command, Officer Military Intelligence Branch, Future Readiness Officer. He previously served in light and airborne infantry units as a maneuver battalion intelligence officer-in-charge, military intelligence company commander, security force assistance advisor in Eastern Afghanistan, and observer/controller trainer at the Joint Readiness Training Center.

LTC Jones is the U.S. Army Human Resources Command, Enlisted Military Intelligence Branch Chief.

TRADOC
CULTURE CENTER

Mission Statement: Established in 2004, TCC provides relevant and accredited cultural competency training and education to Soldiers and DA Civilians in order to build and sustain an Army with the right blend of cultural competency capabilities to facilitate a wide range of operations, now and in the future.

Request training through ATRRS
Course Number:
9E-F36/920-F30 (CT-MTT)

TRAINING AND EDUCATION

Available Training: The TCC provides training and education in cross-cultural competence skills, regional expertise, and functional topics in support of the CJCSI 3126.01A Culture, Regional Expertise, and Language (CREL) competency factors at the basic or fully proficient levels. The course is tailored to meet the requesting unit's cultural competence requirements in these areas.

Cross-Cultural Competence Skills Topics:

- What is Culture?
- Cross-Cultural Communication
- Cross-Cultural Negotiation
- Cross-Cultural Rapport Building
- Self-awareness and Perspective-taking

culture matters

Regional Expertise:

- AFRICOM, CENTCOM, EUCOM, NORTHCOM, PACOM, SOUTHCOM
- Smart Cards and Smart Books are also available

Functional Topics:

- Key Leader Engagement
- Culture and Female Engagement Teams

Primary Training Focus:

- OEF Pre-Deployment Training
- Regionally Aligned Forces
- Train-the-Trainer events
- Advanced Specialty Training

"Like" us on facebook

Search: TRADOC Culture Center

http://www.facebook.com/pages/TRADOC-Culture-Center/135051471239990

Army Intelligence Development Program–Intelligence, Surveillance and Reconnaissance (AIDP-ISR): A Senior Leader Perspective

by Colonel Dwight L. DuQuesnay

Introduction

I first had the opportunity to work alongside Army Intelligence Development Program–Intelligence, Surveillance, and Reconnaissance (AIDP-ISR) graduates in 2008 while serving as the Deputy C-2 for Operations within the Multi-National Corps-Iraq (MNC-I). As part of my duties, I supervised the corps collection manager who was an AIDP-ISR graduate. We interfaced with select Multi-National Division (MND) collection managers who were AIDP-ISR graduates as well. Based on my experience working with these graduates, I became an ardent supporter of the program. As such, when selected to serve as Eighth Army Assistant Chief of Staff (ACofS) G-2, I fought to ensure we received AIDP-ISR graduates to act as our collection managers. I was not disappointed. They made significant contributions in Korea at the field army and division levels.

AIDP-ISR Contributions in Iraq—2008-2009

Multi-National Force-Iraq (MNF-I) and MNC-I ran a combined collection management section. An Air Force colonel, assigned to the MNF-I Combined Joint Staff Branch for Intelligence (CJ2), with the corps collection manager serving as his deputy, led the office. The combined collection management section was staffed by the corps modified table of organization and equipment (MTOE) collection management section; the MNF-I side was filled with joint manning document (JMD) billets. The section also had several liaison officers from operational units, such as Task Force ODIN, a Navy P3 Orion squadron, and JSTARS. The strength of the combined collection management section was approximately 30 personnel.

Strength. While staffing always seemed short, the joint nature of the combined collection management section was a strength. For example, Air Force personnel were intimately familiar with the operations of the Intelligence, Surveillance, and Reconnaissance Directorate (ISRD) within the Combined Air Operations Center (CAOC). In this environment, our AIDP-ISR graduate quickly learned how to integrate the combined forces air component command intelligence, surveillance, and reconnaissance (ISR) contribution with a combination of Army units (e.g., Task Force ODIN/U.S. Army Intelligence and Security Command aerial exploitation battalions) and contract platforms into a truly joint aerial ISR force.

Individual replacements filling JMD billets rotated in and out on a different schedule than the corps relief in place (RIP)/transfer of authority (TOA), which meant a higher level of continuity. The corps collection management section deployed with the corps analysis and control element, which had an offset RIP/TOA from the rest of the corps. This allowed the incoming team to serve under the leadership of the outgoing corps C-2 for several weeks, thereby preventing a cold start for the incoming team. In addition to the offset RIP/TOA for the corps collection manager, the AIDP-ISR program facilitated a two-week in theater orientation for students. As such, about three to four months before rotating in, the incoming collection manager would deploy forward for two weeks to conduct a right seat/left seat ride.

Photo by COL Dwight DuQuesnay

MNF-I CJ2 and the location of the combined MNF-I/MNC-I collection management section within the Perfume Place, Camp Slayer, Iraq.

ISR Planning. From the corps perspective, location was the combined collection management section's one drawback. The section was located at Camp Slayer in the Perfume Palace with the MNF-I CJ2 vice with the corps main in Al Faw Palace on Camp Victory. This prevented the corps collection manager from participating in some routine planning events, primarily on the future operations side. To compensate, the corps intelligence planners, all of whom were consolidated in the C-2 under my direction, picked up the slack on ISR planning to support operations. Operating split-based, the corps collection manager had wide latitude in the conduct of daily operations. Considering the challenges of combined collection management and split-based operations, having a strong school-trained officer as collection manager was an integral component of successful ISR support to the corps.

While the combined collection management section was led by MNF-I, all of the ISR allocation decisions were made by MNC-I. MNF-I played a key role in interfacing with the U.S. Central Command (CENTCOM), lobbying to retain assets in Iraq vice a CENTCOM reallocation to Afghanistan. MNF-I also played a key role in planning for the deployment of new capabilities to Iraq, for example, the deployment of the Air Force's Liberty aircraft.

MNF-I and MNC-I retained very little ISR (if any) at the force or corps level. MNC-I allocated ISR down to the Marine expeditionary force, MNDs, combined joint special operations task force, and other units. We allocated monthly 75 to 80 percent of the corps ISR to major subordinate commands, providing them with predictability. We referred to this allocation as corps direct support (DS). We retained the remaining 20-25 percent in corps "packages" as a surge capability, which we generally allocated weekly, depending on threat activity and ongoing operations. A small percentage of ISR was general support (GS) to the corps, based on the nature of the collection discipline (i.e., airborne signals intelligence [SIGINT] was generally kept in GS serving as a shaping effort in the corps-layered ISR strategy).

XVIII Airborne Corps, as the MNC-I headquarters, developed a system for visualizing ISR capability using three hours as the base block. Three hours was generally the minimum ISR sortie when looking at medium altitude fixed-wing platforms. Figure 1 is an example of the XVIII Airborne Corps system of allocating and visualizing ISR by capability blocks.

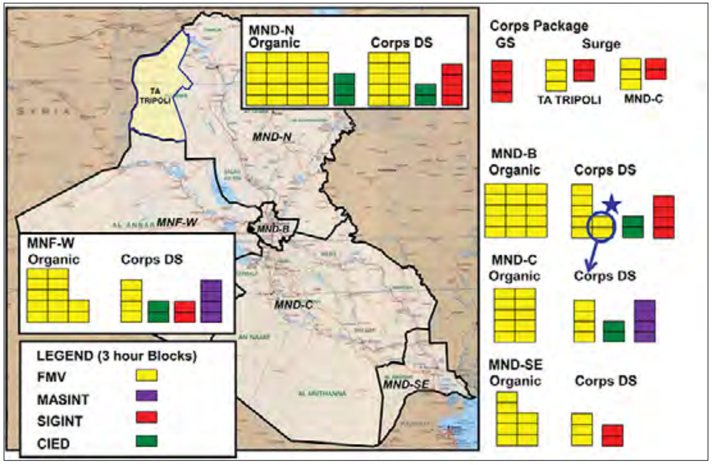


Figure 1. Airborne ISR – Visualization / Allocation.

The corps collection manager was responsible for maintaining these so-called "chicklet charts" and provided the operators with an easy-to-visualize snap shot of the ISR weight of effort. Figure 2 shows the corps collection layered ISR strategy—from wide-area search using airborne SIGINT and moving target indicator, down to find, fix, and finish using full motion video (FMV) and geo-location capabilities.

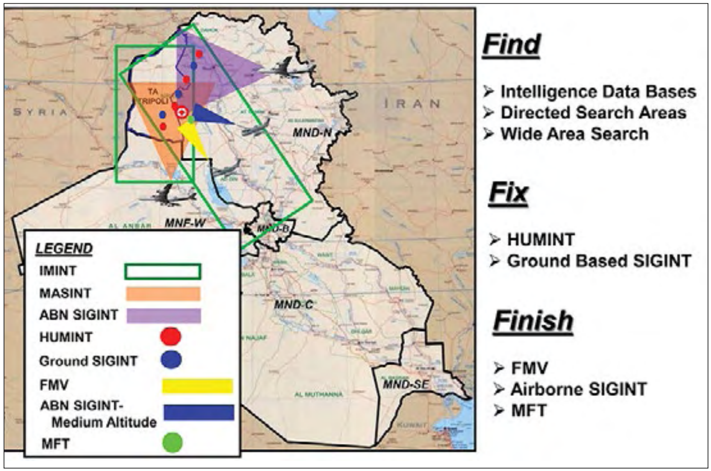


Figure 2. Layered ISR Strategy.

The corps system (layered strategy, visualization method, and allocation system) meant frequent allocation decision briefs to the corps C-3. As such, the corps collection manager kept detailed measures of performance and measures of effectiveness to support allocation recommendations. While the allocation of the battlefield surveillance brigade terrestrial assets (such as human intelligence collection teams, multifunction teams, and SIGINT teams) did not change often, their movements were briefed to the corps C-3, when necessary, in conjunction with the corps SIGINT advisor and/or corps C-2X.

In addition to the thorough assessment process and detailed allocation briefings, the corps collection manager fought ISR daily. This consisted primarily of dealing with schedule changes due to maintenance, weather, or CAOC re-allocations. The collection manager worked these changes primarily through the C-3 chief operations in conjunction with the C-2 operations. CAOC re-allocations occurred primarily during troops in contact (TIC). Based on fighter squadron redeployments from Iraq, the CAOC relied more on Predator and Reaper unmanned aircraft systems (UASs) for close air support (CAS). As such, a Predator allocated to a MND to execute an ISR operation might be pulled to respond to a TIC as a CAS asset.

In retrospect, the corps collection management team, working as part of the combined collection management section, was a well-oiled machine. The primary benefit of the AIDP-ISR program was getting the corps and division collection managers prepared and through the RIP/TOA. Given the significant requirements placed on the corps collection manager in terms of the daily fight, assessments, and frequent allocation decision briefs, the strong fundamentals instilled through the AIDP-ISR program were crucial to the success of this officer.

Collection Management Field-Lessons Learned/ Potential Solutions

After my experience in Iraq with MNC-I, I served as the Chief of Staff of the ISR Task Force in the Training and Doctrine Command at the U.S. Army Intelligence Center of Excellence and within the Office of the Undersecretary of Defense-Intelligence. Both organizations were looking to solve issues with collection management (primarily at the brigade combat team [BCT] and below level). Although establishing a collection management military occupational specialty (MOS) was a popular idea, career field experts knew that this would create a career field without a viable career path due in part to a lack of progression.

Interestingly, the Air Force does not have a collection management MOS. Its field expertise is based on its operational experience. Unfortunately, Army military intelligence (MI) officers may have limited opportunities operationally to employ ISR. An AIDP-ISR graduate, on the other hand, coming into a division or corps on an operational tour is set up for success as a BCT S-2, deputy G-2, and ultimately as a division G-2, much as our School of Advanced Military Studies graduates go on to do great things following their utilization tour. Of note, during discussions on collection management issues, participants recognized AIDP-ISR as a positive program that mitigated shortfalls at the division and corps levels. The Air Force ISR liaison program was also recognized for mitigating shortfalls at the tactical level.

AIDP-ISR Contributions in Korea—2014-2016

In 2014, I was assigned as the Eighth Army ACofS G-2, clearly a different environment than my C-2 days in Iraq. My collection manager, an AIDP-ISR graduate, was new to our team when I arrived. Although forward deployed, Eighth Army did not fight ISR daily. The Eighth Army Headquarters was driven by an exercise schedule, the Ulchi Focus Guardian (UFG) and the Key Resolve/Foal Eagle. The first three months of the tour were consumed by the UFG—the tradition of executing one of the biggest exercises of the year with all new people to immerse everyone in the war plan and build "fight tonight" readiness. However, upon completion of the exercise, one was easily distracted by the daily grind that was Korea. To quote a Korea maxim—it is what you get done between the two major exercises that defines your tour. As such, we set out to improve Army ISR operations in Korea.

Across the street from the Eighth Army Headquarters, the U.S. Forces Korea J-2 ISRD fought ISR daily, executing the target deck to support the warning intelligence mission. The 501st MI Brigade executed part of that deck along with the 7th Air Force and Air Force assets in Japan and Guam. By plugging into that system through daily battle rhythm events, such as J-2 intelligence briefs or combined operations and intelligence briefs, our young collection management team gained ISR operations' experience on the Korean Peninsula.

Further, we looked at collection requirements through the lens of the Eighth Army's countering weapons of mass destruction (WMD) mission. Our collection manager ensured key sites on the WMD master site list were covered to keep mission support folders on those sites up to date.

Most importantly, we looked at ISR operations and collection management through a combined lens. This included collaborating with the Republic of Korea (ROK) Field Armies and the 2nd Operational Command responsible for rear area security—key to Eighth Army's reception, staging, onward-movement and integration, and logistic missions. Our collection manager leveraged his AIDP-ISR experience to conduct classes on U.S. collection management doctrine (i.e., ATP 2-01, Plan Requirements and Assess Collection) and U.S. capabilities. The ROK Army was expanding its UAS fleet. As such, our ROK Army counterparts were interested in U.S. doctrine and tactics, techniques, and procedures associated with UAS training and employment.

Photo courtesy of COL Dwight DuQuesnay

Soldiers with the U.S. Eight Army G-2 Intelligence Plans/Intelligence, Surveillance, and Reconnaissance Team and Republic of Korea Soldiers at the ROK Military Intelligence School pause for a photo during combined tactical discussions, June 2016 (ROK BG **Moon first row fourth from left, Colonel DuQuesnay first row fifth from left).**

The ROK interest in UAS coincided nicely with UFG and Key Resolve. The Multiple Unified Simulation Environment (MUSE), which provided a FMV feed, was one of the more mature intelligence simulations. It lends itself well to training several aspects of UAS employment. Our collection manager's first task was to extend the architecture so we could better share UAS feeds with our ROK counterparts. This included Shadow, Gray Eagle, and 3rd MI Battalion's Airborne Reconnaissance Low.

The architecture for the MUSE feed was very archaic. It consisted of T-1 circuits from the simulation center to various U.S. and ROK headquarters using copper phone lines. In one incident, we could not receive the MUSE feed via circuit to the Eighth Army's operational command post field location due to the lack of copper telephone lines—despite a direct fiber connection to the site. A more realistic method of FMV dissemination during an exercise was through the Global Broadcasting System (GBS). However, GBS-receive suites were isolated to U.S. command posts and a couple of the combined forces command-level headquarters.

Establishing the intelligence architecture is a key step to success for the intelligence warfighting function. Lessons learned from decisive action training environment rotations at combat training centers expose the challenges of establishing an intelligence architecture, especially in an expeditionary environment. Architecture planning and execution are areas AIDP-ISR could probably improve. During my first experience working alongside an AIDP-ISR graduate, we fell in on an existing architecture, and our primary concern regarding the architecture was the maintenance and planning for the imminent deployment of the Liberty aircraft. Initially, in Eighth Army G-2, our collection manager was tasked with improving our intelligence architecture. Subsequently, it became a shared task between collection management and our systems section, which consisted of MOS 35Ts (MI Systems Maintainer/Integrator) and 25 series (Signal Corps) officers, warrant officers, and Soldiers.

Eventually, we were able to stream FMV feeds over the Combined Enterprise Regional Information Exchange System (CENTRIX). Although CENTRIX connectivity was limited in some ROK units, it enabled Eighth Army's partnership with First ROK Army, Third ROK Army, and the 2nd Operational Command. With the introduction of FMV feeds into those headquarters, came the requirement to provide collection management expertise and a rudimentary processing, exploitation, and dissemination (PED) capability. Providing personnel to support the integration of those feeds ensured ROK collection managers considered all collection capabilities. Bottom line, we did not want to create an over dependence on FMV in the form of "TOC TV." Unfortunately, some of the other capabilities provided "little bang for the buck" in simulation, so we were fighting an uphill battle.

Our collection manager supervised the integration of collection management and PED capability into the ROK headquarters. We invested heavily in his team; under his leadership, we built significant depth in collection management. There was a lot of prep work before major exercises, including PRISM training (Planning Tool for Resource Integration, Synchronization, and Management) for our people as well as our ROK counterparts, site surveys, etc.

Although our collection management section was relatively small (three officers and a couple enlisted Soldiers), our collection manager developed standard operating procedures, allowing for the efficient integration of augmentees from the Military Intelligence Reserve Command into major exercises. This augmentation of our operational command post allowed some of our key collection management leaders to spend time during an exercise embedded in one of the ROK headquarters. Additionally, we diverted Air Force ISR liaisons to those headquarters to provide their unique expertise.

Finally, a key task for our collection manager was to represent Eighth Army G-2 on the integrated planning team established between U.S. Forces Korea, the Eighth Army, and

Photo courtesy of COL Dwight DuQuesnay

Eighth Army Operational Command Post during the annual exercise Ulchi Focus Guardian, New Mexico Range, Republic of Korea, August 2014.

the Seventh Air Force in preparation for stationing the Gray Eagle in Korea. Eighth Army, as the Army Forces Korea, was tasked to develop a PED plan to support the deployment. The planning for Gray Eagle stationing was built on a successful proof of principle conducted by the 10th Mountain Division's Combat Aviation Brigade (CAB) in August of 2015. The 10th CAB deployed part of a Gray Eagle company to conduct live flight operations from Kunsan Airbase in the ROK, demonstrating manned-unmanned teaming operations in conjunction with the 2nd Infantry Division's CAB AH-64 Apaches.

In the end, our efforts to improve the Eighth Army ISR architecture and interoperability with our ROK partners were successful. Having a school-trained AIDP-ISR graduate as our collection manager facilitated those efforts. One of my last acts as the Eighth Army ACofS G-2 was finalizing the field grade slate. Fortunately, I was able to backfill our collection manager with another AIDP-ISR graduate who could build on our initiatives. It also provided that AIDP-ISR graduate with a utilization tour, an important component of the program.

Conclusion

The opportunity to supervise AIDP-ISR graduates in two separate environments has left me with a good appreciation for the AIDP-ISR program. I served as a division G-2 under a pre-modular MTOE. The division collection manager was a high-speed captain. There were two- to three-week long collection manager courses available, but at the division level, most learning occurred on the job. In retrospect, I believe two of the most important aspects of the AIDP-ISR program are selection and utilization. I came across both in the high-speed junior field grade officers I received. One came into a well-established system and was then "baptized by fire," gaining a ton of operational experience. The other learned more about building and improving an intelligence architecture, building and training a team, and improving interoperability with a close ally. In both cases, the Army and MI Corps were the winners, with field grade officers who truly knew how to fight ISR and move on to other key jobs. The skills an AIDP-ISR graduate refines during a utilization tour are the same skills we need in our S-2s/G-2s and J-2s.

COL Dwight DuQuesnay served as a brigade S-2 and division G-2 in the 2nd Infantry Division in Korea, and as the Eighth Army G-2 after its transition to a Field Army. He also served as a brigade S-2 and intelligence planner in the 10th Mountain Division. He has three combat training center assignments culminating as the senior intelligence officer for the Joint Readiness Training Center, Fort Polk, LA. Additionally, he served as Deputy Corps G-2 XVIII Airborne Corps / Deputy C-2 Multi-National Corps-Iraq. He culminated his career in May of 2017 after 30 years, serving as the Doctrine Director, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ.

The Army Intelligence Development Program–Counterintelligence

by Chief Warrant Officer 5 Traci A. Goodwin and Chief Warrant Officer 5 Michael D. Dye

Introduction

Army leaders at all levels emphasize readiness, professionalism, and ensuring Soldiers have all available tools at their disposal to effectively carry out the mission the Army entrusts them to conduct. Army counterintelligence (CI) has taken a step to increase readiness with a new initiative—the Army Intelligence Development Program–Counterintelligence (AIDP-CI). In June 2016, military personnel message 16-160 announced the first iteration of AIDP-CI. Established by the U.S. Army Intelligence and Security Command (INSCOM), Army Intelligence Development Programs intend to produce "qualified junior officers who understand how to bring national and theater intelligence systems to the fight—supporting warfighters at the corps and below level." More specifically for counterintelligence, the message states AIDP-CI "develops officer counterintelligence and management skills in preparation for leadership roles in CI assignments."

Army Regulation 381-20, *Army Counterintelligence Program*, directs Army CI to conduct aggressive, comprehensive, and coordinated activities worldwide in the five functional areas of—

- Investigations.
- Operations.
- Collection.
- Analysis and production.
- Technical services and support activities.

The efforts of CI activities through these functions are to detect, identify, assess and counter, neutralize, or exploit the foreign intelligence and international terrorist threat to the U.S. Army and Department of Defense, and to identify and counter the collection efforts and activities of any other foreign adversary which presents a threat to lives, property, or security of Army forces.

Program Background

The AIDP-CI program grew out of a need and desire for Army military intelligence (MI) officers to obtain the 35E, counterintelligence, area of concentration (AOC) and immediately put their training to work in the intelligence community. Previously, upon successful completion of the CI Officers Course (COIC), a large percentage of graduates never received a CI assignment. In other cases, CIOC graduates received relevant assignments much later in their careers, after years of skill atrophy. A major portion of this challenge stems from the number of CI officers in the Army compared with the number of authorized billets. This number is consistently at a ratio of more than two-to-one that creates a large population of CI officers trained to conduct the counterintelligence mission but with no available positions. Now, officers selected for the AIDP-CI program attend the CIOC and receive the 35E AOC then immediately immerse in additional CI training followed by a utilization tour in a CI assignment.

There were previous efforts to create a selection process for CI officers. The original concept presented a simple premise. Enlisted Soldiers submit an application packet that includes an interview, background check and suitability assessment (per AR 381-20 and DA Pam 611-21). Therefore, officers who wanted to serve in the CI field should also undergo some type of selection process. However, one solid argument against this particular initiative resulted from the Army's existing selection requirements for all Army officers. Requiring a second selection process to become a CI officer seemed somewhat redundant and therefore, unnecessary. Less than half the officers with the CI AOC receive a CI assignment in a 20-year Army career, and based on a cost-benefit analysis the selection initiative was never fully implemented.

The Director of Army CI Coordinating Authority (ACICA), INSCOM G-2X, wanted a more practical approach that would allow select MI officers to obtain the CI officer AOC, and immediately put that training to use in the Army and the intelligence community. This would strategically select a small percentage of MI officers from the larger officer population and target them for immersive CI training. The program would be limited to a percentage of the CI officer population and require applicants to meet certain requirements.

The Director of ACICA, INSCOM G-2X, and the Chief of the CI Division, Army G-2X, considered it imperative that the program in no way impede, obstruct, or hinder an officer's career progression or professional military education timelines. The Army G-2X's ultimate goal was a program structured to enhance an MI officer's career with CI training and a follow-on utilization tour, and that the sequence allows time for attending Command and General Staff College and the officer's key developmental assignment as a major. In doing so, the program would broaden select junior officers and key developmentally complete captains with enhanced CI training and experience while simultaneously affording them every opportunity to remain competitive for promotion to lieutenant colonel and selection for battalion command. Simultaneously, the Army would enhance readiness and better prepare CI officers for the intelligence warfighting force of the future. The INSCOM G-2X and Army G-2X, together with the MI lieutenant colonel assignment officer at the U.S. Army Human Resources Command (HRC) determined such a program would succeed if modeled after other existing AIDP protocols.

AIDP-CI Program Requirements and Implementation

Requirements to apply for the program include:

- Possess career management field 35.
- Completion of a key developmental position with demonstrated outstanding performance.
- Successful completion of the Captain's Career Course.
- DA photo in current grade.
- Possess a final Top Secret clearance with sensitive compartmented information access.

Officers must also be deployable, have no flags or adverse actions pending, and display outstanding potential for future service. Application packets are submitted to HRC for review and selection.

In fiscal year 2016, the 902nd MI Group, INSCOM's functional CI brigade responsible for conducting the CI mission across the continental United States (CONUS), and the largest CI organization in the Department of Defense, took on the responsibility of managing the AIDP-CI Program. The 902nd MI Group conducts the Army CI mission primarily from two battalions. The 308th MI Battalion operates all of the INSCOM CI field offices within CONUS and is responsible for conducting the Army's CI Covering Agent Program, Threat Awareness and Reporting Program, and CI support to technology and critical infrastructure programs. The 310th MI Battalion conducts CI technical services, CI investigations, and operations in the cyber domain.

In the summer of 2017, four MI officers will participate in the inaugural AIDP-CI program, an operationally focused 24-month assignment at Fort Meade, Maryland, which includes training at the 7-week Advanced CI Collections Course and 4-week Advanced CI Investigations Course. The Joint CI Training Academy in Quantico, Virginia, hosts both courses. An additional training opportunity available to the program stems from a partnership between the U.S. Army and the Federal Law Enforcement Training Centers in Glynco, Georgia. This partnership will allow selected Army CI agents to attend the 11-week Criminal Investigator Training Program (CITP). While CITP is not a required course for successful completion of AIDP-CI, it is an option within the program based upon availability and 902nd command discretion. In addition to institutional training, AIDP-CI officers will gain real world CI experience through on-the-job training via rotational tours within each of the 902nd MI Group's four subordinate units. These officers will have direct visibility and insight into the planning, conduct, and oversight of some of the Army's most sensitive CI operations and investigations. They will also gain familiarization with assignment opportunities within the greater U.S. intelligence community.

Following completion of the AIDP-CI program, the officers will incur a six-year Active Duty service obligation and a CI utilization assignment that is coordinated through MI Branch, HRC. Additionally, HRC in conjunction with the Office of the Chief, MI and U.S. Army Intelligence Center of Excellence is developing an additional skill identifier for AIDP-CI to track and manage these officers in future assignments.

CW5 Traci A. Goodwin is the Chief of Counterintelligence (CI) Initiatives (manning/training/equipping), Headquarters, Department of the Army, Office Deputy Chief of Staff, G-2 with 29 years of CI experience. Her past assignments include 3rd Infantry Division; 1st Infantry Division; I Corps; Headquarters, Intelligence and Security Command; 650th Military Intelligence (MI) Group; and the 902nd MI Group. She has served as a CI team leader, special agent in charge, CI analysis cell officer in charge, CI collection manager, corps CI coordinating authority, International Security Forces Joint Command, CJ2X CI coordinating authority, CI operations officer, and allied MI battalion operations officer. She has deployed in support of several operations, including Operation Joint Endeavor, Operation Joint Guardian, Operation Iraqi Freedom, and Operation Enduring Freedom. She holds a bachelor of science in criminal justice from the University of North Carolina, Chapel Hill.

CW5 Michael D. Dye is the first Command Chief Warrant Officer of the 902nd Military Intelligence (MI) Group at Fort Meade, MD. He has 31 years of Active Federal Service, 27 of which are in the counterintelligence (CI) discipline. His past assignments include 902nd MI Group, 501st MI Brigade, U.S. Army Foreign CI Activity, and Army Field Support Center. In 2005, CW5 Dye helped establish the Intelligence and Security Command Theater Detachment - Afghanistan, later renamed the Strategic CI Detachment-Afghanistan, to provide strategic CI support to U.S. Forces Afghanistan and U.S. Central Command. In 2013, he returned to Afghanistan to serve as operations officer of the Joint CI Unit-Afghanistan, now known as the Joint Detachment Apollo-Afghanistan, a combined CI and human intelligence platform supporting Operation Inherent Resolve J-2.

Learning the Cyber Trade: Intelligence Support to Defensive Cyberspace Operations

by Captain J. Brooks Jarnagin

Introduction

Cyberspace threats are becoming more prevalent in our society as the internet of things continues to expand into the many different facets of our daily lives. We rely on cyberspace architecture to surf the web, read the news, shop for goods, conduct online banking, communicate with others (e.g., email, phone, text, and Skype), access information databases, and even stream media. With the emerging threat continuing to evolve, the U.S. Army has recognized the need to train, build, and sustain intelligence professionals and capabilities to meet our adversaries on this digital battlefield. Since 2012, the military intelligence community has invested time and energy to create a core of intelligence professionals to support this endeavor. These select few individuals are graduates of the Army Intelligence Development Program (AIDP)–Cyber.

The intent of this article is to assist future AIDP–Cyber interns and other intelligence professionals with understanding the program and understanding how intelligence can support cyberspace operations. The complexity of intelligence support to cyberspace operations requires —

- An understanding of the high level of training required to process the technical intelligence reports used to develop threat assessments.
- An effective planning method to analyze the threat.
- A deep understanding of the request for support, information, and action from both internal and external organizations.

Analysis of this degree is not simple and requires an agile professional that can synthesize and fuse cybersecurity concepts and relate them to our adversaries.

Knowing how to leverage both cyber expertise and intelligence support are key for intelligence professionals to provide commanders with a holistic understanding of threats in the cyberspace domain. Also key is an understanding of how threats can use dominance of cyberspace to transcend and effect the remaining four dimensions of the battlefield. This is a new and exciting time to enter the cyber profession and assist the professionals of today with shaping how intelligence can support cyberspace operations tomorrow.

The AIDP–Cyber Boot Camp

Many Intelligence professionals have very little exposure to cyberspace fundamentals. To bridge this gap, AIDP–Cyber has created the cyber boot camp training pipeline. The goal of the pipeline training is to provide a foundational comprehension of critical cybersecurity concepts that correlate with industry standards for information technology (IT) professionals. The pipeline provides a baseline for incoming interns to gain a general understanding of basic IT fundamentals prior to integration into one of the many cyber work roles. The courses consist of A+, Network+, Security+, and Certified Ethical Hacker. These courses typically last one to two weeks and culminate with an industry level certification examination.

A+ is designed to give foundational training on network hardware and software and provide basic troubleshooting skills for new IT professionals. This course should not be taken lightly, as it covers a wide range of cybersecurity topics. Think of it as an overview primer for the remaining certifications. Network+ is centered on a firm grasp of both wired and wireless network technologies and the troubleshooting methodology. From this course, an intern receives a basic understanding of cybersecurity concepts and gains the cyber lexicon.

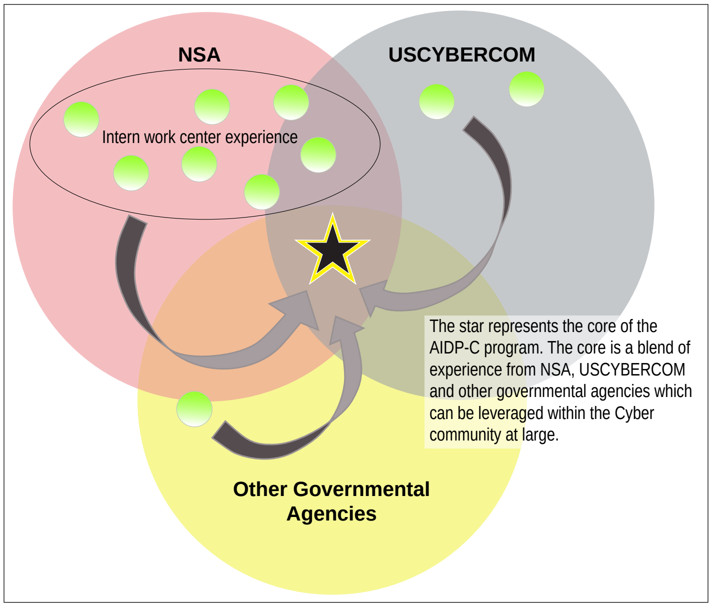
Security+ is simply revisiting Network+ concepts of keeping a network running, but this time around, interns learn how to safeguard a network and all its users from external factors. The course has interns thinking like cyber network defenders rather than help desk technicians. Completion of the Security+ certification will assist interns' successful transition to the final course—Certified Ethical Hacker. During this course, interns leverage all the training received during the pipeline certification and begin to realize the basic tactics, techniques, and procedures (TTP) for conducting an area reconnaissance of a blue space network and how to exploit potential vulnerabilities. Once an AIDP–Cyber intern completes all of these certification courses, they will have an introductory/intermediate level of knowledge of cybersecurity concepts and will be well poised to begin their rotation through one of the various operational missions.

Additional courses are available to AIDP–Cyber interns for professional development and are also available to units to build a core section of cyber specialists. One venue that offers similar classroom and online training is the Defense Cyber Investigations Training Academy (DCITA). This training is provided at no cost to the unit. However, the unit will have to provide temporary duty funding when sending a Soldier or government civilian to an instructor led course. This is a small price to pay compared to the cost of sending a Soldier or civilian to any of the industry certification courses. Before registering Soldiers or civilians for online training, ensure they have at least a basic understanding of hardware and network fundamentals. Introduction to Network and Hardware is a mandatory pre-requisite before attending any other DCITA courses.

AIDP–Cyber interns now have a basic understanding of cybersecurity, but how do they apply it in a cyber work role? They have two training options for receiving their cyberspace planner identifier, N9. First is the Army Cyberspace Operations Planners Course (ACOPC). This training is an Army internal course that does an excellent job of providing a policy review of how the Army plans, approves, and conducts cyberspace operations. ACOPC also provides students with a practical exercise designed to analyze a cyber-threat and works through the process of planning and executing a cyber-response. The second option that also produces the N9 identifier is the Joint Cyberspace Operations Planners Course (JCOPC). The major difference between the two courses is the planning method implemented; Army versus joint. The content of both courses remains the same and either will provide an AIDP–Cyber intern with a great foundation for planning and supporting cyberspace operations.

Intelligence Support to a Cyber Protection Team

With the foundation training completed, the AIDP–Cyber intern can focus on applying their newly acquired skillsets in a cyber work role that reside either in the National Security Agency or in U.S. Cyber Command (USCYBERCOM). The three main work roles for AIDP–Cyber interns to experience are defensive cyberspace operations (DCO), offensive cyberspace operations, and the cyber planner. The work roles are designed to build upon the intern's foundational training and start to connect the critical concepts of cyberspace. During this phase of the AIDP–Cyber experience, interns begin to understand how intelligence supports cyberspace operations.

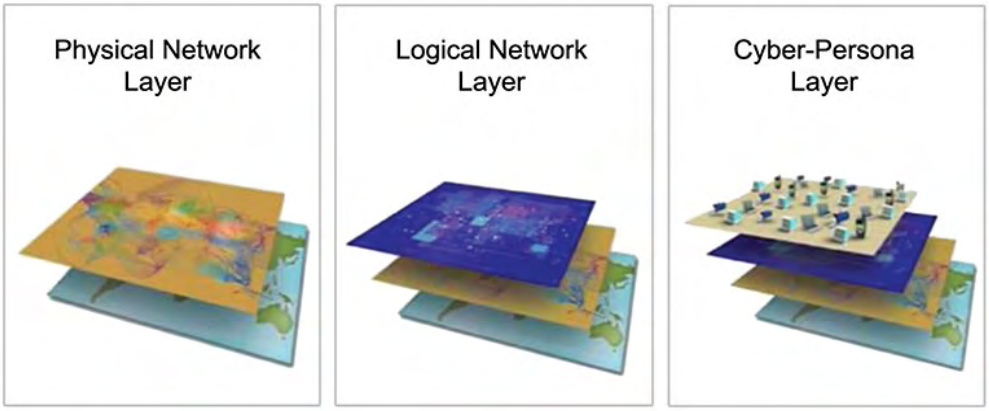

NSA
USCYBERCOM
Intern work center experience
Other Governmental Agencies
The star represents the core of the AIDP-C program. The core is a blend of experience from NSA, USCYBERCOM and other governmental agencies which can be leveraged within the Cyber community at large.

Cyber Intern Work Roles.[1]

AIDP–Cyber interns are encouraged to seek a DCO position first to continue reinforcing the training they have received. Interns will immediately begin to immerse themselves in learning how the Department of Defense Information Network (DODIN) infrastructure is arrayed, but more importantly how to defend the network from intrusions. A part of USCYBERCOM's mission is to "…direct the operations and defense of specified Department of Defense information networks..."[2] USCYBERCOM accomplishes this task with multiple cyber protection teams that align to various nation state actors known as intrusion sets. A cyber protection team consist of cyber, signal, electronic warfare and intelligence warfighters that work as a cohesive team to identify network compromises, eradicate adversaries from the DODIN, and are on standby to defend the nations critical infrastructure.[3] When an intern is assigned a role on a cyber protection team, one of their chief goals is understanding how the intelligence section can best support the operation. There are multiple methods for cyber protection teams to receive DCO missions. For example, there are directed incident response missions from USCYBERCOM and there are team-initiated missions. During the latter, all-source analysts review threat reporting and develop vulnerability assessments for Army networks of interest and nominate operations for a potential DCO mission. This list is not all-inclusive, but does show the necessity for all-source analysts to remain flexible and provide appropriate support to mission planning.

One trusted and tested method for an intelligence officer supporting planning efforts of unified land operations is the military decisionmaking process (MDMP), specifically intelligence preparation of the battlefield (IPB).[4] Cyber interns should consider using the IPB process, with a cyber-focus, during the planning phases of any DCO. While the word "intelligence" precedes "preparation of the battlefield," this is not solely an intelligence responsibility. The intelligence analyst leads the effort, but receives support from the cyber, signal, and electronic warfare Soldiers. The all-source intelligence analyst may not possess the technical background to understand network topologies and should not make the IPB products in a vacuum. All-source analysts can have a general knowledge of IT fundamentals, but their strength resides in analyzing traditional intelligence reporting and all-source production. The intelligence warfighter's analysis efforts will center on defining the physical, logical and cyber persona layers of the cyber environment and describing the effects on blue space.

Step 1 of the IPB Process—Define the Operational Environment.[5] During this step, the intelligence analyst will begin to examine the network owner and develop a general knowledge of the history of the network, highlighting significant facts about the network and whom the network is intended to support. Next, the intelligence analyst will examine the physical layer and determine the geographic location and the hardware infrastructure used to run the network. An example of this is "X" type of web server, running a "Y" operating system that is physically located on "Z" installation. Next, the intelligence analyst will begin to examine the logical layer and determine how network traffic is supported. The logical layer is abstract from, but related to the physical layer. One example is multiple web servers that are geographically separated, but support one particular network (e.g., Non-classified Internet Protocol Router Network [NIPRNet]). To the NIPRNet user these logical connections are transparent. A further abstraction is the cyber persona layer. This is a combination of a real person operating from the physical layer, in/through the logical layer, and their actions are represented as a virtual cyber persona.[7]



Three Layers of Cyberspace.[6]

Step 2 of the IPB Process—Describe Environmental Effects on Operations.[8] During this phase, the analyst will determine the effects of terrain, weather, and civil considerations that affect the network. The analyst needs to think about how users access the network, which users have elevated privileges, and from where users geographically access the network. Analysts will then create a modified combined obstacle overlay that focuses on identifying observations and fields of fire, cover and concealment, obstacles, key terrain, and avenues of approach to the network. For example, the analyst would identify locations of intrusion detection systems (observation), analyze firewall settings and understand their restrictions (cover and concealment), understand authentication procedures to gain access to the network (obstacles), identify cyber key terrain (key terrain), and understand where the gateway access points to the network are located (avenues of approach). When done correctly analysts will have a firm grasp of the targeted networks topology and will have started to identify intelligence gaps.

Step 3 of the IPB Process—Evaluate the Threat.[9] This is the most difficult phase of IPB because it requires a certain level of technical expertise to understand an adversary's TTPs. It can take months to years to train an all-source analyst how to analyze effectively a threat's capabilities. As a profession, the cyber force can mitigate the knowledge gap of the all-source analyst with either an embedded cyberspace operations specialist or a cryptologic network warfare specialist dedicated to supporting the intelligence mission. Each of these work roles provide expertise in the understanding of network topologies and analyzing network traffic, and are already a part of the cyber protection team. The cyber protection team can task organize either of these assets to meet this requirement. However, there is no current capability within the brigade combat team to conduct this level of analysis. As the cyber domain continues to professionalize and expand its support base to lower echelons it may be prudent to consider adding these specialty work roles to the formation. The all-source analyst can leverage the expertise of these work roles when reviewing/creating kill chain analysis (KCA)[10] reports or just general threat reporting from the intelligence community. A KCA report is a method used to describe a threat actor's TTPs for conducting a cyber-attack. The TTPs discussed within the KCA will assist all-source analysts with developing a list of potential indicators to confirm the presence of an adversary in blue space.

Step 4 of the IPB Process—Determine Threat Courses of Action.[11] Analysts will review the body of reporting and determine the threats' most likely and most dangerous course of action. A graphical depiction describing how the adversary will maneuver through cyberspace and accomplish their mission can help the commander visual, understand the various threat vectors, and allow the commander to mitigate risk. Intelligence analysts will consolidate all known threat TTPs and indicators of compromise from previous adversary operations, and assist the cyber protection team in creating advance analytics and signature-based rules designed to detect an adversary's activity on the network. Ultimately, the cyber protection team will have enough information to develop thoughtful priority intelligence requirements and a detailed collection plan to drive DCO.

Updating Our Doctrine:

A current best practice identified for cyber protection teams is MDMP using IPB, as a foundation for any DCO planning effort. Army commanders are familiar with this planning model and the S-3 can use it to plan for addressing a threat. ATP 2-01.3, *Intelligence Preparation of the Battlefield/Battlespace*, JP 3-12, *Cyberspace Operations*, and FM 3-38, *Cyber Electromagnetic Activities* are great foundation blocks for intelligence support to cyberspace operations. However, each of these publications needs additional refinement solidifying how intelligence can further support planning efforts in cyberspace operations. Current doctrine is broad and lacks this level of specificity. For example ATP 2-01.3, lists IPB support to cyberspace operations as a unique environment and provides wave top guidance for an analyst to follow.[12] FM 3-38, Chapter 6, provides an overview for how the cyber electromagnetic activities cell can provide input/assistance to the S-2 and S-3 during MDMP, but does not adequately detail effective TTPs for accomplishing this task.[13] Detailing the IPB process in ATP 2-01.3 with an emphasis on analyzing cyberspace domains would greatly improve an intelligence analyst's ability to support cyberspace operations and further assist in maturing the cyberspace domain. Analyzing the threat belongs to the intelligence warfighter; updating doctrine to reflect the seriousness of the cyber threat and techniques to combat it is a necessity.

Seek External Support to Enable Cyberspace Operations

The cyber protection team is not limited to just internal resources to answer collection requirements. Best practices include interfacing with the intelligence community (IC), law enforcement (LE) and other cyber mission force organizations during similar planning phases of the mission. The cyber protection team needs to understand that our adversaries have a marked advantage when attacking U.S. IT infrastructure systems. Adversaries in cyberspace operate in geographically separated areas of operations, possess a high level of technical expertise, use obfuscation TTPs to conceal their attack vectors, and exploit our national policies to impede our ability to detect their presence in blue space.

Understanding where collection gaps exist and what agencies can provide assistance is crucial. Several lessons learned have provided successful vignettes that leveraged the IC and LE resources to accomplish the mission. These organizations will not impede DCO missions. On the contrary, the IC or LE may have the missing pieces to the overall threat picture that the cyber protection team needs to detect an adversary. LE agencies can also assist with victim notification and ensure the cyber protection team has a vetted trusted agent at the compromised network location. Reaching out to IC and LE resources early and often is an effective way of ensuring a holistic view of the threat picture and negating our adversary's use of national policies to obscure a cyber protection team's detection capability.

Conclusion

Cyberspace presents our nation's cybersecurity forces with a wide range of potential threats that require a measured and unified response. This requires an elite group of cybersecurity and intelligence professionals dedicated to understanding the complex and diverse threats to our nation. The AIDP–Cyber program is one method of integrating cybersecurity and intelligence professionals to support and enable cyberspace operations. Cyber protection teams need to link the right technical expert with the right intelligence analyst to understand fully the threat. Cyber protection teams can also seek assistance from the IC and LE agencies to ensure a holistic representation of the threat as the cyber domain is too complex to rely on the analysis of one agency alone. Each member of the cyber community has a particular role in defending networks from external forces. The key is to appropriately dedicate time and resources to create a cohesive team driven to one end state—the security of our networks. This fight is not purely a cyber-fight or an intelligence fight. It is a maneuver fight that occurs on a digital battlefield and requires thoughtful understanding across the spectrum to deter threats against the nation.

(Continued on page 30)

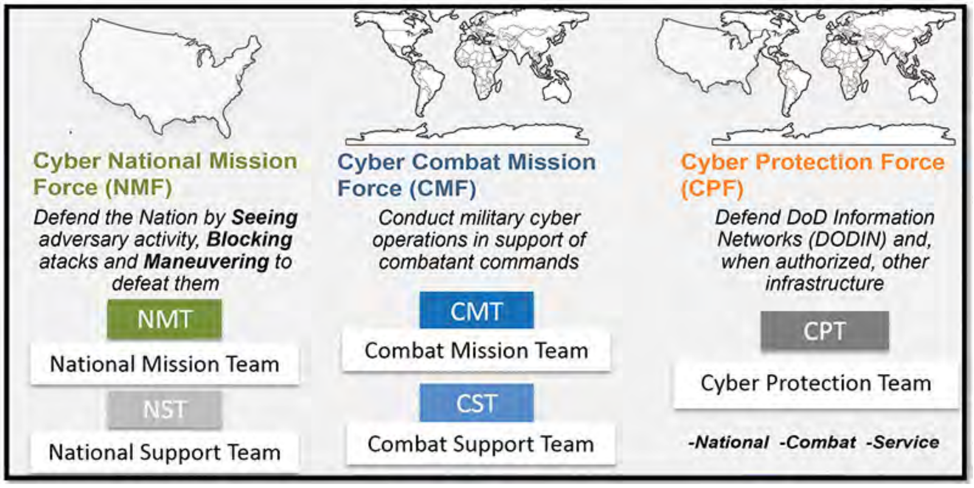
Army Intelligence Development Program–Cyber

by Lieutenant Colonel Justin D. Considine and Major Deonand S. Singh

Introduction

Conflict has and always will be a human endeavor. Conflict is a clash of human wills driven by passions like hatred, enmity, and fear, and is a struggle that begins and ends in the minds of men.[1] This conflict maintains its relevancy in the current digital age, operating among air, land, maritime, space, and cyber domains, but with its own set of added complexities. For military professionals, there is an increasing demand to support military operations by leveraging cyberspace to support all warfighting functions. As conflict applies to cyberspace, this manmade domain enables adversaries to "operate" in domestic, international, clandestine, and contested areas. The intent of this article is to explore and assist future leaders with understanding how the Army Intelligence Development Program (AIDP)–Cyber program develops knowledgeable intelligence professionals who can "maneuver" in cyberspace and enhance the warfighting capabilities of their formations.

AIDP–Cyber is a military intelligence (MI) program designed to produce a cohort of well-trained Army leaders with the knowledge, credentials, and experience to contribute to the tactical, operational, and strategic levels of cyberspace operations in support of national and combatant commander requirements. The AIDP–Cyber program's purpose and intent was established by a 781st Military Intelligence Battalion Memorandum for Record dated 1 March 2012. Fiscal year 2017's AIDP–Cyber interns mark the seventh iteration of the program. In order to appreciate and understand the AIDP–Cyber program, one must understand the vision, assessment, training, and future return on investment from educating intelligence professionals about cyberspace operations.



Cyber National Mission Force (NMF)

*Defend the Nation by **Seeing** adversary activity, **Blocking** atacks and **Maneuvering** to defeat them*

NMT

National Mission Team

NST

National Support Team

Cyber Combat Mission Force (CMF)

Conduct military cyber operations in support of combatant commands

CMT

Combat Mission Team

CST

Combat Support Team

Cyber Protection Force (CPF)

Defend DoD Information Networks (DODIN) and, when authorized, other infrastructure

CPT

Cyber Protection Team

-National -Combat -Service

Cyber Mission Force Overview.

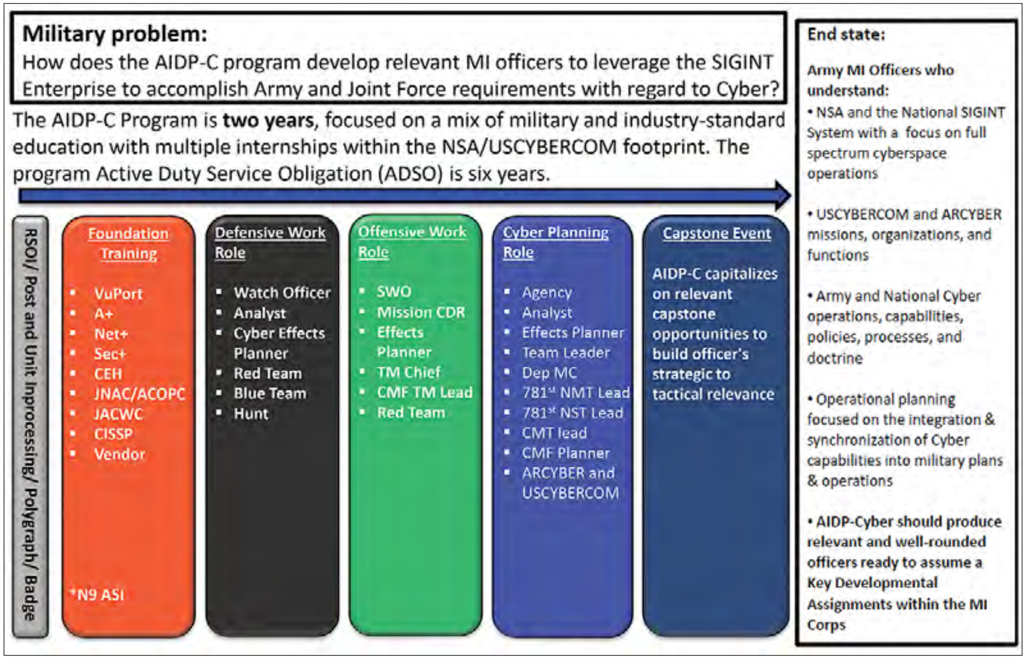
The Vision

Cyberspace presents an important challenge for our national security interests. Cyberspace has direct correlations with securing military information systems. The Department of Defense defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers".[2] The AIDP–Cyber program will enable intelligence professionals to understand the cyberspace domain as it applies to all warfighting functions. The program will also familiarize officers with the National Security Agency (NSA) and United States Signals Intelligence (SIGINT) System, with a focus on cyberspace. Graduates will also become familiar with the cyber mission force and its mission. Finally, AIDP–Cyber interns will gain a thorough understanding of the Army and national cyber capabilities with a focus on operational employment within a decisive action environment.

Assessing AIDP–Cyber Interns

What type of intelligence professionals are good candidates? The AIDP–Cyber application and selection process follows a timeline set by the U.S. Army Human Resources Command in the military personnel message released annually pertaining to all MI programs. All applicants must have a Top Secret clearance with sensitive compartmented information access. The candidates are also required to pass a counterintelligence polygraph examination prior to the program start. Applicants should be senior captains who are highly encouraged, but not required, to have a degree or strong background in computer science, electronic engineering or other science, technology, engineering, and mathematics field. We also recommend applicants be complete with key developmental assignments due to the length of the training pipeline, which is addressed in the next section of this article. AIDP–Cyber interns incur an Active Duty service obligation of six years with a utilization requirement into the MI Branch for selection, training, and development under the program.

The AIDP–Cyber selection process includes an assessment panel that reviews an average of 30 or more candidates. The best-qualified candidates (2-4 each cycle) are officers who demonstrate leadership excellence, technical competence, and managerial ability for future positions of responsibility. SIGINT experience is preferred but not required. Common to all MI programs, criteria include a strong record of performance, completion of key development assignments, primarily while in the rank of captain, experience in corps and below formations and combat experience. Once the officer is selected, they are enrolled in the AIDP–Cyber track. The 780th Military Intelligence Brigade administers the program with the potential for duty locations and operational tours at Fort Meade, Maryland; Fort Gordon, Georgia; San Antonio, Texas; and Schofield Barracks, Hawaii.



Military problem:
How does the AIDP-C program develop relevant MI officers to leverage the SIGINT Enterprise to accomplish Army and Joint Force requirements with regard to Cyber?

The AIDP-C Program is **two years**, focused on a mix of military and industry-standard education with multiple internships within the NSA/USCYBERCOM footprint. The program Active Duty Service Obligation (ADSO) is six years.

RSOI/ Post and Unit Inprocessing/ Polygraph/ Badge

Foundation Training
- VuPort
- A+
- Net+
- Sec+
- CEH
- JNAC/ACOPC
- JACWC
- CISSP
- Vendor

*N9 ASI

Defensive Work Role
- Watch Officer
- Analyst
- Cyber Effects Planner
- Red Team
- Blue Team
- Hunt

Offensive Work Role
- SWO
- Mission CDR
- Effects Planner
- TM Chief
- CMF TM Lead
- Red Team

Cyber Planning Role
- Agency
- Analyst
- Effects Planner
- Team Leader
- Dep MC
- 781st NMT Lead
- 781st NST Lead
- CMT lead
- CMF Planner
- ARCYBER and USCYBERCOM

Capstone Event

AIDP-C capitalizes on relevant capstone opportunities to build officer's strategic to tactical relevance

End state:

Army MI Officers who understand:

- NSA and the National SIGINT System with a focus on full spectrum cyberspace operations
- USCYBERCOM and ARCYBER missions, organizations, and functions
- Army and National Cyber operations, capabilities, policies, processes, and doctrine
- Operational planning focused on the integration & synchronization of Cyber capabilities into military plans & operations
- AIDP-Cyber should produce relevant and well-rounded officers ready to assume a Key Developmental Assignments within the MI Corps

AIDP-Cyber Program Training.

AIDP–Cyber Training

The AIDP–Cyber program consists of a mixture of formal classroom instruction, self-paced online instruction, and on-the-job training. Participants receive instruction at the National Cryptologic School, through Department of Defense cyber-related courses, and through commercial information technology certification courses. Throughout the course, there is a mix of military and industry-standard education training.

Once selected, interns move to Fort Meade, Maryland, for the two-year program. On-the-job training consists of separate six-to-eight month operational tours in up to four work centers at the NSA, or U.S. Cyber Command (USCYBERCOM). Officers who complete this program will then serve a 12-24 month utilization tour applying their newly acquired skills in positions involving cyber capabilities. There are numerous opportunities within the cyber community for utilization tours to broaden interns. AIDP–Cyber interns are also afforded the opportunity to deploy as part of an expeditionary cyber support element—capstone of the program. The experience an AIDP–Cyber graduate gains deploying in support of a combatant commander and leveraging national SIGINT and cyberspace is invaluable. As the adversary continues to evolve in the cyberspace domain, the AIDP–Cyber program continues to enable recent graduates to leverage cyberspace operations in tactical, operational, and strategic operations deployed forward.

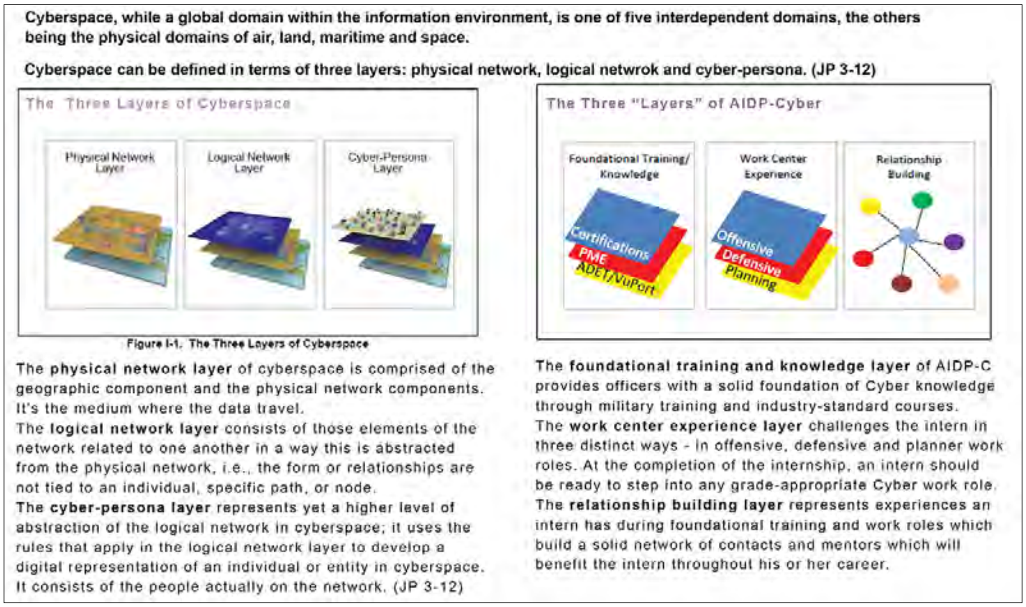
Senior Leaders Perspective

Senior leaders have a responsibility to obtain a basic knowledge of the cyberspace domain. We must then develop intelligence professionals who understand the cyberspace domain, cyber state and non-state actors, and the feasibility and proliferation of technology as it effects the commander's decision cycle. Cyber in the next 15 years will be like counterterrorism has been for the last 15 years. [Cyber] will be a foundational mission set that drives us as an organization and it will require us to do things on a scale we have never done before.[3] Intelligence and cyber professionals must both understand the adversary's capabilities and vulnerabilities in cyberspace and how cyberspace is leveraged within the operational environment. Investing in cyberspace planners is essential to ensuring cyberspace operations efforts focus on achieving the commander's objectives with the delivery of cyberspace effects integrated into multi-domain battle.

A major goal outlined in the Comprehensive National Cybersecurity Initiative is to strengthen the future cybersecurity environment by expanding cyber education and working to define and develop strategies to deter hostile or malicious activity in cyberspace.[4] The Army Cyberspace Operations Planners Course and the Joint Cyberspace Operations Planners Course are two options for foundational cyberspace planning.

Studying warfare helps leaders understand the principles of war. Like technological advances with cyber weapons and its impact on warfare, innovation in air power, armored warfare, amphibious warfare, and the development of the radar has significantly changed doctrine and development of leaders in professional military education institutions.[5] Army professionals must exercise personal initiative and intellectual curiosity through self-study. GEN (Ret.) James Mattis stated, "The problem with being too busy to read is that you learn by experience (or by your men's experience), i.e. the hard way. By reading, you learn through others' experiences, generally a better way to do business, especially in our line of work where the consequences of incompetence are so final for young men."[6]

AIDP–Cyber interns will apply personal research; writing and reading throughout the program to build individual and professional skills that improve their understanding of cyberspace as an operational domain. The key take away is to recognize Army, joint, and industry training must also include self-development so interns can educate future commanders and staffs. AIDP–Cyber graduates who leverage this model will assist staffs with visualization of the desired end state and accomplish the commander's objectives in and through the physical domains while leveraging cyberspace in the operating environment.



Cyberspace, while a global domain within the information environment, is one of five interdependent domains, the others being the physical domains of air, land, maritime and space.

Cyberspace can be defined in terms of three layers: physical network, logical netwrok and cyber-persona. (JP 3-12)

Figure I-1. The Three Layers of Cyberspace

The **physical network layer** of cyberspace is comprised of the geographic component and the physical network components. It's the medium where the data travel.
The **logical network layer** consists of those elements of the network related to one another in a way this is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node.
The **cyber-persona layer** represents yet a higher level of abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity in cyberspace. It consists of the people actually on the network. (JP 3-12)

The **foundational training and knowledge layer** of AIDP-C provides officers with a solid foundation of Cyber knowledge through military training and industry-standard courses.
The **work center experience layer** challenges the intern in three distinct ways - in offensive, defensive and planner work roles. At the completion of the internship, an intern should be ready to step into any grade-appropriate Cyber work role.
The **relationship building layer** represents experiences an intern has during foundational training and work roles which build a solid network of contacts and mentors which will benefit the intern throughout his or her career.

AIDP–Cyber Program Overview.

AIDP–Cyber Return on Investment

The AIDP–Cyber program is a six-year-old opportunity to develop intelligence professionals on the three cyberspace operations missions—offensive cyberspace operations, defensive cyberspace operations, and Department of Defense Information Network operations. According to the previous Chairman of the Joint Chiefs of Staff, GEN Martin E. Dempsey, more than 20 countries now have military units dedicated to employing cyber capabilities in war.[7] As conflict and cyberspace mature, intelligence and cyber leaders must work together to comprehend, and take action to defend the increasing threat to our Nation. At the conclusion of the AIDP–Cyber program, interns will be able to access and utilize doctrine to lead Army and national cyber operations, capabilities, policies, and processes under approved authorities. The AIDP–Cyber graduate will understand USCYBERCOM, U.S. Army Cyber Command and the intelligence community missions, organizations, and functions. These Army MI officers will understand NSA and the national SIGINT system with a focus on decisive action. An AIDP–Cyber graduate will also be able to leverage organizations to accomplish cyber mission force requirements with national and theater-level intelligence, using cyber systems to support warfighters at corps and below. The end state of the AIDP–Cyber program will produce relevant and well-rounded officers ready to assume a key developmental assignment within the MI Corps, armed to mentor, integrate, and execute cyberspace operations within the operational environment.

Endnotes

[1] U.S. Marine Corps Doctrinal Publication 1, *Warfighting,* (Washington, DC: U.S. Government Printing Office [GPO], 20 June 1997), 13-17.

[2] Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: GPO, 5 February 2013), I-1.

[3] Admiral Michael S. Rogers, Director of the National Security Agency, statement during a hearing of the Senate Select Intelligence Committee, 24 September 2015.

4. The White House, "The Comprehensive National Cybersecurity Initiative", https://obamawhitehouse.archives.gov/node/233086 . The Comprehensive National Cybersecurity Initiative (CNCI) was established by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008 and consists of a number of mutually reinforcing initiative with major goals designed to help secure the United States in cyberspace.

5. Willamson R. Murry and Allan R. Millet, eds., *Military Innovation in the Interwar Period* (New York: Cambridge University Press, 1996), 3.

6. James Mattis, quoted in Geoffrey Ingersoll, "General James 'Mad Dog' Mattis Email About Being 'Too Busy to Read' is a Must Read" *Business Insider,* May 9, 2013, http://www.businessinsider.com/viral-james-mattis-email-reading-marines-2013-5.

7. Lisa Ferdinando, "Demsey: Cyber Vulnerabilities Threaten National Security." *DoD News,* January 21, 2015, http://www.defense.gov/news/newsarticle.aspx?id=128001 .

LTC Justin D. Considine is currently the commander of the 781st Military Intelligence Battalion. Formerly a military intelligence officer, he transitioned to the cyber branch in 2015. His recent assignments include the Joint Staff J39 Cyberspace & Electronic Warfare Operations Division, 781st Military Intelligence Battalion operations officer, and Chief of the Army Remote Operations Center.

MAJ Deonand S. Singh is currently the battalion operations officer and the executive agent of the military intelligence program for Army Intelligence Development Program–Cyber at Fort Meade, MD. His recent assignments include serving as cyber support to corps and below, officer in charge for the 780th Military Intelligence Brigade (Cyber), brigade S-2, military intelligence company commander, and battalion S-2.

Learning the Cyber Trade: Intelligence Support to Defensive Cyberspace Operations

(Continued from page 26)

Endnotes

1. 781st Military Intelligence Battalion, Army Intelligence Development Program–Cyber overview brief for incoming interns.

2. "U.S. Cyber Command (USCYBERCOM) Fact Sheet", U.S. Strategic Command, September 30, 2016. http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/.

3. U.S. Department of Defense, "All Cyber Mission Force Teams Achieve Initial Operating Capability", U.S. Cyber Command News Release, October 24, 2016. https://www.defense.gov/News/Article/Article/984663/all-cyber-mission-force-teams-achieve-initial-operating-capability.

4. U.S. Army Doctrinal Reference Publication 5-0, The Operations Process, (Washington, DC: U.S. Government Printing Office [GPO], 17 May 2012), 2-11.

5. U.S. Army Techniques Publication (ATP) 2-01.3, Intelligence Preparation of the Battlefield/Battlespace, (Washington, DC: U.S. GPO, 10 November 2014), 3-1.

6. Joint Publication 3-12, Cyberspace Operations, (Washington, DC: U.S. GPO, 5 February 2013), I-3.

7. Ibid, I-2 – I-4.

8. ATP 2-01.3, Intelligence Preparation of the Battlefield/Battlespace, 4-1.

9. Ibid, 5-1.

10. Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Advesary Campaigns and Intrusion Kill Chains" (white paper, Lockheed Martin Corp.). http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

11. ATP 2-01.3, Intelligence Preparation of the Battlefield/Battlespace, 6-1.

12. Ibid, 9-12.

13. U.S. Army Field Manual 3-38, Cyber Electromagnetic Activities, (Washington, DC: U.S. GPO, 12 February 2014), 6-1.

CPT J. Brooks Jarnagin is currently in his first year of the military intelligence program for AIDP–Cyber at Fort Meade, MD. His recent assignments include serving as executive officer for the Headquarters, Department of the Army, Assistant Deputy Chief of Staff, G-2; military intelligence company commander; battalion S-2 and brigade assistant S-2.

The Junior Officer Cryptologic Career Program

by Major Brian Nicklas, Major Philip Wingo, and Major Christian Wollenburg

Introduction

Recognizing the need for a core of highly trained officers to fill key leadership positions throughout the cryptologic community, the Director of the National Security Agency/Central Security Service (NSA/CSS), established the Junior Officer Cryptologic Career Program (JOCCP) in 1971. The JOCCP is a selective, joint cryptologic leadership program that provides participants with unique training and understanding of the cryptologic enterprise, and how signals intelligence (SIGINT) is a critical facet of the intelligence warfighting function supporting the Army's Operating Concept. The JOCCP offers participants a three-year opportunity to develop broad and operational expertise in the cryptologic field through a combination of academic studies and work center experiences within the NSA/CSS and associated intelligence community partners. Graduates of the program typically receive assignment to key cryptologic leadership positions providing the Army with a cadre of specially trained officers capable of effectively leveraging the NSA/CSS enterprise to fulfill intelligence requirements and better inform their commanders.

Program Overview

The program executive panel selects perspective participants for the program based on the following eligibility criteria:

- Active duty military intelligence officers in the cohort year group specified in the annual military intelligence (MI) programs military personnel message sent out by U.S. Army Human Resources Command.
- Must have completed the Captain's Career Course.
- Demonstrated outstanding performance in key developmental positions while a captain in accordance with DA PAM 600-3, *Commissioned Officer Professional Development and Career Management*.
- Current DA photo.
- Possess a final Top Secret clearance with access to sensitive compartmented information and able to successfully complete a counterintelligence polygraph.
- Must be deployable (non-waiverable).
- Not flagged or pending adverse action.
- Must have outstanding potential for future service.

Upon selection for the program, an officer moves on permanent change of station orders to the 704th Military Intelligence Brigade, with duty at the NSA, Fort Meade, Maryland. The program consists of multiple requirements and selected officers will incur an Active Duty service obligation of six years (three years in the program and a three-year utilization tour).

The first major requirement of the program is an academic portion that requires officers to complete 1300 hours of formal instruction through the National Cryptologic School (NCS). There participants are exposed to a wide range of training in SIGINT and cyberspace operations. Additionally, program participants are required to complete NSA work center tours in four focus areas:

- Analysis and production.
- Collection management.
- Information operations.
- Support to military operations.

If time permits, a policy and/or cyber tour is strongly recommended, or may be substituted for the information operations tour following executive approval. In completing the program's work center tours, officers will interact with various members of the intelligence community, major military commands, and other government agencies and organizations. Program participants can also serve on temporary duty status or deploy in support of global cryptologic operations. The objectives of the JOCCP are to fully support NSA/CSS missions and are directly linked to the goals laid out in the NSA/CSS organizational strategy.

An executive panel manages the JOCCP for the Director of the NSA/CSS consisting of a senior military officer at the O6 level, as well as a civilian senior-level executive manager, for each military service. The executive panel determines the programs policies and ensures it addresses the needs of the services cryptologic elements. A civilian executive who advises each officer on academic and work center requirements manages day-to-day administration of the JOCCP.

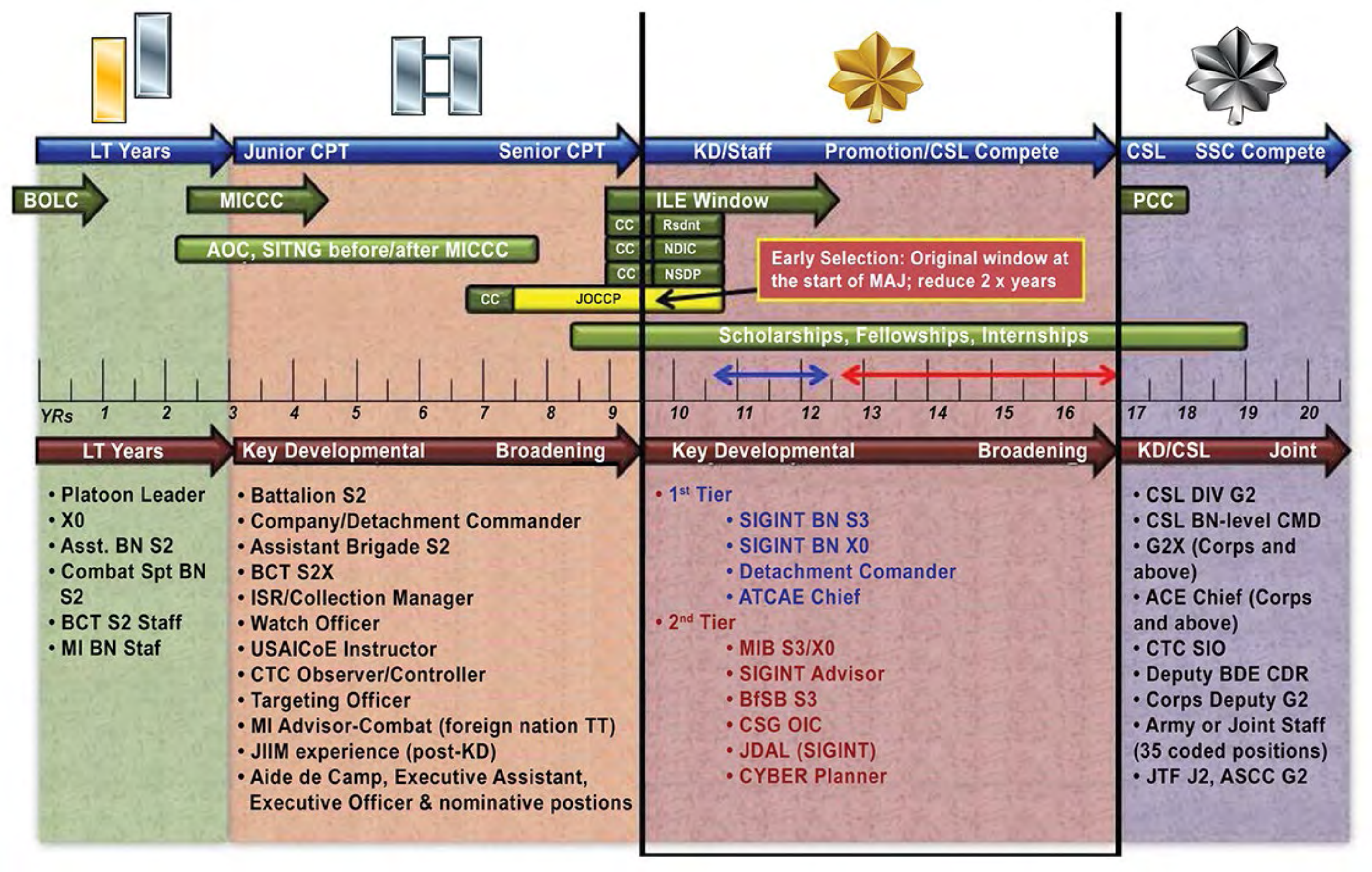
Experience and Benefits

While assigned to NSA's Army service component, the 704th MI Brigade, officers work in direct support of the NSA/CSS. The JOCCP provides a unique opportunity for officers to be exposed to each component of the cryptologic enterprise aiding in their development of in-depth knowledge of capabilities and resources of the NSA/CSS. By transitioning between multiple work centers, officers gain SIGINT knowledge, understanding of missions, and exposure to the national SIGINT system. That knowledge, coupled with the development of professional networks creates exceptional officers with the ability to leverage tremendous assets in support of Army operations. Beyond the NSA/CSS, officers gain a broad understanding of the greater intelligence community and exposure to strategic level decision making and intelligence operations.

Once core requirements are complete, participants possess the flexibility to pursue additional learning objectives and/or professional certifications. For example, participants often pursue civilian information technology certifications such as CompTIA Network+, Security+, and EC Council Certified Ethical Hacking. Additionally, the required four work center tours are not limited to fulfillment at NSA/CSS Washington; they can be completed throughout the cryptologic enterprise. This permits participants to shape their work center tours, and to establish a glide path for opportunities following completion of the program such as pursuing a civilian graduate degree.

Professional Military Education

Historically, Army officers accepted into JOCCP completed professional military education via satellite Command and General Staff Officer Course (CGSOC) and receive Advanced Operations Course (AOC) credit from JOCCP. This changed as of the 2017 cohort; JOCCP no longer prevents attending resident CGSOC at Fort Leavenworth, Kansas, or equivalent resident courses. Army officers in JOCCP are now considered with their year group for attendance at resident CGSOC



following completion of the program. Army officers in the program selected to attend the satellite course must now complete AOC via correspondence, as JOCCP no longer provides credit. The impact is that officers in the program will likely be out of the available officer assignment pool for up to four years. Applicants that are more senior will need to plan their timelines accordingly, understanding the program may limit availability for some key developmental positions. The strong profile most officers earned prior to entry into JOCCP combined with the reputation they earn upon completion, opens additional avenues for successful graduates as majors.

Conclusion

JOCCP offers a unique opportunity for officers to gain tremendous depth and breadth in SIGINT knowledge unparalleled in other intelligence disciplines. Former Army JOCCP panel member, COL Michael A. Marti summarized it best when he stated,

> ***“JOCCP graduates bring broad and specific knowledge of the NSA/CSS mission, organizational structure, and key relationships. Cryptologic capability impacts the Army’s unified action, enabling intelligence and network warfare operations in support of unified land operations. The immediate impact of JOCCP graduates in Army units is through the integration of signals intelligence into the lethal and non-lethal targeting process and intelligence preparation of the environment. The academic expertise gained from the NCS, blended with practitioner experience from NSA/CSS’s collection/analysis support to expeditionary forces, leverages JOCCP graduate knowledge and reach into the cryptologic enterprise to enhance mission command at the direct, organizational, and strategic levels of leadership.”*** [1]

The JOCCP provides officers the opportunity to experience and learn the real-world application of SIGINT exploitation and support to cyberspace operations. Upon graduation, each participant will receive the additional skill identifier, 3W, and will have demonstrated superior performance in their work center tours. The knowledge and skills gained allows them to return to the Army and have immediate effect on their commander’s ability to leverage NSA/CSS capabilities in support of operations.

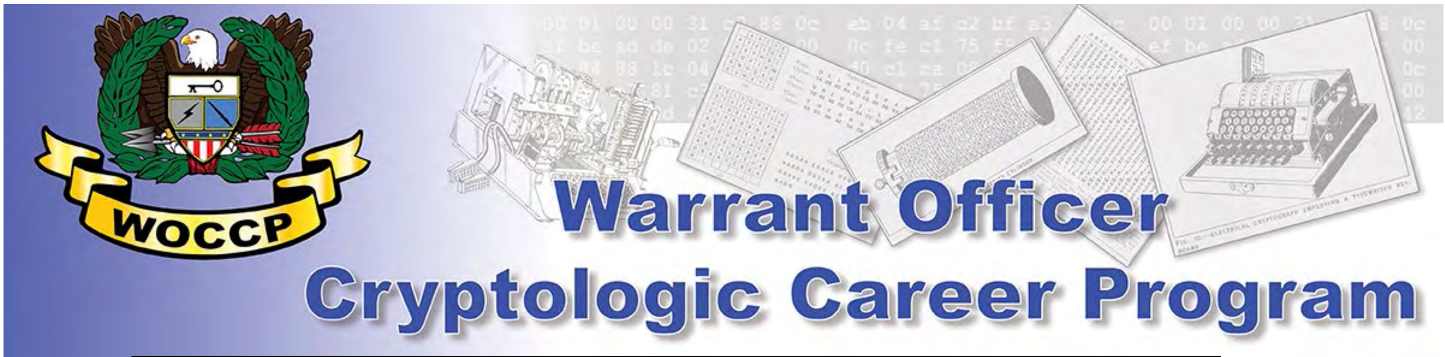
Endnotes

[1] This quote from COL Marti was in response to an email inquiry from the article authors in which they asked for his observations of the program as an executive panel member.

MAJ Brian Nicklas holds bachelor’s and master’s degrees in foreign affairs from the Hawaii Pacific University. Prior to JOCCP MAJ Nicklas served as a company commander with 1st Brigade, 2nd Infantry Division and a battalion S-2 at the Joint Readiness Training Center. He is currently in his final year of JOCCP and will graduate in June 2017.

MAJ Philip Wingo holds a bachelor’s degree from the Citadel. Prior to JOCCP, MAJ Wingo served with the 1st Brigade, 82nd Airborne Division as a company commander and battalion S-2. He is currently in his final year of JOCCP and will graduate in June 2017.

MAJ Christian Wollenburg holds a bachelor’s degree from the United States Military Academy. He is a recent graduate of the JOCCP. Prior to JOCCP, MAJ Wollenburg served with the 525th Battlefield Surveillance Brigade at Fort Bragg, NC as a company commander and brigade S-2.



Warrant Officer Cryptologic Career Program

by Chief Warrant Officer 2 Shawn King and Chief Warrant Officer 2 Dubby Black

Army signals intelligence (SIGINT) warrant officers have an unprecedented opportunity to further enhance their technical and operational expertise through the Warrant Officer Cryptologic Career Program (WOCCP). This three-year program resides at the National Security Agency/Central Security Service (NSA/CSS) at Fort George G. Meade, Maryland. The program provides a unique SIGINT education to warrant officers in the ranks of chief warrant officer 2 or chief warrant officer 3 in military occupational specialties (MOS) 352N, SIGINT Analysis Technician, and 352S, Signals Collection Technician. The program provides participants with formal training and individually tailored work assignments within the NSA/CSS and intelligence community partners.

Selection

A panel comprised of senior Army intelligence professionals convenes annually to select warrant officers to attend the WOCCP. Slots are limited to the three most qualified warrant officer applicants each year. Warrant officers who apply should treat the application process as if they were preparing for a promotion board. According to the Command Chief Warrant Officer of the Intelligence and Security Command (INSCOM), to be competitive for selection to WOCCP applicants should have an updated board file, DA photo, and a strong performance record.[1] INSCOM modeled the WOCCP after the Junior Officer Cryptologic Career Program (JOCCP) and the Middle Enlisted Cryptologic Career Program (MECCP). Since the 2014 academic year, the U.S. Army Human Resources Command (HRC) has announced the WOCCP through the military intelligence (MI) programs military personnel (MILPER) message. The MI warrant officer career development timeline on the next page identifies the ideal period for a warrant officer to apply for and attend the WOCCP.

History

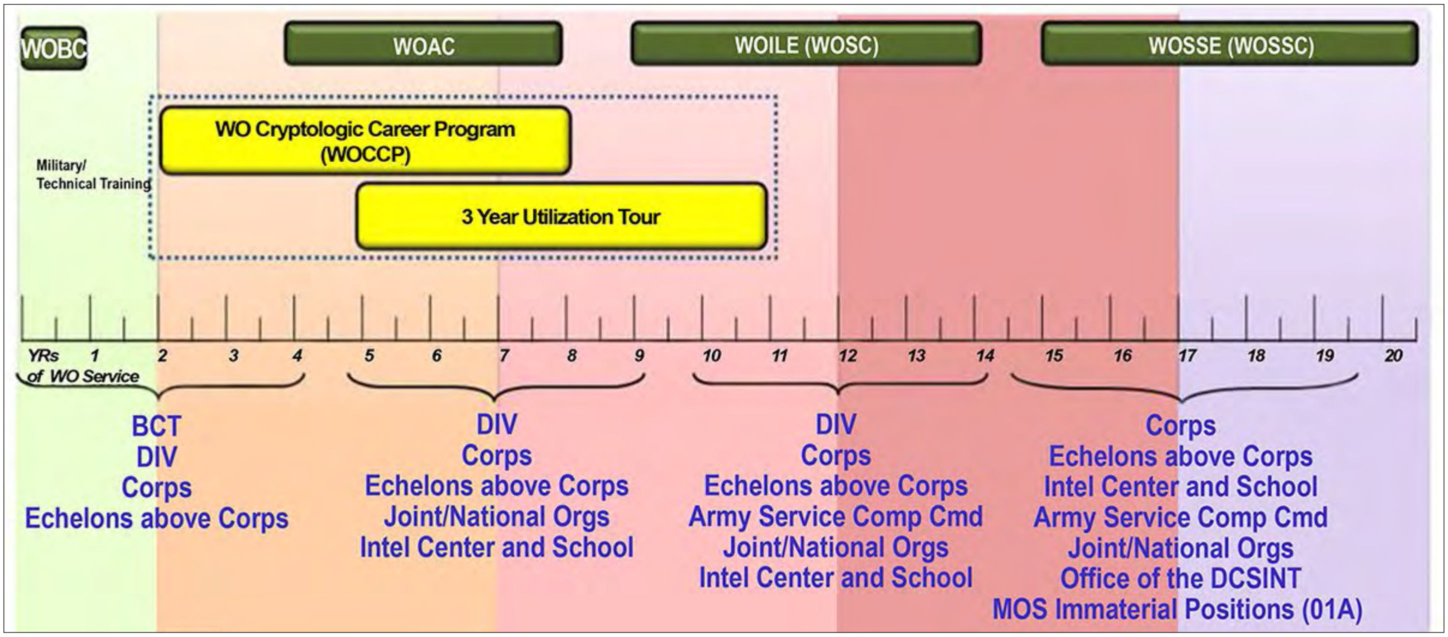
Intelligence leaders at many levels recognized the potential to further enhance the SIGINT warrant officer career fields through an education and training program similar to JOCCP. The INSCOM Commander led the effort to formerly establish the WOCCP, and in 2013, INSCOM launched the WOCCP pilot program with the selection of three warrant officers from the 704th MI Brigade. When asked recently about his motivation for creating the program, MG Stephen G. Fogarty replied—

> ***"I grew up in the tactical Army and learned very early in my career the importance of our warrant officer corps. As the G-2 of the 101st Airborne Division (Air Assault), I noticed that the few SIGINT warrants in the division with NSA experience were usually much more capable than those who didn't have experience at NSA. During my commands at Kunia, Hawaii and at NSA-Georgia, we had superb warrant officers who understood how to leverage the enterprise, but often didn't have the broad experience at NSA that some of my JOCCP graduates possessed. My intent for the program was to give our SIGINT warrant officers an opportunity to gain technical and organizational expertise in the broader cryptologic enterprise. I wanted them to build the same relationships with key players at NSA that our JOCCP officers did. It was simply about creating a cadre of SIGINT professionals who understood where to go to solve the most challenging SIGINT issues for their commanders and G-2s. The program benefits the Army by creating true cryptologic enterprise subject matter experts who then take that knowledge back to the Army and start leveraging the power of the entire cryptologic enterprise to solve the hardest problems."[2]***

Objectives

The WOCCP has three objectives designed to broaden the warrant officer's SIGINT expertise. Those objectives are:

- ✦ Develop a cadre of highly qualified warrant officers trained in cryptologic and information operations, and information systems to support combatant commanders and national policy makers.
- ✦ Increase the participant's knowledge and skills in cryptologic operations, information operations, system security, and intelligence production disciplines.
- ✦ Provide participants with an in-depth understanding of the NSA/CSS and the relationship within the national intelligence community.



MI Warrant Officer Career Development Timeline.

Types of Tours

Warrant officers further define the program by serving in at least four of six different focus areas comprised of—

- Collection management.
- Information and intelligence analysis.
- Support to military operations.
- Information operations.
- Cyber operations.
- Policy.

Participants find that each tour will hone and expand their existing skillsets to assist them in future assignments while benefiting the Army and the NSA/CSS. These tours also provide warrant officers the opportunities to mentor those around them, receive mentorship, and expand their professional network of military and civilian subject matter experts. Program participants have some latitude to structure their tour order to meet their particular course graduation requirements.

Warrant officers conducting collection management tours gain an understanding from multiple levels about how the Army and the NSA collect signals of interest. These tours help participants to develop an awareness for passive and active SIGINT collection systems and to identify and analyze vulnerabilities in technology. Additionally, warrant officers learn how a customer's intelligence request travels through the SIGINT system to become an intelligence requirement and validated collection requirement.

Information and intelligence analysis tours provide warrant officers experience in performing complex integrated analysis to produce information and intelligence that meets the nation's most critical needs. Warrant officers may find themselves learning to use the analytic tools that many junior enlisted and officers use. These tools are often on the cutting edge of agency technology and provide the participants with a more in-depth understanding of available capabilities.

Information operations tours, in accordance with FM 3-13, *Information Operations*, familiarize the participants with the core information related capabilities (IRC) which are used with other lines of operation to influence, disrupt, corrupt, or usurp the enemy's or adversary's decision making cycle while protecting our own. IRCs include, but are not limited to, operations security, electronic warfare, and cyberspace operations.

Support to military operations tours may be continental United States based support to deployed military forces, or outside the continental United States based support, whereby the warrant officer deploys in support of overseas contingency operation to perform the intelligence mission for a battle space owner or ground force commander. Participants, in coordination with the WOCCP leadership, determine which types of deployments would benefit the participant based on experience and training and then compete for those positions to fulfill the support to military operations requirement.

The cyber operations tour is an optional tour that offers the SIGINT warrant officer a solid understanding in the ever-evolving interaction between SIGINT and cyber operations. CW2 Joseph Feist, a 2016 WOCCP graduate, stated—

> ***"I already had a strong understanding of the national and tactical SIGINT architecture; however, I realized that I was not as keen on the processes of cryptologic network operations. To be able to fully understand and utilize the full gamut of our SIGINT capabilities I inserted myself into a cyber-focused track to familiarize myself with the basic knowledge required to properly vet and incorporate cyber capabilities into the SIGINT collection process."***[3]

Finally, WOCCP defines a policy tour as a rotation in any office within NSA that reviews regulations and guidance and provides answers to collection, production, and dissemination issues. Policy tours provide an education in SIGINT procedural guidance for the warrant officer to assist future commanders in setting up a new system, capability, or SIGINT mission. CW3 Kevin Nungester, another recent WOCCP participant had this to say about the program—

> ***"The highlight of my internship has been as a member of the small NSA21 military placement team [NSA21 is an agency restructuring/modernization initiative]. We intermediated between agency leadership and the military service commands to place military officers into service-relevant and sustainable leadership roles. Under the NSA21 reorganization, one of the Director's primary initiatives was to increase the amount of military leaders in agency leadership positions. It gave me a great perspective into where the organization is moving and also where the Army and the other four services see their personnel investment being most impactful in future operations."***[4]

All tours generally span six to nine months in length and allow the participants the opportunity to attend National Cryptologic School (NCS) courses, attend Army professional development courses or language courses. Each officer is required to accrue 800 NCS hours in order to graduate, but they usually exceed that requirement. NCS courses typically augment the current work center assignment the warrant officer is serving to further assist them in the learning process and provide subsequent hands-on training with the learned material. Practical application of all learned material is a principal goal of the program. A 2016 WOCCP graduate, CW3 Kathy Hall, had this to say about NCS courses—

> ***"One of the benefits of the program is the variety of courses that are made available to participants through the National Cryptologic School. The program had a set curriculum of standard courses and once completed the electives available ranged from information operations to collection management to advanced analytic tools. With advice from panel members, program glide paths were tailored to compliment work center assignments and steer the direction of each individual's program."***[5]

As a final work center, the warrant officers will culminate their WOCCP experience by working in the Army Technical Control and Analysis Element or the Army Cryptologic Operations office. This assignment prepares them to support the operational needs and current operating tempo of their gaining unit. This final work center is typically 60-90 days in duration.

Guidance during the Program

An executive panel for the Director, NSA/CSS manages the WOCCP. A senior military officer on the panel in the rank of colonel, and a senior warrant officer advisor in the grade of chief warrant officer 4 or chief warrant officer 5, in addition to a civilian senior level executive manager represents each of the services. Participants receive supervision and mentorship from both the 704th MI Brigade senior warrant officer and the Director of the Army Cryptologic Operations Office who is the current Army executive panel member.

Day-to day guidance and daily operations of the WOCCP falls to a civilian executive agent who directs each participant through the academic and work center requirements. The daily operations of the JOCCP, WOCCP, and MECCP all fall to the executive agent for the programs, Mr. Christopher Callahan. When asked for his comments about the program, he said—

> ***"WOCCP graduates leave the program with newly acquired skills in a variety of cryptologic disciplines. This broadened exposure prepares warrant officers for future SIGINT leadership roles at the tactical and national levels. SIGINT skills acquired also provide participants with an in-depth understanding of NSA/CSS and relationships within the national intelligence community. Upon graduation, WOCCP graduates should be able to deploy and operate in a multitude of environments. At a high level, graduates learn SIGINT capabilities and processes, build NSA relationships, and contribute to joint service mission success. The knowledge gained in analysis and reporting, fielding of collection systems, cyber operations, reach back to NSA through key points of contact, policy guidance, information operations, and support to military operations prepares them to assume one deep positions. The networking relationships with 40-50 joint service participants in the program bodes well for coordination throughout the intelligence community"***[6]

Assignments Following WOCCP

Regarding follow-on assignments, MG Fogarty emphasized that his intent in creating the WOCCP was for graduates to benefit the Army. He stated—

> ***"I want Army SIGINT warrants to be the most proficient SIGINT practitioners in the world and I believe the opportunities provided by WOCCP accelerates us toward that goal. But, this is critical. I did not intend for graduates to ensconce themselves in NSA for the remainders of their careers. I want them to get back out to the tactical force, work and solve the hard problems, to train, to encourage, mentor the next crew of WOCCP participants. It is also vital that those who accept the privilege of joining the program agree to be accessible wherever they are to help their fellow warrant officers solve their difficult challenges."***[7]

HRC coordinates with WOCCP leadership to place graduates in specific assignments where they can best serve the Army. Follow-on assignments include but are not limited to—

- ✦ Combatant commands.

- Army service component commands.
- Corps G-2/United States Forces Korea J-2.
- Special mission units.
- Expeditionary military intelligence brigades.
- U.S. Army Intelligence Center of Excellence.

Efforts are also ongoing to align the WOCCP with JOCCP by assigning graduates an additional skill identifier, 3W, that will assist in force management through the course of their careers.

COCOMS | ASCCs | Corps G2 | SMU | E-MIBs | USAICoE

Eligibility

Active Component MOS 352-series chief warrant officer 2s and chief warrant officer 3s with less than one-year time in grade at the beginning of the internship program may apply for the program. Interested warrant officers should refer to the U.S. Army MI program MILPER message for further information, or visit the WOCCP Wiki page on NSANET at https://wiki.nsa.ic.gov/wiki/WOCCP. HRC typically issues the annual MILPER message between June and August. For reference, refer to MILPER message 16-160 dated 10 June 2016.

Conclusion

The WOCCP is a unique opportunity for selected warrant officers to focus exclusively on learning about the NSA/CSS as an organization and how it ties into the Army and greater intelligence community. Warrant officers have the opportunity to accrue hundreds of hours of relevant training taught by subject matter experts in the field and use it in tailored assignments focused on real world missions. Participants learn how other agencies and services operate together to accomplish a wide array of missions. This understanding gives the warrant officer the breadth of knowledge for future assignments, and depth to understand how to integrate with other agencies and services to succeed in any operational environment. A warrant officer graduate of the WOCCP is a force multiplier able to offer guidance to commanders and maintain success at leveraging the capabilities NSA possesses to fulfill the commander's tactical, strategic, and operational requirements. WOCCP graduates receive a world-class SIGINT education and take that knowledge and experience with them, to benefit the Army and their gaining unit.

Endnotes

1. CW5 Wendy Wayman, Command Chief Warrant Officer, Intelligence and Security Command provided this information through a March 2017 email inquiry by the authors in which they asked about the program, its history, and how it benefits the Army.

2. This March 2017 quote from MG Stephen G. Fogarty was in response to an email inquiry from the article authors in which they asked about the history of the program.

3. This March 2017 quote from CW2 Joseph Feist was in response to an email inquiry from the article authors in which they asked how the program had opened his eyes to SIGINT across the force and how the program made him a force multiplier for their next unit. Additionally, they were asked what his best assignments were while part of the program.

4. This March 2017 quote from CW3 Kevin Nungester was in response to an email inquiry from the article authors. A current participant CW3 Nungester was asked the same questions as CW2 Feist in note 3 above, how had the program opened his eyes to SIGINT across the force and how had the program made him a force multiplier for his next unit. He was also asked what his best assignments were while part of the program.

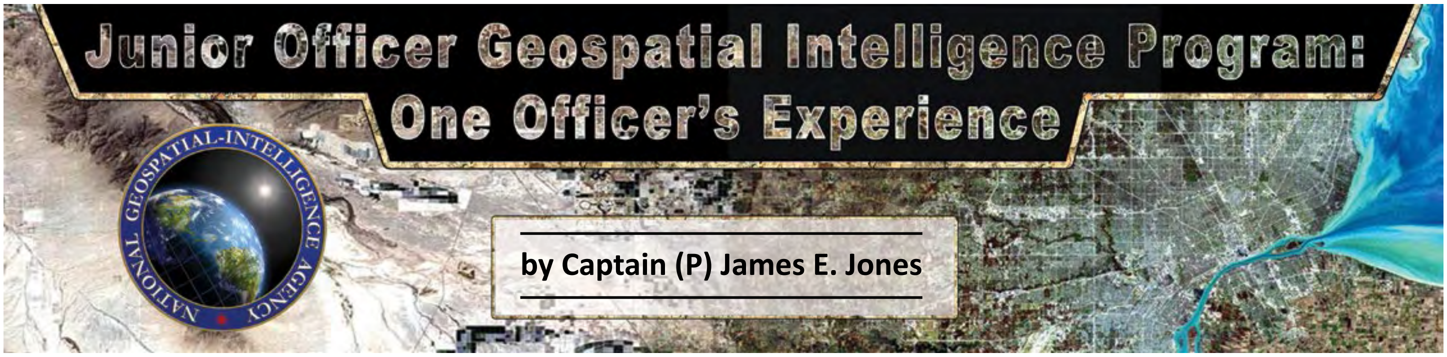
5. This March 2017 quote from CW3 Kathy Hall was in response to an email inquiry from the article authors. As a former WOCCP participant CW3 Hall was asked the same questions as CW2 Feist and CW3 Nungester in notes 3 and 4 above, how had the program opened her eyes to SIGINT across the force and how had the program made her a force multiplier for her next unit. She was also asked what her best assignments were while part of the program.

6. This March 2017 quote from Mr. Christopher Callahan was in response to an email inquiry from the article authors in which they asked for an overview of the program from his perspective as the executive agent.

7. This March 2017 quote from MG Stephen G. Fogarty was in response to an email inquiry from the article authors in which they asked how the Army benefits from the program.

CW2 Shawn King is a first year WOCCP intern at the 741st Military Intelligence Battalion, Fort Meade, MD. His previous assignments include the 204th Military Intelligence Battalion, Fort Bliss, TX, as SIGINT officer in charge, 1st Battalion, 10th Special Forces Group, Panzer Kaserne, Germany as Special Operations Team Alpha team leader, and 3rd Military Intelligence Battalion, Camp Humphreys, Korea as a linguist and operator supervisor. His combat and operational deployments have supported Operation Enduring Freedom and Operation Observant Compass. CW2 King holds a master's degree of management and leadership from Liberty University in Virginia.

CW2 Dubby Black is a SIGINT Analysis Technician in his first year of the WOCCP. He is currently assigned to the 741st Military Intelligence Battalion, 704th Military Intelligence Brigade, Fort Meade, MD. His prior assignments include Bad Aibling Station, Germany; Fort Bragg, NC; Fort Meade, MD; and Stuttgart, Germany.



Junior Officer Geospatial Intelligence Program: One Officer's Experience

by Captain (P) James E. Jones

Introduction

My journey into the world of geospatial intelligence (GEOINT) began in the summer of 2015 when I arrived at the National Geospatial-Intelligence Agency (NGA). I had just earned a master's degree in geospatial information science and technology from North Carolina State University, funded through the Army's Advanced Civil Schooling Program, and was eagerly seeking out an opportunity to use my new skills. Previously, I had been assigned to various engineer and branch immaterial positions, including stints in S-3 operations offices, construction units, and a battalion headquarters and headquarters company command in Afghanistan. In Afghanistan, I regularly used maps, imagery, and web based geospatial applications like GoogleEarth and the Tactical Ground Reporting System, but the fact that I was leveraging one of the most essential forms of intelligence never crossed my mind. That has since changed thanks to a relatively new NGA program called the Junior Officer GEOINT Program (JOGP).

In the summer of 2014, the NGA officially started an umbrella internship program called the Military Service Intern Program, consisting of a 3-year GEOINT Career Advancement Program (GCAP) for noncommissioned officers and a 2-year Junior Officer GEOINT Program (JOGP) for company grade officers. Both programs were created with the intent of building a cadre of highly qualified service members who can fulfill managerial and technical GEOINT requirements within their respective services and the National System for GEOINT (NSG); GCAP focusing on GEOINT Analyst development and the JOGP on developing senior GEOINT supervisors and functional managers.

The NGA selects interns from all military services and provides them with classroom training, professional credentialing, and the opportunity to meet, collaborate, work with, and learn from leading experts and GEOINT practitioners. In return for hosting these service members, the NGA and its civilian workforce are enriched with the experience and perspective of the warfighter, lasting intra-NSG partnerships are formed, and future leaders within the military services gain understanding of the mission, intent, policy, and procedures of the NGA, thus strengthening the bond between services and the NGA.

The JOGP and GCAP both revolve around four key requirements that result in a depth and breadth of experience that meets the program's stated objectives. Upon completion of these requirements, interns return to their services as expert GEOINT analysts and managers, prepared to lead their respective GEOINT organizations in accordance with national standards and the needs of their services. The JOGP and GCAP program requirements are:

- Complete 500/1000 (JOGP/GCAP) hours of approved NGA college course work.
- Earn GEOINT Professional Certification (GPC) Fundamentals/Level II (JOGP/GCAP).
- Complete three/four (JOGP/GCAP) six-month work cell rotations throughout the agency.
- Become a certified NGA college adjunct professor, qualified to instruct NGA courses.

The Intern Experience

My first months at the NGA main campus in Springfield, Virginia, consisted of back-to-back NGA college courses covering a wide array of GEOINT topics, from high-level national GEOINT policy to analyst level GEOINT data retrieval and exploitation. During this time and between subsequent work cell rotations, I completed over 1,000 hours of courses on topics such as our nation's satellite constellations, including a course at the National Reconnaissance Office. I received training on the software and procedures for retrieving, processing, and analyzing both imagery and geospatial data. I took courses that detailed the interagency network of GEOINT partners forming the NSG, and participated in leadership, critical thinking, and intelligence briefing/writing classes. I also completed technical courses in GEOINT phenomenology, covering the fundamentals of collection through exploitation of electro-optical, thermal infrared, synthetic aperture radar, full motion video, ground moving target indicator, and more. This period was critical to the development of my overall GEOINT capability and provided me with the core skills required to take and pass the GPC-Fundamentals exam; a newly accredited national certification that signifies a person's knowledge of the NSG and GEOINT policy.

After building a solid GEOINT knowledge base and proficiency level, I began the core element of the program by working at the NGA Source Key Component (KC), the second largest NGA office. The Source KC helps fulfill the GEOINT enterprise's almost insatiable need for data—an impressive feat. During this rotation, I worked with nine different sub-offices split between two major divisions, Foundation and Collection.

During my time in the Foundation Division, I spent between 2 and 4 weeks in each of its four sub-offices—the NSG Operations Executive (NOX), Content Management, Geography, and Geomatics. From the Foundation Division I gained an understanding of how—

- Foundation data is requested, prioritized, and tasked at the national level.
- GEOINT data is conflated and published for GEOINT community exploration and retrieval.
- Physical features are extracted into geospatial data.
- Maps are made and quality controlled.
- The earth geographic system and gravitational model are surveyed and maintained.

After the Source Foundation Division rotation, I moved into the Source Collection Division, which as its name indicates, is focused on collecting traditional and non-traditional imagery, open source GEOINT, and statistics on collection performance. While there, I spent weeks with the Commercial Collection Branch, Airborne Coordination Element, Collection Throughput and Analysis Branch, a Regional Integrated Strategies Team, and the Aerospace Data Facility. From these offices, I learned how GEOINT needs are turned from simple requests into validated requirements to leverage collected data via government means, ranging from ground based images to data collected by satellites thousands of miles in the sky. Throughout these rotations, I completed real world GEOINT projects in support of the offices that hosted me, including geospatial and imagery related assignments that prepared me to take and pass the GEOINT Professional Certification - Geospatial Analysis Level II exam.

One of the greatest opportunities afforded me was the chance to complete a six month deployment to the Resolute Support (RS) Mission Afghanistan Headquarters, in Kabul, Afghanistan. Early into my NGA experience, I decided I wanted to directly apply GEOINT during real world operations. I reached out to the NGA Volunteer Deployment Team and received full support from the JOGP management team. I completed the required NGA testing and board review, and was selected to serve as the NGA Analytic Site Lead in the RS HQ Combined Joint Intelligence Operations Center – Afghanistan. This period would prove to be the defining experience of my internship. It was here that I had the opportunity to lead a team of four NGA civilian analysts. My team answered over 400 requests for information using a full range of GEOINT products from basic electro-optical imagery analysis through advanced geospatial analysis. As site lead, I received intelligence requests from throughout RS and applied the knowledge I gained from the JOGP experience to direct team production, assure the quality of products, and personally complete numerous GEOINT projects. The six months of GEOINT management experience in a real world combat support role solidified many of the lessons I had learned at NGA and provided an irreplaceable experience in the application of GEOINT to military operations.

Upon returning from deployment, I began my current rotation as an adjunct professor in the NGA College,

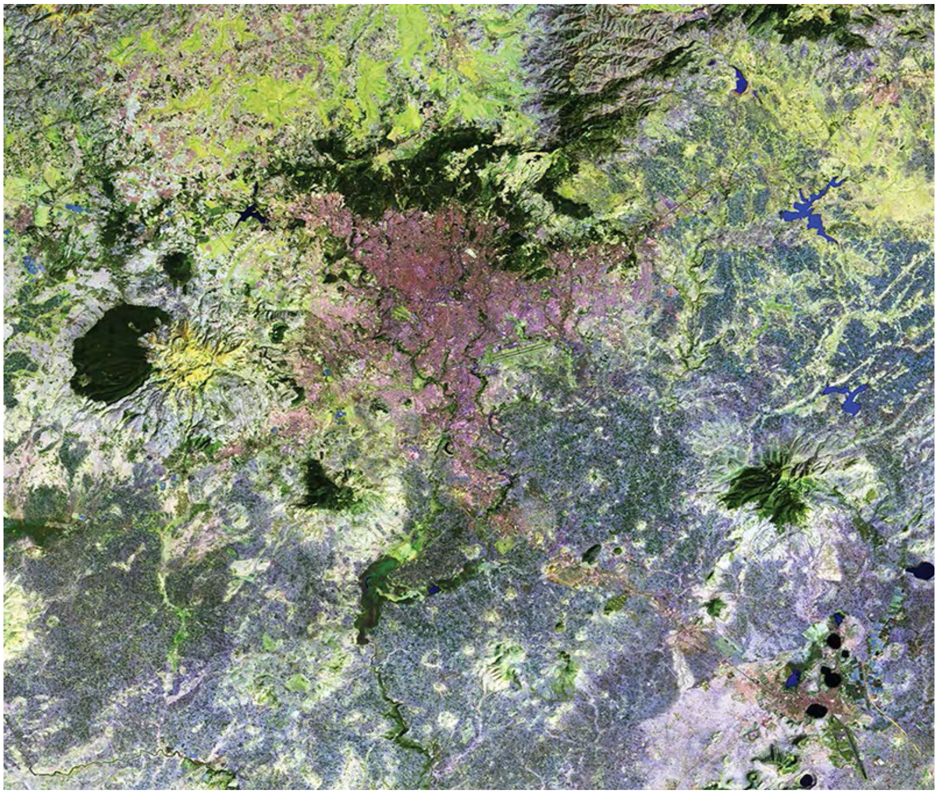


Photo from Wikimedia Commons - Public domain where I teach Fundamentals and Intermediate Geospatial Information System courses. To become a certified adjunct professor, interns first complete the NGA's weeklong Fundamentals of Instruction Facilitation course to become qualified to teach NGA courses according to the adult learning methodology. Then interns are certified to instruct specific courses after teaching the course twice with a full time instructor present. The adjunct/intern is able to teach the course alone, awarding students official NGA certificates upon completion. As long as interns maintain their certification by instructing 80 hours of class per year, they will be available to teach and award NGA certificates at follow on duty stations after leaving the NGA.

Program Benefits

Overall, the JOGP has proven to be the U.S. government's premiere GEOINT officer training program. To summarize the key elements that make this program exceptional and essential to a robust GEOINT capability for the U.S. military, I would categorize the benefits into four areas—networking, GEOINT expertise, leadership opportunities, and service return on investment.

Networking. The JOGP puts service members in the same room as subject matter experts and leaders across the spectrum of GEOINT organizations. Other than the obvious technical skill development that comes from working directly with GEOINT analysts, the JOGP also provides significant opportunity for interns to attend senior level GEOINT meetings, meet and brief executives, and collaborate with a diverse set of GEOINT mission partners. Since I started the program, I have had the privilege of—

✦ Meeting numerous Senior Executive Service leaders throughout NGA's various offices.

✦ Regularly attending Army specific gatherings, such as Army GEOINT Office and Geospatial Enterprise Governance Board meetings, to discuss Army GEOINT policy.

✦ Providing input to geospatial engineer training through the Training and Doctrine Command Capabilities Manager for Geospatial.

✦ Meeting all seven geospatial planning cell commanders.

Simply getting interns together with such a huge array of leaders helps to "flatten" the GEOINT enterprise's organization, which enables collaboration and coordination between GEOINT entities once interns return to their service.

GEOINT Expertise. Perhaps the most essential element of the intern program is the GEOINT expertise gained. In addition to the top-notch classes provided by the NGA College, interns work directly with subject matter experts on real world projects during their work cell rotations. During my time at NGA's Source KC, I completed numerous projects such as extracting features from imagery and converting them into geospatial data in the Middle East for mapping purposes, and acquiring and publishing Army Geospatial Center engineering data on official NGA data repositories, all in a collaborative environment with seasoned experts.

Interns attend professional conferences and conventions, such as the ESRI Federal Convention, NSG Foundation GEOINT NOX Forum, and the Motion GEOINT Community of Practice, to keep abreast of emerging technologies, capabilities, and policies. Interns also regularly conduct site visits to other intelligence agencies, such as the National Security Agency, National Ground Intelligence Center, and the Federal Bureau of Investigation to learn about their capabilities and their ties to the NSG. These experiences combine to provide interns with a solid understanding of GEOINT and its application to answering intelligence requirements.

Leadership Opportunities. Both the GCAP and JOGP provide service members the opportunity to take a leadership role on projects. The JOGP is especially oriented towards providing officers with the opportunity to lead in the GEOINT field. This occurs by assigning officer interns to team lead or project lead positions within an NGA branch, where the officer prioritizes efforts, leverages team experience, and ensures quality completion of requirements. Officers receive the opportunity to solidify their newfound knowledge and develop the instinct and experience desired in a military GEOINT leader. In addition to these team and project lead positions, interns are given the chance to teach, coach, and mentor military and civilian employees from throughout the services and intelligence community at the NGA College. This alternate form of leadership not only increases the officer's knowledge of the topic they are teaching, but also bolsters an officer's skills in problem solving, public speaking, and general instruction; all of which are highly coveted among the services.

Return on Investment for Services. Giving up high quality commissioned officers and NCOs for two to three years is obviously a serious investment and is a topic that has been discussed at length within the Army engineer and military intelligence branches. While definitely a considerable time investment, what the Army obtains in return makes the investment worth the cost. JOGP interns return to the force with invaluable experience and knowledge making them particularly well suited to lead the Army geospatial and GEOINT organizations. The Army is returned leaders with real world GEOINT experience acquired through work cell rotations, professional training, and team and project lead assignments, who are nationally credentialed via the GEOINT Professional Certification and certified to instruct on behalf of the NGA. These are the experiences needed within the Army.

Photo from Wikimedia Commons - Public domain

Conclusion

The JOGP provides officer interns with an unparalleled education and training experience that simply cannot be replicated at the service level. The NGA's position as national functional manager for GEOINT means interns are ideally placed where they can keep abreast of new and emerging national level policy decisions, technology, and analytic methods, and maintain direct relationships with senior leaders and subject matter experts within the GEOINT community. In return for sending qualified officers, the Army gains leaders well versed in geospatial-intelligence who are trained and ready to advance the tradecraft in both the engineer and military intelligence fields. The Army must make this investment in the professional development of today's junior leaders to shape them as tomorrow's senior GEOINT leaders. Luckily, the Junior Officer GEOINT Program can assist the Army in this endeavor.

CPT (P) James E. Jones is an engineer officer assigned to the National Geospatial-Intelligence Agency (NGA) under the Junior Officer GEOINT Program, where he currently serves as an adjunct professor in the NGA College. His previous assignments include horizontal construction platoon leader, company executive officer and battalion construction officer (Operation Iraqi Freedom 2008-09), battalion and brigade assistant S-3, and company command (Operation Enduring Freedom 2012-13). He holds the W2, Geospatial Engineer, additional skill identifier, a bachelor of arts from Ohio University, and a master of geospatial information science and technology from North Carolina State University. His next assignment will be to the Command and General Staff College at Fort Leavenworth, KS.

The U.S. Army Intelligence Center of Excellence–Communications-Electronics Research, Development and Engineering Center Military Intelligence Program

by Colonel William G. McDonough, Colonel Matthew F. Schramm, and Chief Warrant Officer 3 Cynthia K. Louie

Introduction

A new opportunity exists for military intelligence (MI) professionals to contribute and make a difference in developing intelligence capabilities for future forces operating in complex, uncertain, and changing environments in the next 5 to 30 years. This professional development opportunity allows select intelligence Soldiers to be key user representatives helping manage doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) integration. This integration supports resourcing, testing, fielding, and sustaining of new and existing hardware and software advancements for existing intelligence capabilities in the form of enhancements. Additionally, these Soldiers will witness and contribute to innovation and the development of intelligence capability advancements for the future force. This experience is different, exciting, and challenging; something a vast majority of MI professionals will never encounter in their career.

The U.S. Army MI Corps has a lack of intelligence professionals who understand the Army's science and technology (S&T) enterprise. Nor do they understand its relevance and importance to the MI Corps in developing and delivering intelligence capability to the force. A majority of the Army's S&T enterprise resides in the Army Material Command's subordinate Research, Development & Engineering Command, which is comprised of the Army Research Laboratory and several Research, Development & Engineering Centers (RDEC). The Army's S&T enterprise exploits opportunities to provide increased capability to the current force and researches technological capabilities for the future force. Understanding the Army's current and future capability needs is a key driver for the Army's S&T enterprise. The U.S. Army Intelligence Center of Excellence (USAICoE) provides intelligence capability needs to a particular RDEC—the Communications-Electronics Research, Development and Engineering Center (CERDEC). There are other efforts to increase the collaboration between the Army's MI Corps, other sister services, and the S&T enterprise. For example, the Massachusetts Institute of Technology's Lincoln Laboratory Military Fellowship Program. Despite these cooperative efforts, seams still existed. In 2015, an ideal formed to increase the engagement and bond between the USAICoE and CERDEC.

Background

In the fall of 2015, after discussions with the Director of CERDEC, the Director of USAICoE's Capabilities Development and Integration Directorate (CDID) proposed the idea of creating a new MI program between USAICoE and CERDEC. USAICoE is the Army's proponent for intelligence training, education, concepts, doctrine and integrated capabilities and CERDEC is the Army's lead for S&T development in the domains of cyber operations, electronic warfare, signals intelligence technologies, radar, and information systems and processing. The CDID is USAICoE's lead for concepts, doctrine, and integrating capabilities for both Army and joint forces.

A key component of the CDID effort is a 30-year intelligence modernization strategy to integrate capability developers, materiel developers, training developers, and the supporting S&T community; identify essential tasks and other planning factors; and align strategy actions to meet the visions and tenets of the Army Operating Concept and support the Army Functional Concept for Intelligence. Correspondingly, the Army's S&T community also has a 30-year portfolio plan across the acquisition lifecycle phases to assess strengths, weaknesses, understand opportunities vice threats, define critical capability gaps, and refine S&T initiatives to close capability gaps. The USAICoE–CERDEC relationship is critical to assist CERDEC's understanding of unique Army intelligence warfighting function problems, provide knowledge of an uncertain future operational environment, work in partnership to ensure that applications research focuses on specific and prioritized military intelligence problems, and assess the military utility of advanced S&T development.

Unfortunately, very few MI Soldiers understand the S&T partners who are critical for developing or contributing to potential military intelligence capabilities. Placing MI Soldiers into the CERDEC organization for a period was a logical decision since CERDEC is the Army's lead for S&T development in many of the same areas of interest to the USAICoE CDID. These Soldiers will have myriad face-to-face interactions with CERDEC S&T developers and contribute ideas to CERDEC efforts. After a period, those Soldiers return to Fort Huachuca, Arizona, into the CDID to use their knowledge and ties with CERDEC to facilitate the CDID's efforts at a 30-year intelligence modernization strategy.

USAICoE's Commanding General approved the USAICoE-CERDEC MI program in December 2015. The CDID and the U.S. Army Human Resources Command (HRC) military intelligence branch chief quickly established a mechanism for the pilot year and subsequent years.

Concept of Operations

Conceptually, a snapshot of a one-year cycle for selection to the USAICoE–CERDEC program would follow this sequence:

- HRC generates a MI programs military personnel message in the summer for all MI programs.
- Soldiers submit their prioritized preferences (approximately July/August) and a selection panel considers applicants for programs in which they are eligible (approximately September).
- In December or January, selectees and non-selectees are informed.
- Selectees report to CERDEC in the summer to begin the program.

Currently, this MI program is limited to a modest investment of two Soldiers per year. The ideal mix is:

- A 35D, All-Source Intelligence Officer.
  - Captain or major who is key developmental complete and has completed the Captain's Career Course (for captains) or Intermediate Level Education (for majors).
- A chief warrant officer 3 or chief warrant officer 4 who has completed the MI Warrant Officer Advanced Course, and holds one of the following MOSs:
  - 350F, All-Source Intelligence Technician.
  - 350G, Imagery Intelligence Technician.
  - 352N, Signals Intelligence Analysis Technician.
  - 352S, Signals Collection Technician.
  - 353T, Intelligence/Electronic Warfare Equipment Technician.

USAICoE–CERDEC program candidates report to CERDEC at Aberdeen Proving Ground, Maryland, between July and August for a one-year tour. After the first year at CERDEC, Soldiers spend an additional two years at Fort Huachuca, Arizona, for a utilization tour in the CDID.

Year One

While at CERDEC for the first year of the program, Soldiers are assigned to the CDID at Fort Huachuca, Arizona, and are attached to CERDEC at Aberdeen Proving Ground, Maryland. Soldiers learn the S&T process, gain Program Objective Memorandum experience, learn about the CERDEC organization and stakeholders, and learn how CERDEC works with the Program Executive Offices and acquisition communities. Soldiers provide CERDEC with a military perspective and current tactical and operational expertise for their portfolios and S&T efforts.

For the pilot year (2016-2017), the Military Deputy Director at CERDEC, the Deputy CDID Director, and the first MI program Soldier established a framework for MI program personnel to use during their tour at CERDEC. At this current time, the next two selectees will have started

Photo by Kelly White, U.S. Army CERDEC

CERDEC engineers give an overview of the C4ISR Systems Integration Laboratory to BG Patricia Frost, Director of Cyber, Office of the Deputy Chief of Staff, G-3/5/7 during a tour of the CERDEC Space and Terrestrial Communications Directorate labs to highlight what the S&T Community is doing to support Army's Cyber mission.

their tours at CERDEC using this framework.

Prior to arrival at CERDEC, Soldiers are encouraged to enroll and complete the Defense Acquisition University online course ACQ 101, Fundamentals of Systems Acquisition Management. This will introduce acquisition language, acronyms, and processes. Additionally, Soldiers should attend the resident Capabilities Development Course at Fort Lee, Virginia (preferably within the first few months at CERDEC), which is essential to understanding the Joint Capabilities Integration Development System (JCIDS) process. The JCIDS process is what the CDID uses to support acquisition requirements and evaluation criteria for future defense programs. There are also online prerequisite courses for the Capabilities Development Course. These prerequisites and the Capabilities Development Course are all useful while at CERDEC and in the CDID at Fort Huachuca, Arizona.

Photo by Edric Thompson, U.S. Army CERDEC

Soldiers evaluate one of CERDEC Command, Power and Integration Directorate's Expeditionary Battalion Command Post prototype shelter structure at Network Integration Evaluation 16.1.

After in-processing CERDEC (e.g., routine in-processing, badging, workspace and computer systems), Soldiers are given relatively open access to meetings, working groups, and tours within CERDEC and its directorates. This facilitates information sharing and introductions to project leads, engineers and team members working on myriad ongoing and planned projects within each of CERDEC's Research and Development (R&D) facilities. Attending various meetings leads to awareness of upcoming events and invitations to activities of interest to the USAICoE CDID. The working groups provide awareness of numerous projects at different stages of development and the ideas for new R&D projects involving emerging technology, which could fill known or anticipated future gaps.

In addition to spending time in the CERDEC headquarters learning the fundamentals of CERDEC and cross organization ties and efforts, Soldiers will visit some of the subordinate CERDEC directorates. Since not all of CERDEC's directorates work on intelligence efforts, the visits focus on three of the six directorates. The Intelligence and Information Warfare Directorate (I2WD) at Aberdeen Proving Ground, Maryland is the primary directorate with ties to the USAICoE CDID. I2WD works on reconnaissance, intelligence, surveillance and target acquisition, intelligence fusion and dissemination as well as other initiatives. I2WD develops and applies emerging technology to significantly advance current and future fighting capabilities. They also develop and integrate critical technologies related to information warfare and intelligence systems. One area of interest is Vigilant Pursuit—a platform agnostic system combining human intelligence and signals intelligence capabilities. It provides Soldiers information necessary to identify persons of interest while in the field and uses cross cueing and tipping enabling Soldiers to make decisions that require time-sensitive responses. Another area of interest is the Distributed Common Ground System-Army–the Army's primary system for posting data, processing information, and disseminating intelligence, surveillance and reconnaissance information. The second CERDEC directorate that MI Soldier's will visit is the Night Vision & Electronic Sensors Directorate located at Fort Belvoir, Virginia. They conduct research and development in advanced sensor technology with persistent airborne and ground electro-optic/infrared sensor technologies. The third organization is the Space and Terrestrial Communications Directorate at Aberdeen Proving Ground, Maryland. It is the Army's technical authority to ensure the availability, connectivity, and security of mission critical information in the face of information warfare attacks and unintentional network disruptions.

Soldiers will participate in numerous laboratory tours that highlight R&D efforts and enable information sharing and introductions. Some of the laboratory tours include:

- Power and Integration Directorate
- Prototype Integration Facility
- Space Terrestrial Communications Directorate

- ✦ Joint Satellite Communication Engineering Center
- ✦ Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Systems Integration Lab
- ✦ C4ISR Prototype Integration Facility
- ✦ Information Operation Cyber Lab
- ✦ High Fidelity Lab

Some of the efforts these organizations are working on include:

- ✦ Command posts beyond 2025 to expand their expeditionary functionality.
- ✦ Improving the network during maneuver and expeditionary operations.
- ✦ A CERDEC developed modeling simulation capability called MODESTA to simulate any number of radios or networks desired.
- ✦ Cyber Blitz – a CERDEC effort to assist in future acquisition and materiel development for cyber and electronic warfare initiatives.

MI program Soldiers participate in a variety of conferences, technology enabled capability demonstrations (TECD), and training in the Military District of Washington. The conferences allow CERDEC to educate and inform outside stakeholders on their R&D efforts. CERDEC also receives information on emerging technologies created by civilian companies that can inform CERDEC S&T efforts. TECDs illustrate how CERDEC researches emerging technology and any commercial-off-the-shelf technology that has potential for incorporation into current or projected R&D projects. There are also some training opportunities within CERDEC's I2WD where technical experts present their view of how technologies were, are, and could be used.

CERDEC is involved in multiple partnerships and leverages other military services, agencies (e.g., Defense Advanced Research Projects Agency), academia (e.g., Massachusetts Institute of Technology [MIT]), industry (primarily for technology development to create options for program managers), and international R&D efforts. For example, in January 2017, CERDEC hosted sister service representatives and partners from India focused on C4ISR. As another example, CERDEC works with the MIT Lincoln Laboratory on the modular open radio frequency architecture that directly affects C4ISR and electronic warfare systems.

Additionally, these seasoned MI officers and warrant officers provide valuable and recent tactical and operational experience to CERDEC directorates developing the next generation of the Army's intelligence capabilities. This experience is incorporated into these critical CERDEC efforts:

- ✦ Processing, exploitation, and dissemination
- ✦ Multi-function airborne intelligence, surveillance and reconnaissance
- ✦ Next generation ground multi-intelligence capabilities
- ✦ Cyber
- ✦ Electronic warfare and signals intelligence
- ✦ Integrated air and ground survivability

Years Two-Three

After their year at CERDEC, the MI program Soldiers are brought to Fort Huachuca, Arizona, into the USAICoE CDID for a two-year utilization tour. They bring their knowledge of CERDEC S&T efforts to help develop, assess, manage, validate, and synchronize DOTMLPF-P intelligence capabilities that support Army, joint, interagency, intergovernmental, and multinational partners.

The intent is to place MI program personnel within the CDID where their knowledge of CERDEC and S&T activities can best leverage the capabilities development process. The process provides a means to determine required capabilities, assess gaps, specify risks, and develop DOTMLPF-P solutions. The CDID integrates intelligence capabilities across

Photo by Kelly White, U.S. Army CERDEC

BG (P) John A. George, Director, Force Development, Office of the Deputy Chief of Staff, G-8 visits CERDEC to see what technology opportunities CERDEC is working on to improve and refine the Army Network.

Photo by Kelly White, U.S. Army CERDEC

The Brazilian Army visits CERDEC to facilitate a more effective C4ISR system to improve command and control of the battlefield.

the DOTMLPF-P and all warfighting functions. The CDID also conducts studies and analysis, operational architecture development and integration, science and technology, and force design to support the JCIDS—the formal Department of Defense process that defines acquisition requirements and evaluation criteria for future defense programs.

MI program personnel will directly influence Training and Doctrine Command's Force 2025—a campaign plan that drives proactive, long-term focused modernization out to the year 2040. They will also influence the Army warfighting challenges (particularly situational understanding) as part of the campaign of learning to bridge current to future capabilities by focusing on enduring first-order capabilities the Army must develop to ensure current and future combat effectiveness.

Conclusion

For those who want to push and expand themselves, get outside of their comfort zone, add to their skillset, and make a difference, the USAICoE–CERDEC MI program offers a unique experience in a MI professional's career. This professional development opportunity offers a wide latitude for Soldiers to explore and discover in many areas—science and technology and associated research and development; joint, academic, industry and international partnerships; and getting the right intelligence requirements into the Joint Capabilities Integration and Development System. USAICoE–CERDEC MI program candidates will measure their contributions and accomplishments to the MI Corps in years and decade, not weeks or months. It is truly a broadening assignment that deepens a Soldier's experience base, provides diversification of their skills, and exposes them to an environment that most Soldiers will never know.

COL William G. McDonough is the Deputy Director for the Capabilities Development and Integration Directorate at Fort Huachuca, AZ. He has served for the past 34 years in a variety of assignments as an infantry and military intelligence Soldier to include deployments in support of Operations Hurricane Andrew, Restore Hope, Uphold Democracy, Joint Endeavor, Iraqi Freedom VI, and Enduring Freedom IV, VII, and 13-14. He holds bachelor's and master's degrees in history from the California State University, Sacramento; a master's degree in military operational art and science from the Air Command and Staff College; a master's degree in airpower arts and science from the School of Advanced Air and Space Studies; and a master's degree in strategic studies from the U.S. Army War College.

COL Matthew F. Schramm is the Military Deputy Director for the Communications-Electronics Research, Development and Engineering Center. He is a member of the Army Acquisition Corps and a basic branch Signal Corps officer with previous assignments as the product manager for Program Executive Office Enterprise Information Systems; assistant product manager for Counter Radio Controlled Improvised Explosive Device Electronic Warfare; and various command and staff positions with the 57th Signal Battalion, 1st Squadron, 7th U.S. Cavalry and the 123rd Signal Battalion. He is a graduate of The Citadel and holds a master of business administration from Pennsylvania State University.

CW3 Cynthia K. Louie is the first U.S. Army Intelligence Center of Excellence–Communications-Electronics Research, Development and Engineering Center (CERDEC) Military Intelligence Program candidate currently at the CERDEC at Aberdeen Proving Ground, MD. She has served as a warrant officer in multiple capacities with 8th Army in Korea; 94th Army Air and Missile Defense Command at Hickam Air Force Base, Hawaii; and both the National Ground Intelligence Center and the Intelligence and Security Command at Fort Belvoir, VA. She also served in Iraq in 2003, 2005, and 2006/2007. She holds an associate degree in intelligence studies from Cochise Community College and is a graduate of the Warrant Officer Advanced Course and the Capabilities Development Course.

NSA | CSS

The NSA Director's Fellowship

by Lieutenant Colonel Jeffrey Fair, Lieutenant Colonel Angelina Maguinness (USAF), and Lieutenant Commander Geoff Christmas (USN)

Introduction

In 1976, the Director of the National Security Agency (NSA), Air Force Lt. Gen. Lew Allen, Jr., created the Director's Fellowship Program. Only four years after the creation of the Central Security Service (CSS), the organization charged with integrating the service cryptologic elements with the NSA, Lt. Gen. Allen recognized the need for a program to develop future leaders of the cryptologic community. In 1978 Vice Admiral Bobby Inman, then the Director of NSA (DIRNSA) and Chief of CSS, formalized the program with the service cryptologic elements, establishing nominations and the selection process.

Over its 40-year history, the fellowship has gone through some changes but remains a program to develop future leaders. NSA/CSS Circular 40-12, dated 29 November 1982, states it is designed "to develop the highest potential of military and civilian members of the cryptologic community to enable them to perform as future leaders in the community." The circular goes on to guide the daily activities of the fellows, instructing them "to participate in and observe the decision-making process at the highest level of management and undergo an educational and career development process while making meaningful contributions to the mission of NSA/CSS." The program today still aims to provide officers in the grade of O4 or O5 with a learning environment that develops and hones cryptologic skills and knowledge.

Program Objectives

The objectives of the program, outlined on the senior military advisor's website are to:

✦ Enhance the professional development of high-potential career military officers, so they are able to serve in senior positions in the NSA/CSS global cryptologic enterprise, joint service cryptologic component (SCC) operational commands, SCC headquarters, or to command one of the major cryptologic centers in the future.

✦ Provide an opportunity to make contributions to NSA/CSS and SCC goals via the direction of, or participation in an on-going program, project, or initiative.

✦ Promote a strong working relationship among NSA/CSS major resource authorities, the SCCs and intelligence and information assurance customers.

As evident from the description above and the amount of exposure to senior decision makers within the agency, fellows develop a deep knowledge of the cryptologic enterprise that prepares them well for future assignments across the NSA. In fact, two former fellows reached the general officer ranks—MG Roderick Isler, U.S. Army; and BG Robert Carr, U.S. Army. Both officers later served in senior leadership positions within NSA. Many other fellowship graduates have also returned to NSA to fill leadership roles both at NSA-Washington and within the extended cryptologic enterprise.

The current program consists of four military fellows, one each from the Army, Navy, Air Force, and Coast Guard. The Coast Guard started to participate in the program in 2005 and the Marine Corps' last fellow participated in that same year. The program description in the circular does mention civilian fellows, but civilian participation in the fellowship discontinued when other civilian development programs came online in the early 2000s. While visiting NSA work centers, the fellows often meet civilians who participated in the program in the past and now hold senior positions in NSA leadership. They all are extremely happy to have participated and credited the fellowship with developing a broader perspective of the NSA mission and its capabilities.

Current Participants Observations

Over the last year, fellows received introduction to more of the agency than most civilian employees see over a 30-year career. Fellows visit every part of the agency and discuss mission, capabilities, challenges, and opportunities with leaders who are remarkably candid about how they view their organization. Offices roll out the red carpet for the fellows and provide in-depth briefings on daily operations as well as technical capabilities and technological challenges. Generally, fellows visit an office over the course of a day or two and move on to the next location, making for a constant influx of new information and people. Even though the fellowship only lasts 10 to 11 months, the amount of information presented on a daily basis makes it a challenge to retain and apply.

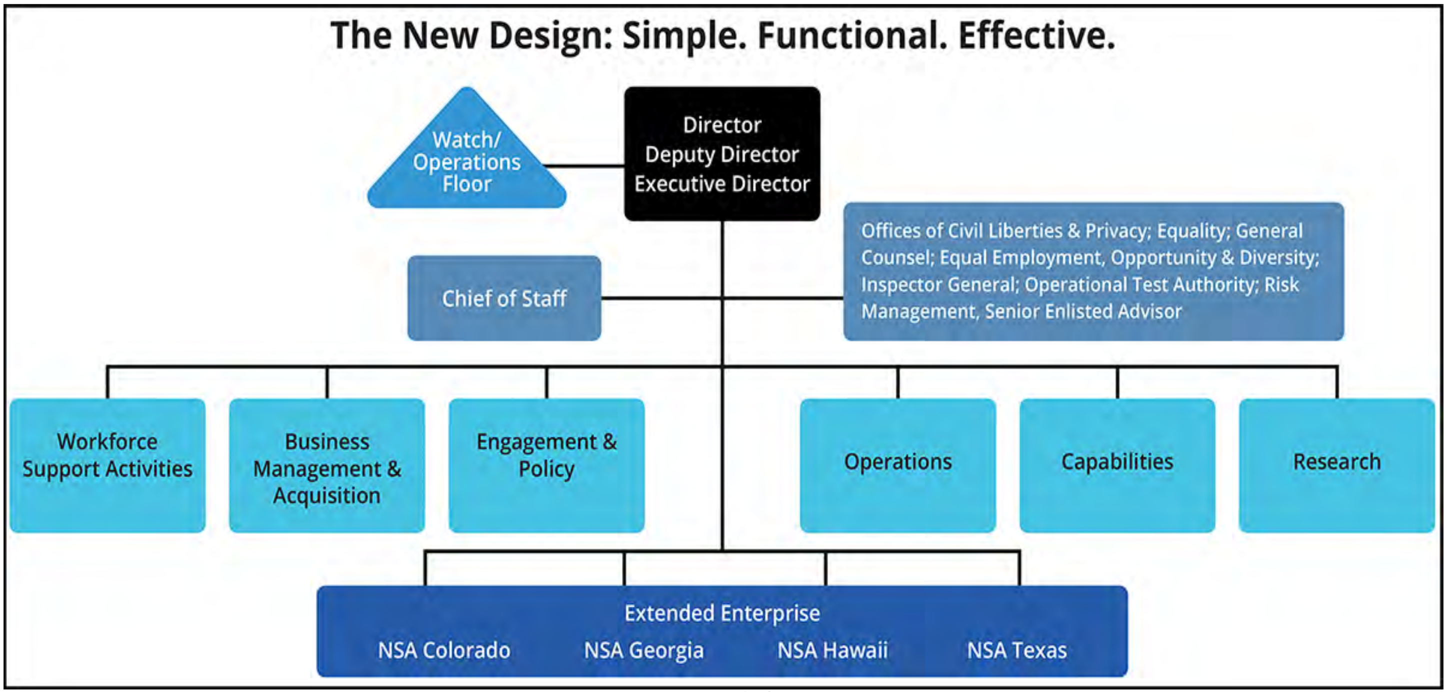
The fellowship begins in August each year, following a July report date and, as with any assignment, mandatory training. Although we were all required to complete the more familiar service-based training, the focus here was the NSA required courses. These classes provide a base of knowledge in diverse topics from the organization of NSA, signals intelligence (SIGINT) and information assurance authorities, policy and regulatory guidance, and basic SIGINT theory. The fellows also have time before the formal portion of the fellowship begins to take classes or seminars in areas of individual interest from the National Cryptologic School at NSA. Two current fellows participated in a great seminar on the NSA and the National Security Council (NSC) that was only a half-day class, but included discussion with the national cryptologic representative at the NSC and NSA staffers for the NSC and the White House Situation Room.

The formal portion of the fellowship begins with visits to each NSA directorate and its component offices. The larger the organization, the longer the fellows are scheduled to stay. Some offices allow the fellows to shadow senior leaders for the day. This year the fellows spent a day with the Deputy Director of Operations, as well as other civilian leaders across the agency. In other organizations, senior leaders hosted the fellows for office calls, initial in-briefs for their organization, and even lunch. The amount of time provided to informing and educating the fellows by leaders across the agency is unparalleled by any other program.

The fellowship also provides opportunities to observe decision making at the highest levels within the agency. Each year the fellows serve as note takers at the Executive Leadership Seminar, a three-day gathering of the NSA senior leaders from across the enterprise held only a few times each year. Fellows also sit in on meetings with the Director and supported organizations such as the joint Special Operations Command or combatant commands. Finally, fellows attend some of the agency's many governing boards and councils, where more routine decisions and program implementation determinations are made. These venues provide eye-opening insight into how not only NSA runs, but also how it is supporting the warfighter.

When fellows visit a work center, people often ask if a project, manuscript, or other yearlong project is required. The short answer is no. Previous fellows proposed the addition of a project, but were reminded the fellowship's goal is to educate participants and provide a broad perspective of a very large organization, not to hone in on one aspect. The program, at various points in the past, had papers and other projects assigned to fellows, but it was heavily dependent on the sitting director and existing agency initiatives.

The focus and overarching theme for the fellows and the program this year is NSA21, or NSA in the 21st Century. NSA21 is massive agency wide reorganization to "position the Agency to meet tomorrow's challenges by staying ahead of threats while effectively leveraging our current missions – thwarting terrorists, protecting the warfighter, enhancing cybersecurity, protecting national security systems and strategic weapons – which are all critical elements in


The New Design: Simple. Functional. Effective.
Watch/ Operations Floor
Director
Deputy Director
Executive Director
Offices of Civil Liberties & Privacy; Equality; General Counsel; Equal Employment, Opportunity & Diversity; Inspector General; Operational Test Authority; Risk Management, Senior Enlisted Advisor
Chief of Staff
Workforce Support Activities
Business Management & Acquisition
Engagement & Policy
Operations
Capabilities
Research
Extended Enterprise
NSA Colorado
NSA Georgia
NSA Hawaii
NSA Texas

NSA21 Redesign.

keeping our Nation safe."[d] The three core tenants of the effort are people, integration, and innovation, all are essential to ensure a forward-looking posture for the agency. Very few parts of the agency were unaffected by the reorganization, which began in earnest in July of 2016.

Because of NSA21, the fellows' tour of NSA has less focus on where the agency is today and more focus on the future of the enterprise. NSA21 presented many offices with major leadership and organizational change challenges. This made work center visits more than just mission, capabilities, and technology briefings, but exchanges about the type of leaders required to manage change on a 40,000-person agency. The lessons learned by one organization are also easily shared with other work centers as the tour continues, making the fellows a unique asset during this time of change. Following the NSA21 structure change, there are few in the enterprise that will have the depth and breadth of new organizational knowledge possessed by this year's fellows.

With extensive focus on the reorganization and the future of the agency, it was an intriguing year to be in the fellowship. Beyond NSA21, there were two other prevalent themes throughout the agency—technological edge and partnerships. Arguably, both of these areas could align under the NSA21 focus areas of innovation and integration respectively, but both require deeper looks than what is included in their NSA21 comparisons.

The NSA is known across the intelligence community (IC) as a technology leader. In the last year, the fellows were exposed to cutting-edge research and development in almost every work center visited. It is important as leaders in such a technology-enabled organization to understand its role, and understand how to foster its continued development. The NSA leads the IC in technologic innovation and integration and the same holds true in cooperation with partners. Both international and IC partnerships are integral to the NSA accomplishing its mission for the nation.

Conclusion

With these themes in mind, the current fellows recommend three books to intelligence professionals seeking to learn more about the NSA. First, GEN Michael Hayden's book *Playing to the Edge* begins with his time as the DIRNSA and provides amazing insight into the last major organizational change the NSA conducted and the challenges created following 9/11.[2] Second, David Priess describes the President's Daily Briefing in his book *The President's Book of Secrets*, explaining where the NSA's goes and how it gets to the President.[3] Finally is Pedro Domingos' *The Master Algorithm*, a layman's guide to algorithms. For liberal arts majors, Domingos' book helps during highly technical briefing with multiple doctorates in varied disciplines as mathematics, computer science, engineering, the physical sciences, and every conceivable language.[4]

The fellowship has been a great opportunity. It provided all of the fellows with invaluable experience in one of the nation's most important intelligence agencies. The professionals who work at the NSA made this an exceptional year, provided access to unique experiences, and shared invaluable insights. We look forward to continued service in the nation's cryptologic enterprise and to making a difference for the warfighter. If you are interested in the program, the U.S. Army Human Resources Command publishes an annual military personnel message containing eligibility requirements and instructions for how to apply.

Endnotes

[1] https://www.nsa.gov/news-features/initiatives/nsa21

[2] Michael V. Hayden, *Playing to the Edge: American Intelligence in the Age of Terror* (New York, NY: Penguin, 2016)

[3] David Priess, *The President's Book of Secrets: The Untold Story of Intelligence Briefings to America's Presidents* (New York: Public Affairs, 2017)

[4] Pedro Domingos, *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World* (New York: Basic, 2015)

LTC Jeff Fair holds a bachelor's degree from the George Washington University, a MBA from Hawaii Pacific University, a MPA from the University of Washington and a MSSI from the National Intelligence University. He is a PhD candidate at George Washington's Trachtenberg School of Public Policy and Administration and is the current Army DIRNSA Fellow.

Lt. Col. Angelina Maguinness holds a bachelor of political science and history from Boston University, a master of military studies–air warfare from the American Military University, a master of military studies from the Marine Corps University and a master of philosophy in military strategy from the School of Advanced Air and Space Studies. She is the current Air Force DIRNSA Fellow.

LCDR Geoff Christmas holds a bachelor of political science from Providence College and a MBA from the University of Phoenix. He is the current Navy DIRNSA Fellow.

NATIONAL INTELLIGENCE UNIVERSITY

Preparing Today's Intelligence Leaders for Tomorrow's Challenges

by Mr. Tom Van Wagner

National Intelligence University: Deep Roots, Bright Future

For more than 55 years, National Intelligence University (NIU) has provided high-quality intelligence education for intelligence professionals. From its humble beginnings in World War II-era wooden barracks in the early 1960s to a brand new, state-of-the art facility in Bethesda, Maryland, NIU continues to prepare military and civilian intelligence professionals to better address the security challenges facing the nation in the coming decades through the application of rigorous academic thought to real-world problems.

Photo courtesy of NIU Outreach

Two distinguished NIU alumni are shown here. MG Paul Menoher, Class of '69 (right), congratulates LTG Sidney T. Weinstein, Class of 1963 on his induction into the MI Hall of Fame in 1990.

NIU Has a Long, Proud History with Army Intelligence

From its very beginnings, NIU has had strong ties to Army intelligence. Immediately after WWII, General of the Army Dwight Eisenhower and Fleet Admiral Chester Nimitz oversaw the creation of the Army Strategic Intelligence School and the Naval Intelligence School, respectively. In 1962, they became the Defense Intelligence School; now the National Intelligence University.

When the first class graduated in May 1963, one of the graduates was CPT Sidney T. Weinstein. CPT Weinstein's distinguished 33-year Army career culminated in his promotion to Lieutenant General and service as the Army G-2 from 1985 to 1989, making him the first of many subsequent Army alumni to lead in the profession.

Today, NIU's Army alumni continue to fill key military and civilian leadership roles in intelligence including, the current U.S. Army Deputy Chief of Staff, G-2, LTG Robert P. Ashley, Jr. (Class of '90); Commanding General of U.S. Army Cyber Command, LTG Paul M. Nakasone (Class of '91); Commanding General of U.S. Army Intelligence and Security Command, MG Christopher S. Ballard (Class of '91); U.S. Army Intelligence Center of Excellence, CSM Thomas J. Latter (UGIP Class of '98 and MSSI Class of '04); and many others. Chances are that if you work in an intelligence unit, you probably know some NIU graduates – just ask around.

Why You Should Be Thinking about Coming to NIU

"We need you," said then-National Security Agency Director, GEN Keith B. Alexander, in recent NIU commencement remarks as he listed U.S. national security challenges ranging from the ongoing conflicts in Syria and Iraq to the downing of a Malaysia Airlines plane in eastern Ukraine. Citing terrorism as their biggest challenge, GEN Alexander charged the students to protect the country. "This is a dangerous time for the nation. You will be leading the intelligence community in providing the information policymakers will need to make good decisions for our nation."

For strategic intelligence officers, NIU is a requirement to qualify for FA34 (Strategic Intelligence), but the student body includes professionals from other officer and enlisted career fields as well—military intelligence, special forces, aviation, medical service corps and others who meet the admissions prerequisites and have the appropriate academic preparation. Full-time attendance requires a nomina-

Photo courtesy of NIU Outreach

Then-NSA Director, GEN Keith Alexander, delivered the commencement address at the annual NIU graduation ceremony on 25 July 2014.

tion from the Army, but more than half of NIU's 700+ student body are part-time students who apply directly to the University for evening or weekend classes at the main campus or at one of the additional academic locations outside the national capital region. NIU has part-time students who work at U.S European Command and U.S. Africa Command in Europe; U.S. Central Command, U.S. Special Operation Command, and U.S. Southern Command in Florida; Fort Gordon, and Fort Bragg.

NIU is the most "joint" of any professional development program in the Department of Defense (DoD) or the intelligence community (IC) because its staff and student body include representation from all branches of the military services and from across the entire national security and intelligence communities. NIU is also the only professional development school in the DoD that is open to everyone from E-5 to O-6 and GG-7 to SES. Academic awards presented at graduation are based on the quality of individual performance and it is not uncommon for noncommissioned officers and junior civilians to earn their share of recognition each year.

Joint Professional Military Education. NIU provides an opportunity for selected students to earn joint professional military education (JPME) Phase 1 credit while enrolled in full-time graduate study, a program that is expected to expand in the coming years. U.S. Army Human Resources Command determines which warrant and commissioned officers are eligible to pursue JPME credit at NIU. Civilians nominated for full-time study in an NIU master's program who are interested in participating in the JPME curriculum may contact the NIU JPME program director directly for approval.

The strength of the NIU JPME program is in its diversity. Unlike service command and staff colleges where classes have a high concentration of officers from their own service, the JPME cohort at NIU comprises a broad cross-section of students from each armed service, the Coast Guard, and civilians from several federal agencies.

In an 11 December 2012 memorandum announcing approval of the NIU JPME initiative, then-Joint Chief of Staff Chairman GEN Martin Dempsey, U.S. Army, wrote:

> ***I applaud the efforts of the NIU faculty, course directors, and staff for developing a curriculum that instills a joint perspective. It provides today's corps with an ability to overcome diverse 21st century challenges and operate effectively in a joint, interagency, intergovernmental, and multinational environment.***

IC Joint Duty Qualification for Civilians. Since 2012, Army civilians and their supervisors have additional incentive to consider full-time study at NIU. By enrolling full-time in one of the three NIU degree programs, civilians can complete mid-career professional education in an accredited degree program while also qualifying as IC joint duty officers. This is a win-win scenario—achieving two professional development milestones in a single year —which maximizes both manpower resources and training/education funds. Rather than lose a top performer for a joint duty assignment and again later for full-time study, supervisors may reward top performers by allowing them to "kill two birds with one stone" at National Intelligence University.

At NIU, You Don't Just Earn a Degree—You Earn a Degree that Allows You to Make a Difference

The NIU is a federal degree-granting institution with a far-reaching mission—to educate and prepare intelligence officers to meet challenges to the national security of the United States. The main campus is located in Bethesda, Maryland, with additional instructional sites in Virginia, Maryland and Florida as well as in the United Kingdom at RAF Molesworth.

NIU provides career professionals a rigorous and collaborative joint-learning environment to hone critical thinking and analytical skills, conduct research on real-world problems, and build trust and mutual understanding that will last a lifetime.

NIU Academic Offerings Include:

- Master of Science of Strategic Intelligence.
- Master of Science and Technology Intelligence.
- Bachelor of Science in Intelligence.
- Graduate certificates addressing intelligence issues in regional areas and special topics.

NIU provides a unique opportunity for students to learn in a classified environment where they may conduct research at all levels of classification up to and including Top Secret/Sensitive Compartmented Information. With faculty and students from every organization in the IC, the setting is truly a joint-learning environment, which facilitates collaborative problem solving.

Learn Directly from Intelligence Community Leaders and Subject Matter Experts. The NIU faculty is a rich body of career professionals that includes long-term resident faculty, military officers on 2 to 3 year teaching assignments with fresh perspective from the field, representatives from IC agencies teaching while on rotational assignment, and adjunct faculty culled from the rich pool of experts in the national capital region.

Photo courtesy of NIU Outreach

The Honorable James R. Clapper was a frequent guest lecturer at NIU while serving as Director of National Intelligence.

Students also have direct contact with IC senior leaders and subject matter experts who serve as guest lecturers in the classroom or as featured speakers in the weekly NIU President's Lecture Series. During the 2016-2017 academic year, NIU students had the opportunity to hear from and pose questions to the Director and the Principal Deputy Director of National Intelligence; the Directors of NGA, NSA and DIA; as well as the heads of intelligence for Marine Corps, Coast Guard, and State Department.

Unique Research Opportunities. At NIU, we believe that producing and publishing research will develop the analytical and creative thinking skills of our students, faculty and research fellows, contribute to the intelligence mission, and spark innovation. The National Intelligence Press—NIU's publishing arm—is expanding the literature of intelligence by publishing books used by analysts, practitioners and educators at a growing number of colleges and universities around the world.

NIU administers research fellowship programs that allow selected analysts to spend a full year at NIU to conduct in-depth research on individual or collaborative projects. As a result of NIU research and publication, there is a growing collection of intelligence literature of more than 60 titles published by NIU's National Intelligence Press. NI Press books are authored by students, faculty, research fellows, international partners, and IC professionals on relevant and timely topics of interest to the community and the U.S. government.

A New Beginning on a New Campus!

In February 2017, NIU relocated to Roberdeau Hall in the Intelligence Community Campus-Bethesda (ICC-B). The new state-of-the-art NIU facility, designed by a firm specializing in academic architecture, was the result of a significant capital investment by IC leadership in the career development of future leaders of the intelligence and national security communities. The new campus is situated in the scenic Palisades, an area along the Potomac River characterized by wooded bluffs and natural vegetation.

The move represents an inflection point in the institution's 55-year history: it is the culmination of the evolution of NIU from a Defense Department schoolhouse housed in WWII-era wooden barracks on a military base in southeast Washington, DC, to a regionally accredited university, situated on an IC campus, serving the entire U.S. intelligence community.

The new Bethesda campus provides more room for NIU to grow and achieve its vision as *the center of academic life* for the intelligence community. It incorporates current best practices in higher education design including a layout that facilitates collaboration. The design of the classrooms provides an environment that is more conducive to the delivery of a broad curriculum, and includes a variety of student labs and student study areas on par with peer institutions.

Faculty and staff spaces are outfitted with updated information technology and communication infrastructure necessary to collaborate with our partners throughout the IC. From a student perspective, one of the best features of the new campus is that there are now plenty of computer workstations—more than double the number at the old campus—an important amenity during mid-terms, finals, and thesis crunch times.

Transforming the National Intelligence University: Strategic Planning 2017-2021

The move to the new campus in Bethesda, which has been termed "an inflection point" in the history of NIU, brings with it the promise of transformation into a nationally recognized intelligence university serving the defense of our Nation. To achieve its mission and vision in an era when resources are expected to remain tight, in 2017 NIU embarked on a new five-year strategic plan with three primary goals to guide planning and resource decisions:

Goal 1: Develop Leadership in the Profession of Intelligence. Emphasis will be applied to maintaining federal degree authorizations and regional accreditation; crafting curricula that anticipate and meet emerging national security priorities; developing a critical mass of faculty with strong academic credentials; producing the highest quality graduates; developing certificate programs which contribute to lifelong learning; and using innovative techniques to deliver education.

Goal 2: Contribute to the Body of Knowledge of the Intelligence Profession and the Intelligence Community and Inform Strategic Intelligence Solutions. NIU will organize and produce research products that invite collaborations with IC leaders and researchers; publish and present cutting-edge research; and strengthen research support.

Goal 3: Fully Integrate NIU into the Intelligence Community. NIU will enable relationships between the University, academics, and key partners that create mutual benefit; actively engage the IC and national security communities to ensure the highest-quality NIU outcomes; and build and sustain an engaged community of current and former students, faculty and staff to enable networked relationships within the intelligence and national security communities, academia, think tanks, and private industry.

Integrating the Intelligence Community One Alumnus at a Time

When you graduate from NIU, you become part of an alumni network that is second to none. NIU alumni are past, present, and future leaders in the intelligence and national security communities, and in the private sector. Notable alumni include a former Director of National Intelligence; former Directors of CIA, DIA, NSA and NGA; former heads of military intelligence; and a growing number of senior government executives and corporate leaders. Just this past year, there were two more notable alumni "firsts" for NIU: our first U.S. Ambassador, Todd Chapman (Class of '00), U.S. Ambassador to Ecuador, and our first member of Congress – Representative Michael Gallagher (R-WI), Class of '10.

We Want to Hear from Our Alumni. NIU is proud of all its alumni and their collective achievements in service to the nation, but there are other reasons we value ongoing contact. Alumni help keep the University relevant and accredited by providing feedback and advice at various points during their careers via alumni surveys. Some alumni return later in their careers as subject matter experts to lecture, to serve as thesis mentors, or to teach. Other alumni return to serve as IC leaders who promote the vision of NIU as the center of academic life for the IC.

NIU Office of Alumni Relations. If you were a student, faculty or staff member at the NIU or its predecessor schools—National Defense Intelligence College (2006-2011); Joint Military Intelligence College (1993-2006); Defense Intelligence College (1983-1993); or Defense Intelligence School (1962-1983)—please contact the Alumni Relations Office (NIU_Alumni@dodiis.mil) so we can update our records and reengage with you!

NIU Alumni Association. Following the establishment of a formal NIU Alumni Association in September 2015 as a component of the 501(c)(3) National Intelligence University Foundation, alumni networks are forming around the country and around the world, promoting lifelong learning, facilitating professional networking, and fostering pride in alma mater. Working closely with the university to promote activities of mutual benefit, the Alumni Association leadership has set up a website for alumni to register as members. There is no cost to join. For more information, visit www.niuf.org.

For More Information and How to Apply

Individuals interested in applying for full-time study at NIU should contact their career manager and refer to the annual military intelligence programs military personnel message: The National Intelligence University (NIU) Master of Science of Strategic Intelligence (MSSI) and Master of Science and Technology Intelligence (MSTI) Programs.

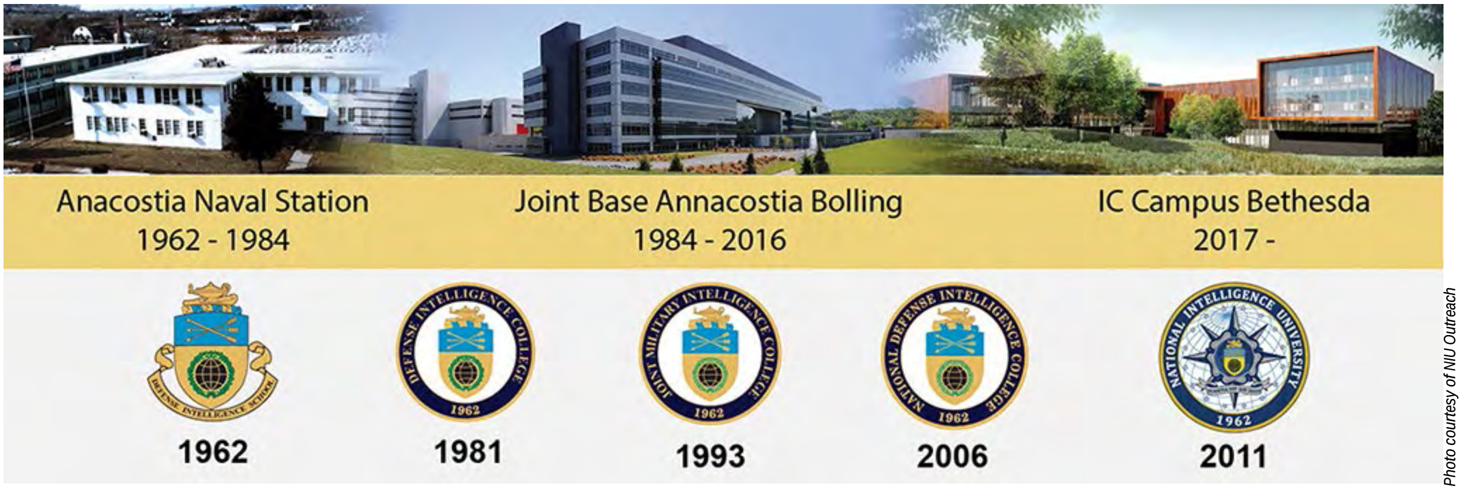


Photo courtesy of NIU Outreach

The main campus move to the IC Campus Bethesda, Maryland represents an inflection point in the 55-year evolution of the University.

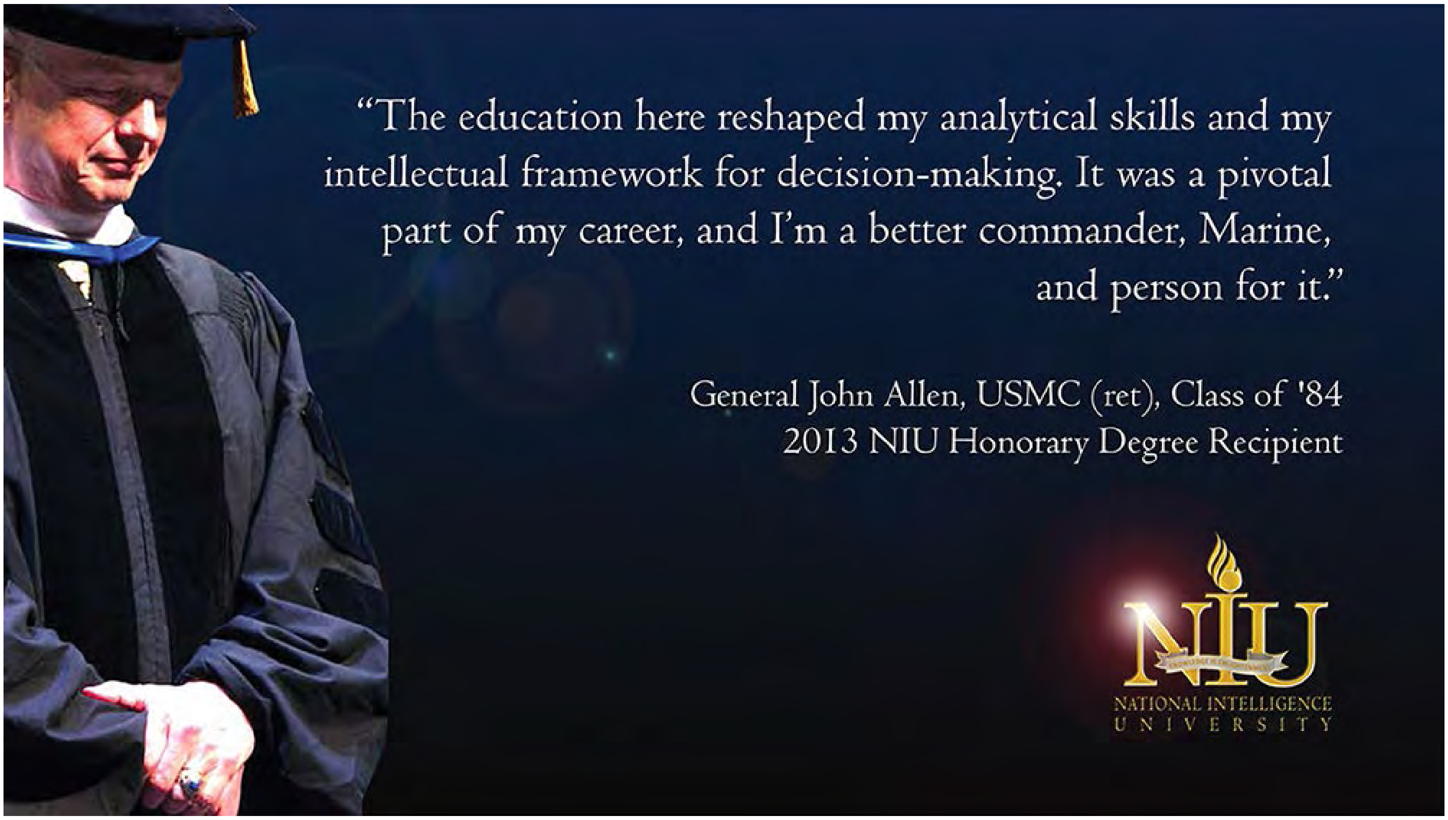
For more information about NIU programs, including part-time study, admissions requirements, application timelines, visit www.ni-u.edu or contact NIU_admissions@dodiis.mil.

For general information, visit www.ni-u.edu or contact NIU_outreach@dodiis.mil.

Courtesy of NIU Outreach

The new NIU main campus is a state-of-the-art facility designed by an academic architect.

Tom Van Wagner serves as deputy vice president for outreach and director of outreach and alumni relations at the National Intelligence University. He has 35 years of federal government service, including 12 years as a navy surface warfare officer. He is a joint-qualified intelligence community officer. Tom earned his bachelor's degree from Colgate University in 1980 and is a 1994 graduate of the Master of Science of Strategic Intelligence Degree Program at NIU.


"The education here reshaped my analytical skills and my intellectual framework for decision-making. It was a pivotal part of my career, and I'm a better commander, Marine, and person for it."

General John Allen, USMC (ret), Class of '84
2013 NIU Honorary Degree Recipient

National Intelligence University Master's Program

by Chief Warrant Officer 4 Wendy Hare

The National Intelligence University (NIU) offers a unique opportunity for intelligence community members, to obtain a bachelor's degree or one of two master's degrees. United States citizens serving in the Armed Forces and Federal government are eligible for this program.

History

During an era of increasing turmoil, such as the U-2 crisis with Russia[1] and the deteriorating situation in Southeast Asia[2], President Dwight Eisenhower appointed a Joint Study Group to examine the organizational and management structure of U.S. foreign intelligence. Eisenhower recognized the need for a new intelligence organization to act as the primary point of coordination for the military intelligence community—a defense intelligence community, a defense intelligence agency.[3]

In January 1961, President John F. Kennedy and Secretary of Defense, Robert S. McNamara, assuming responsibility for national security in the era of Khrushchev[4] and the Bay of Pigs[5], took an interest in the concept of an agency that would integrate military intelligence efforts for all Department of Defense (DoD) elements.[6] In August 1961, the DoD established the Defense Intelligence Agency (DIA). DIA was responsible for the integration of DoD intelligence and counterintelligence training programs and the career development of intelligence personnel.[7]

In 1962, the Office of the Secretary of Defense issued a memorandum to establish the Defense Intelligence School, to consolidate duplicative strategic intelligence institutes. The Director of DIA was tasked to develop a curriculum based on existing Naval and Army Intelligence schools. The focus was on enhancing the preparation of select military officers and DoD civilians for essential command, staff and policy-making positions in the national and international security structure; for duty in the military attaché organization; and to assist the broad career development of DoD military and civilian personnel assigned to intelligence functions.[8]

In 1980, President Carter and Congress passed a law authorizing the Defense Intelligence School to award a master of science degree in strategic intelligence degree. The school was renamed the Defense Intelligence College upon accreditation in 1983. The 1990s brought more change and DIA shifted the school's training courses elsewhere. The college became devoted solely to intelligence education and research.[9] Several more changes occurred between 1993 and today. These include:

- In 1993, the college was renamed the Joint Military Intelligence College (JMIC).
- In 1997, Congress authorized JMIC to award a bachelor of science degree in intelligence.
- In 2006, JMIC changed its name to the National Defense Intelligence College (NDIC).
- In 2010, NDIC established the Science and Technology Intelligence School.
- In 2012, the Department of Education and Congress were issued degree-granting authority, and resulting from establishing a second master's degree program, NDIC was designated a university and renamed the National Intelligence University (NIU).
- In early 2017, NIU relocated from DIA Headquarters at Joint Base Anacostia-Bolling to its new facility on the intelligence community campus in Bethesda, Maryland.[10]

What to Expect

Since my experience involves the Master of Strategic Intelligence Program, this article will focus on personal observations and knowledge. Regardless of which degree, it is likely those seeking to attend NIU will still gather some useful information.

The master's program is eleven months in length, divided into four quarters. During the first quarter, students are assigned to a *track* – a group of about ten personnel, from

First Look at NIU's main campus at ICC-B.

various military and civilian organizations, who provide general support, networking opportunities, and a means of accountability. As with most military educational establishments, the track leader is the senior ranking military member. Students receive assignment of their first quarter schedule of core classes, which the entire track attends. A key course during this quarter focuses on the initial stage of thesis development.

In the second and third quarters, students have the opportunity to arrange their own schedule. Like other universities, class size is limited and certain classes are mandatory, so register early and prepare an alternative schedule. For those seeking to expand their knowledge of the DoD, the intelligence community, and unfamiliar regions of the world, this is the time to select courses that are outside their expertise. Each quarter provides courses to continue refining your thesis topic, to develop a thesis statement, and to learn research methods and identify resources.

The fourth and final quarter is spent writing your thesis. It is due about two weeks prior to graduation. Though students can obtain additional time to complete their thesis after departing NIU, the percentage of those that complete the thesis after departing is statically low. It is in your best interest to finish your thesis prior to departing NIU or you may never graduate.

There are a few additional aspects about NIU I feel it is important to highlight. First, required reading assignments may be daunting. It is not unusual to receive assignments of hundreds of pages per class. It is not possible to complete the required reading in the allotted time and take comprehensive notes. However, it is possible to read the material and take notes of key concepts presented in the textbooks. Be sure to take notes during course lectures, which identify key points. You can always review the text again to prepare for an exam or write an essay.

Second, it took me about a month to realize that I *could* focus solely on my education. As most in the military, I spent years working long hours while attending night school or taking online classes to continue my education. The amount of coursework assigned at NIU quickly became overwhelming and stressful, until my mind made the adjustment. If you experience this phenomenon, just give yourself time to adapt.

Third, some courses may require research and an essay, ranging from 10 to 20 pages in length. Be aware that a certain percentage of these essays may be included in your thesis. Therefore, the sooner you identify your thesis topic, the easier it will be to identify related topics for class papers pertinent for inclusion in your thesis.

During the first three quarters, weekly guest speakers provided insight into their organizations, about their experiences, or about the cause and effects behind historical events. For me, one of the most memorable was the individual from a here unnamed, but well publicized agency, that increased my paranoia about my social media accounts, email, and smart phone. Each guest speaker provided a unique perspective into a variety of topics involving strategic intelligence.

Recommendations for Success

It is important to recognize strengths and weaknesses, not just about yourself but also about the learning environment.

Do you need structure? Can you write well, while omitting the military tone found in Army documents? Do you have a place to study and write, eliminating distractions? If your thesis topic is classified, do the network, available access, and resources meet or hinder your efforts?

When faced with the task of writing a thesis, I found I needed someone to provide guidance on the topic, set deadlines, and hold me accountable to established goals. I also needed to develop my thesis over the course of the year, rather than attempting the undertaking in the final quarter. I expressed this requirement immediately and was directed to a thesis advisor that not only exceeded my needs, but also specialized in all things Russia, my preferred topic for my thesis.

As previously mentioned, during the first three quarters students attend classes designed to narrow and select their thesis topic, develop a thesis statement, and learn research methods. This makes it difficult, though not impossible, for those seeking to develop a thesis over the course of the school year. The greatest hurdle was deciding on a topic. I arrived at NIU with a specific idea, which survived about one day.

The only portion of my thesis idea that survived the thesis process was my intent to focus on Russia. Most students discover that their thesis idea is either too broad, too narrow, or was already undertaken by another graduate. If a topic is too broad, it results in too much information to research and support. If a topic is too narrow, it makes it difficult to meet the minimum page limit for a thesis – typically a minimum of 80 pages, though there were some that were several hundred pages in length. My final thesis discussed Russia's vast energy resources and how they are used to further the nation's foreign policies.

Upon acceptance to NIU, I urge you to contact the school and seek guidance from the appropriate thesis advisor – dependent on area of expertise. They can direct you to resources, such as recommended research topics from the intelligence community, and provide thesis suggestions. If you identify and develop your thesis statement prior to arrival, it will better prepare you for success.

Another very important topic is basic writing skills. My current assignment as a doctrine developer provides the opportunity to review numerous publications. In the last two years, I have read more doctrine than I have previously read in my entire military career. Given my experience, one thing is abundantly clear; many writers do not understand basic grammar, a paragraph's structure, or how to organize paragraphs in a manner that flows from one idea to the next. Find a reference about English grammar and refresh your knowledge.

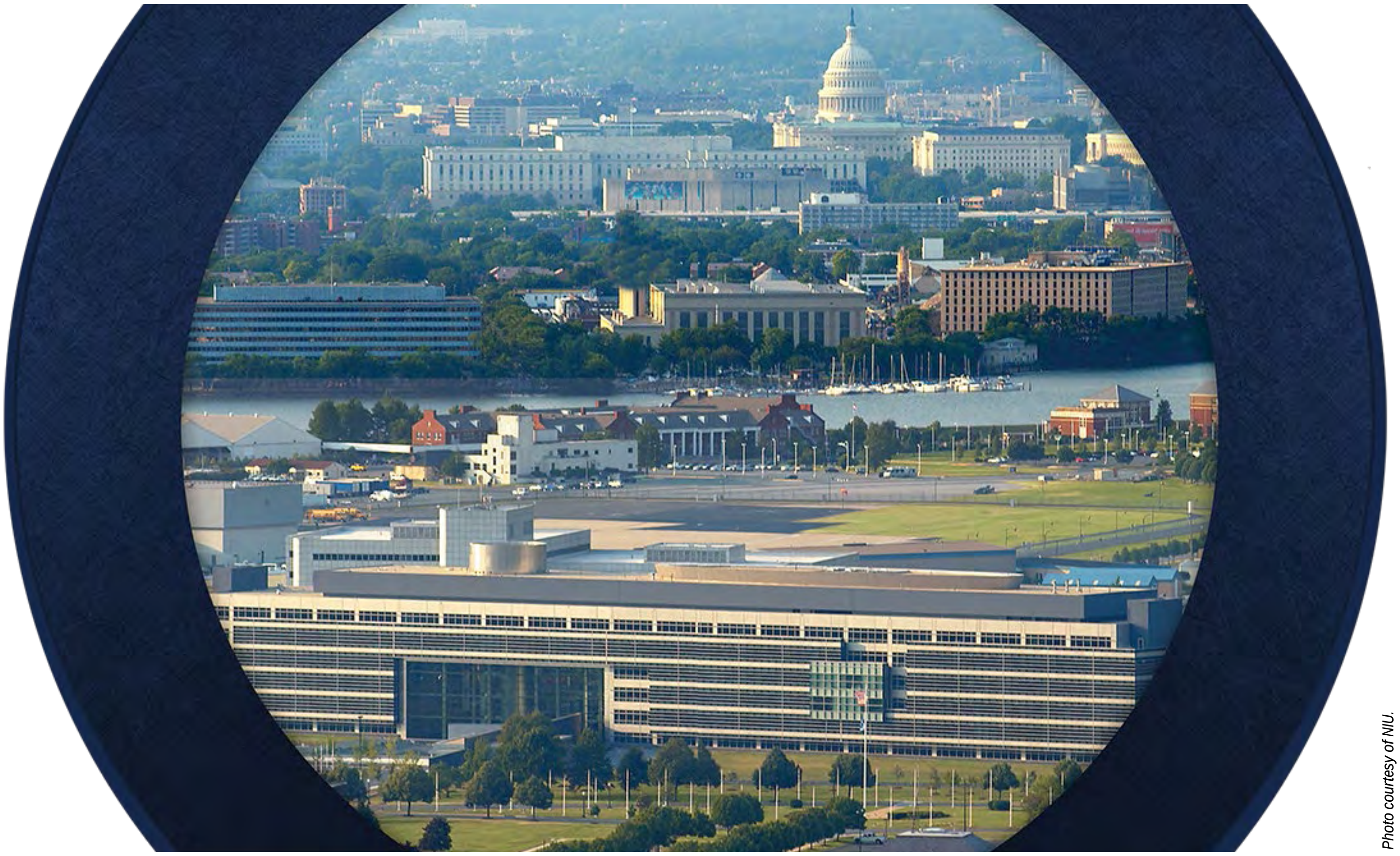


Photo courtesy of NIU.

Eliminating distractions is a necessity. Those with families addressed the issue in a few ways. Some chose to commute to the university each weekday, regardless of their class schedule, and utilized the computer lab. Others established a quiet workspace at home, such as an office. Since my thesis was unclassified, I worked from home and maintained an 8-hour schedule on the days I did not attend classes.

Identify and mitigate network and access challenges early. One issue we encountered was associated with the network. For some unknown reason, my student account seemed to be routed through my previous duty station in South Korea. This meant that it took several minutes every time I opened a document. I realized that the system shortfalls would hamper my efforts, which prompted my decision to write an unclassified thesis. Additionally, the number of classified workstations was limited. The new NIU facility may not present these challenges, but it would be prudent to assess the network and available workstations at the earliest opportunity.

Global Perspective

For Soldiers, our career progression tends to begin at the lower echelons where the focus is narrow and localized. At the tactical level, we focus on the immediate or near term threat. As we advance in rank and experience, our assignments to higher echelons mirror our progress. By the time we reach a division or corps, an intelligence professional should understand the larger global factors contributing to the emergence of local threats. This may be the typical career progression but it is not ideal given today's technology and global awareness.

Regardless of rank or assignment, today's intelligence professional should view their operational area on a global level, by seeking to understand how an event on one side of the world may cause complications in their area of interest. Begin with reviewing the national and defense department strategies.[11] Read the insight provided by think tanks and foreign policy publications.[12] Study the culture, the social norms, and the history of the nation(s) in your operational area. Whether you are able to attend NIU or not, seek to view your assigned region from a global perspective.

The National Intelligence University offers a unique opportunity for military members to enhance their global perspective and learn how world events relate to the nation's security and foreign policies. Graduates also learn about the numerous resources available, such as civilian organizations with decades of experience, which provide finished analytical products on a variety of topics and regional issues. To see if you meet the qualifications needed to attend NIU, visit the admissions page on their site located at: http://ni-u.edu/wp/eligibility-criteria/.

Endnotes

1. U.S. Department of State, "U-2 Overflights and the Capture of Francis Gary Power, 1960," n.d., https://history.state.gov/milestones/1953-1960/u2-incident. The U-2 was a special high-altitude plane that flew at a ceiling of 70,000 feet, developed in response to a growing concern about the relative nuclear capabilities of the Soviet Union and the threat that the nuclear arms race posed to national security.

2. The George Washington University, "Fighting the War in Southeast Asia, 1961-1973," The National Security Archive, n.d., http://nsarchive.gwu.edu/NSAEBB/NSAEBB248/.

3. Director of Institutional Effectiveness, National Intelligence University FactBook: Academic Year 2011-2012 (Washington, DC: National Intelligence University), 1. http://ni-u.edu/wp/wp-content/uploads/2015/01/Factbook2012.pdf.

4. "BBC-History – Historic Figures: Nikita Khrushchev (1894-1971)," BBC News, n.d., http://www.bbc.co.uk/history/historic_figures/khrushchev_nikita.shtml. Nikita Khrushchev served as the General Secretary of the Communist Party of the Soviet Union, the nation's leader, when an American U-2 reconnaissance plane was shot down over Soviet territory in 1960 and during the Cuban Missile Crisis in 1962.

5. U.S. Department of State, "The Bay of Pigs Invasion and its Aftermath, April 1961-October 1962," n.d., https://history.state.gov/milestones/1961-1968/bay-of-pigs.

6. Director of Institutional Effectiveness, NIU FactBook, 1.

7. Ibid.

8. Ibid.

9. Ibid.

10. National Intelligence University, "NIU Begins Historic Move: Main Campus Leaving Washington, DC After 55 Years," National Intelligence University, Defense Intelligence Agency, January 2017, http://ni-u.edu/wp/niu-begins-historic-move-main-campus-leaving-washington-dc-after-55-years/.

11. The National Archives and the Library of Congress house historical documents, including the National Security Strategy and the Defense Strategy. Other resources include the White House site at https://www.whitehouse.gov.

12. Civilian organizations providing finished research or analytical articles are often referred to as a Think Tank. Some resources include: Brookings Institution, the Center for Strategic and International Studies, and the Heritage Foundation. Some publications include World Politics Review at https://www.worldpoliticsreview.com and Foreign Policy at http://foreignpolicy.com/.

CW4 Wendy Hare is a signals intelligence (SIGINT) technician working as a doctrine developer at the U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. Prior to attending the National Intelligence University she was stationed at Field Station Korea for three years, in the SIGINT battalion, serving as the processing and reporting officer in charge, operations assistant, and collection manager. For her post-graduate utilization, she served three years in the 7th Army/U.S. Army Europe G-2 as the requirements manager and as a member of the contingency command post - a deployable element tasked with supporting the commanding general.

National Security Agency/Central Security Service Enlisted Internship Programs

Advanced Training for Exceptional Soldiers

by Mr. Brian Bouchard

Cryptologic Soldiers are highly encouraged to take advantage of the 3-year internship programs that National Security Agency/Central Security Service (NSA/CSS) offers to service members. The military enlisted internship programs the Army participates in are:

- Middle Enlisted Cryptologic Career Advancement Program–for military occupational specialties (MOSs):
  - 35P, Cryptologic Linguist.
  - 35N, Signals Intelligence Analyst.
  - 35Q, Cryptologic Network Warfare Specialist.
  - 35S, Signals Collector.
- Military Language Analyst Program–for MOS 35P, Cryptologic Linguist.
- Military Intern Signals Intelligence (SIGINT) Analysis Program–for MOS 35N, SIGINT Analyst.
- Military Communications Intelligence Signals Analysis Program–for MOS 35S, Signals Collector.

NSA/CSS established these career-enhancement programs in cooperation with the military services, to develop highly skilled cryptologic technicians through advanced formal training and a series of individually tailored operational assignments at NSA/CSS. These internship programs produce highly qualified middle and senior enlisted cryptologic personnel in order to conduct the missions of the U.S. SIGINT System in support of warfighting commanders. Noncommissioned officers (NCOs) have the option to volunteer for deployments or other developmental experiences, while in one of these internship programs. These programs are also an excellent means of identifying and retaining the Army's finest cryptologic NCOs.

Requirements include—

- Having not less than 4 and not more than 14 years total active service.
- Currently serving in the rank of sergeant or staff sergeant.
- Meeting designated time on station requirements.
- Applicants must be worldwide deployable and meet all MOS requirements.

Soldiers must not be on assignment instructions, as of the date that Military Intelligence Branch, U.S. Army Human Resource Command (HRC) receives their application. Program selectees will incur an Active Duty service obligation of six years at the start of the program in order to meet the 36-month service remaining requirement following graduation.

Applicants must possess an outstanding record of military service evidenced by noncommissioned officer evaluation reports and academic evaluation reports. Full application requirements are available in military personnel (MILPER) messages published annually by HRC announcing each internship programs enrollment procedures. The current year's program messages are:

- MILPER 16-151 MECCAP
- MILPER 16-152 MINSAP
- MILPER 16-153 MLAP
- MILPER 16-154 MCSAP

Applications may be submitted at any time as long as they meet application requirements. HRC holds selection boards quarterly, immediately following the end of each fiscal quarter. (i.e., In the first week of October for applications received in the quarter ending the 31st of September.) HRC notifies applicant's commanders of the selection board results within two weeks following the board. HRC designates a permanent change of station report date, normally around six months following notification, for those selected. However, the Noncommissioned Officer Education System, current eligibility date for return from overseas assignment (if applicable), and other factors could prolong the report date.

Important Note: U.S. Army Reservists and National Guard Soldiers are not eligible for these programs.

Middle Enlisted Cryptologic Career Advancement Program

by Staff Sergeant Lee J. Pifer

Introduction

Signals intelligence Soldiers are expected to perform a wide range of SIGINT technical and analytical functions in support of joint, interagency, intergovernmental, and multinational operations as well as Army operations. The Middle Enlisted Cryptologic Career Advancement Program (MECCAP) administered by the NSA is an opportunity for Army SIGINT NCOs to gain operational experience and innovative training required from today's operational environment. The program allows participants to tailor their experience and focus areas towards personal interests and the Army needs. The program allows participants to explore the SIGINT enterprise and expand their knowledge base on associated networks, tools, and databases. The expectation is that MECCAP graduates will develop advanced SIGINT technical abilities and a greater understanding of the intelligence community (IC) to prepare them for more demanding leadership positions supporting highly technical Army operations. MECCAP participants have the opportunity to tailor their experience and training, build a deeper understanding of NSA's capabilities, and learn how to leverage those capabilities for the Army.

This article will inform enlisted SIGINT Soldiers about the MECCAP program from the perspective of a current participant with the intent of determining their own suitability for the program. It will also inform leaders of the benefits of having MECCAP graduates in their units, and identify how graduates can leverage the SIGINT enterprise more effectively in support of commanders.

The Program Requirements

MECCAP is open to NCOs in the following MOSs:

- 35N, Signals Intelligence Analyst.
- 35P, Cryptologic Linguist.
- 35S, Signals Collector.
- 35Q, Cryptologic Network Warfare Specialist.

While other NSA programs are MOS-specific and focused toward creating subject matter experts in their respective fields, MECCAP creates SIGINT leaders who have a broad understanding of the capabilities and limitations of all SIGINT focused specialties. The diversity of skillsets among the participants in the program allows for a variety of cross training and potential tours within the NSA.

The requirements of MECCAP have remained consistent since its inception in 1977. Participants have three years to complete a minimum of four 6 to 9 month operational tours within NSA as well as 1500 hours of academic credit through the National Cryptologic School (NCS). Program managers chose the first four tours from among six focus areas:

- Analysis and reporting.
- Collection management.
- Computer network/information operations.
- SIGINT development.
- Support to military operations.
- Policy and guidance.

If a participant completes the required four tours with time remained, they have the option of a fifth tour within the work center of their choosing. The 1500 hours of academic credit provide a foundational understanding of the NSA and the IC. The core of the academic courses consist of five focus areas that require a minimum of 100 hours each in the areas of—

- Leadership.
- Reporting.
- Cryptologic access.
- Intelligence analysis.
- Cyber operations.

After the minimum 100-hour requirement for each focus area, participants take the remaining credits as electives. Most work center tours are completed with the NSA, but participants have the option to support other agencies and commands worldwide. Likewise, program participants take most of their courses through the NCS, but they can also take external courses with executive approval.

A Participants View

MECCAP provides the freedom for participants to find potential work centers that align with their professional interests and to develop new analytic capabilities and understanding not found outside a cryptologic center. Finding the path for you can be one of the most intimidating parts of the program. The overall requirements are straightforward, but the number of tour options and volume of available courses makes for endless possibilities. Peer networking and personal initiative become incredibly important. MECCAP is an excellent opportunity for an NCO seeking to improve their skills and push their professional limits. MECCAP affords participants numerous opportunities to create long-term professional relationships within the NSA and greater IC that can be leveraged throughout their career for the benefit of the Army.

The MECCAP executive agent and service panel representatives provide oversight of the participants and approve tours and course requests. They offer advice on possible tours and advise how to engage with NSA work center leadership for tour placement. They ensure participants are on track with tour and academic requirements, but mostly maintain a hands-off approach to enable personal growth and encourage individuals to develop their own agency relationships.

Most advice on MECCAP is peer based, coming from other Army and joint service participants. MECCAP participants share their experiences and personal networks to help each other find desired work centers. It is common for participants to follow a peer in consecutive tours where both the work center and participants benefit from the relationship. Participants also collaborate with their officer counterparts in the Junior Officer Career Cryptologic Program (JOCCP) and Warrant Officer Career Cryptologic Program (WOCCP) to share work center experiences and best practices. This partnership further expands participants' networks and aids in tailoring future tours. By bringing all NSA leadership programs together to discuss work center opportunities, NCS course options, and deployments, an environment of shared understanding of work role requirements and potential tours to match professional interests is created. The overall experience of world-class training, developing relationships with NSA civilian leadership, the greater IC, and other NSA programs' participants, is of immeasurable value to the Army and joint force.

To facilitate the networking process, MECCAP participants are required to interview with a minimum of three work centers before selecting one for a tour. This creates connections and exposure to a large number of civilian and military NSA leaders and identifies future opportunities across the enterprise. If a peer informs a participant about a great tour opportunity, they must then connect with office managers to schedule interviews, express their desire to join the team, and coordinate for a tour timeline that works for both parties. Even if the participant decides their first interview is the tour they want, they must still conduct the minimum required interviews to expand their knowledge of NSA work centers. The first work center I interviewed was so exciting that I wanted to sign up for the tour immediately. However, my panel representative encouraged me to continue the additional required interviews before making a selection. After a few more interviews, I was able to understand just how diverse and interesting the missions available for MECCAP participants. In the end, I conducted five interviews and chose the last work center.

Giving Back to the Army

The value of the program lasts long after the internship itself. MECCAP was intended as a preparation program to build SIGINT leaders capable of managing highly complex requirements in an extremely technical field. Enlisted Soldiers completing this program bring a wealth of knowledge from the NSA and unparalleled SIGINT capability back to the Army. Participants develop excellent technical competency in new and emerging technologies and graduate knowing they made significant contributions in support of national security at the highest levels. Participants return to the Army equipped with experience and unique skills unbuildable outside the NSA and invaluable to Army commanders. Any Soldier considering MECCAP should remember it is a leadership-focused program tailored by the participants themselves. There is unlimited potential in the program for a self-motivated NCO to gain experience and advanced training, and develop life-long connections with counterparts at the NSA.

Military Occupational Specialty Specific Enlisted Cryptologic Internship Programs

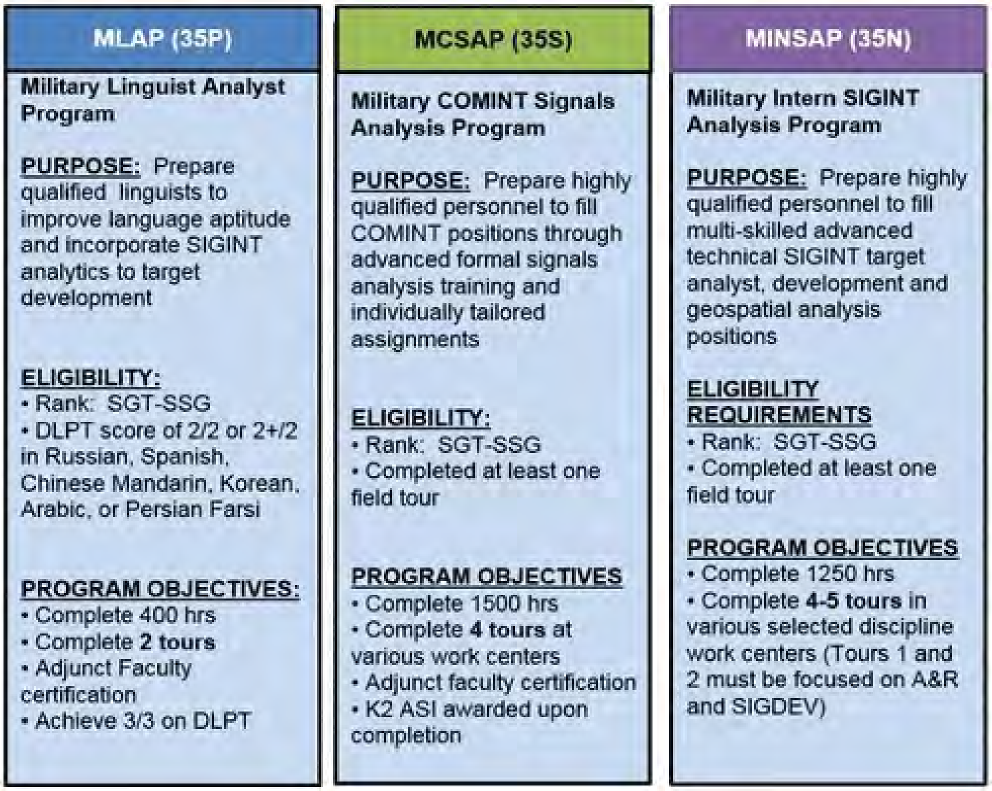
by Sergeant First Class Jeffrey Costa, Staff Sergeant Kristie Shain, Sergeant Paul Droutsas, and Sergeant Marshall Spence

Introduction

Signals Intelligence Soldiers work in a highly technical and constantly evolving career field where they are expected to understand and be experts on emerging technologies and complete a wide range of SIGINT technical and analytical operations. To support development of well-rounded and technically advanced NCOs the NSA created the Enlisted Cryptologic Internship Programs. These programs utilize formal, advanced training with definitive learning plans, academic curriculum, and agreements with NSA work centers to enable participants to gain MOS specific knowledge of the SIGINT enterprise. Participants are exposed to an extremely technical environment focused on developing them into highly skilled cryptologic analysts.

There are three MOS-specific enlisted cryptologic programs at the NSA—Military Communications Intelligence Signals Analyst Program (MCSAP), Military Intern Signals Intelligence Analysis Program (MINSAP), and Military Language Analyst Program (MLAP). These cryptologic programs provide MOS specific challenges to NCOs through advanced formal and informal technical training that is individually tailored to the participant's professional goals and operational assignments. The training is designed to meet the growing complexity of the strategic environment and rapidly evolving technology. The general requirements for all three programs are—

- ✦ Requires 6 years of service remaining (3 years in the program; 3 years post program utilization assignment).
- ✦ Conduct three to five NSA work center tours lasting 6 to 9 months.
- ✦ Complete over 1200 hours of NCS courses.
- ✦ Achieve adjunct faculty certification, which enables participants the ability to instruct anywhere within the cryptologic enterprise.



MLAP (35P)	MCSAP (35S)	MINSAP (35N)
Military Linguist Analyst Program	**Military COMINT Signals Analysis Program**	**Military Intern SIGINT Analysis Program**
PURPOSE: Prepare qualified linguists to improve language aptitude and incorporate SIGINT analytics to target development	**PURPOSE:** Prepare highly qualified personnel to fill COMINT positions through advanced formal signals analysis training and individually tailored assignments	**PURPOSE:** Prepare highly qualified personnel to fill multi-skilled advanced technical SIGINT target analyst, development and geospatial analysis positions
ELIGIBILITY: • Rank: SGT-SSG • DLPT score of 2/2 or 2+/2 in Russian, Spanish, Chinese Mandarin, Korean, Arabic, or Persian Farsi	**ELIGIBILITY:** • Rank: SGT-SSG • Completed at least one field tour	**ELIGIBILITY REQUIREMENTS** • Rank: SGT-SSG • Completed at least one field tour
PROGRAM OBJECTIVES: • Complete 400 hrs • Complete **2 tours** • Adjunct Faculty certification • Achieve 3/3 on DLPT	**PROGRAM OBJECTIVES** • Complete 1500 hrs • Complete **4 tours** at various work centers • Adjunct faculty certification • K2 ASI awarded upon completion	**PROGRAM OBJECTIVES** • Complete 1250 hrs • Complete **4-5 tours** in various selected discipline work centers (Tours 1 and 2 must be focused on A&R and SIGDEV)

This article has three objectives, to introduce and discuss the uniqueness of each program, to inform future participants of the programs expectations and how the programs can help shape their career paths, and to ensure Army leaders understand the unique value cryptologic program graduates bring to the Army.

The Military Communications Intelligence Signals Analyst Program

The MCSAP is a specialized joint internship run by the NSA. Army 35S, Signals Collectors, looking to become technical experts and leaders in their field are eligible to apply. This program is designed to take experienced SIGINT Soldiers and turn them into subject matter experts in the field of signals analysis and collection. MCSAP is self-paced and requires motivated, driven individuals. A program goal unique to MCSAP is the requirement to write an in-depth, technical, professional paper for review. Work center on-the-job training occurs in waveform, bit stream, and protocol domains.

The first tour of the program is facilitated by the MCSAP executive agent with the following two determined by the participants. Remaining proactive and creating a plan are key to meeting graduation requirements and securing a position in the other waveform, bit stream, or protocol work centers. Space is limited in many offices, especially those in high demand or with dynamic missions. To get the most from the program, planning and professional networking early are essential to securing the desired work center tours. This will allow you to map the internship in advance and provides an avenue to success.

Upon completion of the required work center tours, the participants have the option of completing a diversity tour. This allows participants to broaden their understanding of the NSA overall and provides the opportunity to work with other intelligence agencies requiring SIGINT support. Access to the myriad resources within the NSA is one of the program's greatest assets. However, the vast number of choices available can be overwhelming when trying to line up required and diversity work center tours. The options available and competition from other MCSAP participants and civilian-equivalent peers (the Signals Analysis Development Program), make securing a seat in the most sought after work centers a challenge. A participant's work ethic, reputation, and their ability to network throughout the NSA will open doors to some of the more coveted work centers.

Of the required courses, Signals Boot Camp builds towards the required adjunct faculty certification. To satisfy the certification requirement, participants must complete a course, co-instruct it with a certified instructor, and be evaluated while teaching the course. New participants who are already adjunct certified with the NCS will not have to recertify upon acceptance to the program.

The technical signals related paper is the final exam for this program. Program participants present their paper to a board, describe, and defend the paper based on the knowledge gained through work center tours. Upon completion of all MCSAP requirements, participants are awarded the additional skill identifier (ASI) of K2 and become NSA certified Signals Analysts.

In addition to the K2 designator and the networking opportunities, NCOs leave the program with a deeper understanding of the NSA and an understanding of how to leverage the NSA in future Army assignments. Time spent in work center tours provide analysts with the opportunity to work hand-in-hand with senior NSA leaders and experts in the waveform, bit stream, and protocol domains. Through these opportunities, NCOs not only become advanced technical experts, but also gain the capability to help develop various programs for the Army and IC.

The Military Intern Signals Intelligence Analysis Program

The MINSAP is a technically focused program for 35N, Signals Intelligence Analysts, to expand their knowledge through challenging technical development tours at NSA-Washington. MINSAP is an outstanding opportunity for mid-career Soldiers to improve their analytic skills, knowledge, and abilities. The goal of the program is to develop technically advanced NCOs by building upon the skills and experiences they bring to the program.

The MINSAP program manager is a critical player for MINSAP participants. They provide the initial contact for Soldiers upon program acceptance. The program manager helps determine work center tours, lining up interviews and tailoring the experience based on professional interests. While not only supporting newly arrived participants with coordinating their first tour, program managers ensure each Soldier enrolls in the MINSAP curriculum and is meeting the timeline in order to graduate.

Work center tours are chosen from the areas of-

- SIGINT development.
- SIGINT geospatial analysis.
- Target digital network analysis.
- Information management research.
- Intelligence.
- Cyber-related roles.
- Analytics.
- Deployments and temporary duty outside the continental United States to unique duty locations.

A participant's first tour is typically a 9-month target analysis and reporting tour. After completion of that work assignment participants will conduct a signals development tour. Participants interview with perspective work centers based on their professional interests. One unique aspect of MINSAP is the freedom of action within the NSA following the completion of these two required tours. This affords participants the opportunity to choose unique work centers that will challenge their technical abilities and expose them to uncommon missions they would not have access to within a traditional Army assignment.

Participants have three years to complete over 1200 hours of NCS course work. NSA-Washington offers a combination of virtual, self-paced courses, and classroom subjects. This coursework complements the participant's work center tours.

Following completion of the program, NCOs have advanced technical skills, enhanced knowledge of the SIGINT enterprise, and a strong reach back capability through their professional network. Program graduation brings with it a service obligation and a post program utilization. NCOs bring to their gaining command a unique skillset. Whether the utilization is in a brigade combat team or corps analysis and control element, participants have the skills and ability to leverage their knowledge to enhance intelligence collection, analysis, reporting, and dissemination for the Army.

The Military Language Analyst Program

The MLAP offers challenges and benefits like no other language training opportunity in the Army. The program prepares qualified linguists to improve their language aptitude and incorporate SIGINT analytics into target development. Program participants are able to tailor their experience within the program to meet their personal developmental goals and build the capacity to leverage NSA capabilities. The program is open to 35P, Cryptologic Linguists, in the ranks of sergeant or staff sergeant with a Defense Language Proficiency Test (DLPT) score of 2/2 or 2+/2 in either Russian, Spanish, Chinese Mandarin, Korean, Arabic, or Persian Farsi. Similar to other NSA programs, participants engage in over 2000 hours of classroom and computer-based training, complete tours in at least three different NSA work centers, obtain adjunct faculty certification, and are required to score a 3/3 on the DLPT in their target language in order to graduate.

Within the MLAP program, participants receive the unique opportunity to fully utilize their language skills daily. Furthermore, participants in the MLAP do not just conduct language work; they have opportunities to pursue individual projects as well. They are able to work projects from inception through the final products. This allows participants to develop a diverse set of skills and perform a truly multi-disciplined role, broadening their base of knowledge and experience. During the program, they will earn the ASI T5, as Target Digital Network Analysts, through classroom education. This allows them to combine their technological knowledge with their language expertise and achieve results that consistently impact the IC. In MLAP, the time spent in a work center is approximately 6 months, so participants need to have mastered the work within a month or two in order to effectively work mission, produce intelligence, and gain experience. While the program is designed to ensure participants learn and broaden their skills, it is also designed to provide mutual benefit to the NSA work centers. Due to the nature of the languages and intelligence analysis conducted, and the pace of acquisition and performance that must be maintained, ensuring a high level of mental acuity and dexterity are necessary for success in MLAP. Participants must be able to meld critical thinking, clear communication, boldness, and responsibility in order to manage issues and requirements in the workplace. Participants must be self-motivated and prepared to pass on the knowledge gained in a work center in order to maintain a solid foundation across MLAP. This ensures preservation of dynamic institutional knowledge, and helps to build camaraderie with in MLAP.

Upon graduation from MLAP, NCOs return to the Army, whether to U.S. Army Forces Command, U.S. Army Training and Doctrine Command, or to a combatant command bringing expert linguistic skills, knowledge of the SIGINT enterprise and how to leverage it to better enable Army operations. This program will provide participants with a unique perspective of the SIGINT enterprise and overall hone their language and SIGINT analysis skills. Army leaders can utilize MLAP graduates to train, teach, and mentor junior Soldiers, whether they are signals intelligence analysts or cryptologic linguists. MLAP is an incredible opportunity that requires NCOs who are self-motivated, seek and give guidance, and are able to develop and maintain a battle rhythm. They must possess the mental acuity and dexterity to not only excel in their language skills but to broaden their work roles and become technically competent signals language analysts.

Mr. Brian Bouchard is a retired first sergeant and is currently serving as a cryptologic training and proponency action officer in Army Cryptologic Operations, G-3, Intelligence and Security Command. Mr. Bouchard is a 1998 graduate of the Military Language Analyst Program and a former 98G/35P, Cryptologic Linguist Advanced Individual Training course instructor and senior drill sergeant at Goodfellow Air Force Base, TX.

SSG Lee Pifer is an Arabic cryptologic linguist currently enrolled in the Middle Enlisted Cryptologic Career Advancement Program (MECCAP) assigned to the 741st Military Intelligence Battalion, 704th Military Intelligence Brigade at Fort Meade, MD. Prior to being accepted into MECCAP, SSG Pifer was assigned to 4th Stryker Brigade Combat Team, 2nd Infantry Division at Joint Base Lewis-McChord as a cryptologic linguist. While assigned there he deployed in support of Operation Enduring Freedom.

SFC Costa holds a bachelor's degree in chemistry from the Excelsior College. He is a platoon sergeant for Army interns at Fort Meade, MD and the Military Interns Signals Intelligence Analysis program manager.

SSG Shain is an Arabic cryptologic linguist currently enrolled in the Military Language Analyst Program (MLAP) and assigned to Headquarters and Operations Company, 741st Military Intelligence Battalion at Fort Meade, MD. Prior to her acceptance into MLAP, SSG Shain was assigned to the 15th Military Intelligence Battalion at Fort Hood, TX, as a senior cryptologic linguist. While assigned at Fort Hood, she deployed with Task Force Odin in support of Operation Enduring Freedom as an aerial STG mission manager.

SGT Paul Droutsas is from Kerrville, TX, and is currently pursuing a bachelor's degree from American Military University in intelligence studies. He is a first year Military Communications Intelligence Signals Analysis Program intern assigned to Headquarters and Operations Company, 741st Military Intelligence Battalion at Fort Meade, MD.

SGT Marshall Spence holds a bachelor's degree from the University of Central Florida and is a first-year Military Communications Intelligence Signals Analysis Program intern assigned to Headquarters and Operations Company, 741st Military Intelligence Battalion at Fort Meade, MD. As a 35S, Signals Collector, he is a 451 graduate with four years experience as a signals collector and analyst. In addition to being stationed at Ft. Meade, he has worked at Buckley Air Force Base and Alice Springs, Australia.

The Military Intelligence Corps 2017 Hall of Fame Inductees

Brigadier General Henry J. Muller, U.S. Army, Retired

Henry Muller, 100 years old this year, entered the Army as a second lieutenant from the Infantry Reserve in 1940 and was commissioned in the Regular Army in 1942.

In May 1943, during World War II, then MAJ Muller was assigned as the G-2 of the 11th Airborne Division in the Pacific, a position he held until the end of the war. He was promoted to lieutenant colonel in September 1944. When told about a Japanese prison camp at Los Baños, 30 miles behind enemy lines on Luzon in the Philippine Islands, he personally gathered intelligence from photo reconnaissance, guerilla reports, maps, and scouting missions conducted by his section's provisional reconnaissance platoon. In collaboration with the division's G-3, Muller developed a plan for a surprise three-prong land, amphibious, and airborne attack on the camp. Launched on February 23, 1945, the successful raid liberated 2,147 American and Allied civilians with almost no casualties. Nearly 50 years after the raid, GEN Colin Powell, Chairman of the Joint Chiefs of Staff, called the raid "the textbook airborne operation for all ages and all armies," and the 11th Airborne Division commander, LTG Joseph Swing, recalled that it could not have succeeded "without perfect intelligence."

Following the war, Muller served as Assistant G-2 of the U.S. Eighth Army during the occupation of Japan. He returned to the United States in 1947 and was assigned as Assistant G-2, Army Ground Forces, at Fort Monroe, Virginia. From 1950 to 1953, LTC Muller was appointed Special Assistant for Current Intelligence to the Director of the Central Intelligence Agency. In this capacity, he helped prepare and present the weekly intelligence briefings to President Harry Truman.

After completing the Spanish course in the Army Language School, he made use of his language training in El Salvador, the Dominican Republic, and Argentina, as well as in the Panama Canal Zone as Commandant of the Army's Jungle Warfare Training Center. During the Cuban Missile Crisis, then COL Muller commanded the 503rd Parachute Infantry Regiment in the 82nd Airborne Division. His regiment was designated to be first to jump into Cuba shortly before the operation was canceled when Soviet freighters carrying missiles to Cuba turned back.

After his promotion to brigadier general in March 1967, BG Muller served as Assistant Division Commander of the 101st Airborne Division in Vietnam and commanded the U.S. Army Advisory Group in the I Corps tactical zone. His final assignment was Commanding General of the Infantry Training Center at Fort Polk, Louisiana, until his retirement in July 1971.

BG Muller's awards include the Distinguished Service Medal, Silver Star, Legion of Merit, Bronze Star, Air Medal, and the Purple Heart.

Colonel Joe R. Parker, U.S. Army, Retired

Joe Parker was commissioned a second lieutenant in military intelligence upon graduation as a Distinguished Military Graduate from the University of Tennessee in 1970. COL Parker served 28 years of active duty and commanded or established some of the Army's most sensitive human intelligence (HUMINT) and special operations organizations. In total, COL Parker has 47 years of continuous service to the nation, including both active duty and civilian service; during this time, he has become widely acknowledged as the Army's HUMINT subject matter expert.

Following commissioning, COL Parker was detailed to infantry branch and served as a rifle platoon leader, company executive officer, and battalion S-2 with 2nd Battalion, 508th Airborne Infantry, 82nd Airborne Division. Volunteering for special forces, he served in 5th Special Forces Group as an "A" detachment commander and in 1st and 10th Special Forces Groups as a counterintelligence and area intelligence section leader, operations officer and executive officer.

During 1980-1981, COL Parker served in Korea with the United Nations Military Armistice Commission. He served the next six years as operations officer and detachment commander at the U.S. Army Intelligence Support Activity. In 1987, he was assigned to the U.S. Army Office of Military Support (USAOMS) where he directed multi-discipline activities supporting Operations Just Cause, Desert Shield, and Desert Storm.

COL Parker commanded the Army Intelligence and Security Command (INSCOM) Training and Doctrine Support Detachment at Fort Huachuca, Arizona, where he established an unprecedented close working relationship between INSCOM and the Intelligence Center and developed the first action plan to incorporate counterintelligence and HUMINT into the Army Intelligence Master Plan. In 1995, COL Parker established and commanded the first Defense HUMINT Service Operating Base and conducted sensitive HUMINT operations worldwide, including support to Operation Joint Endeavor. He also served detail assignments with the Central Intelligence Agency and Drug Enforcement Administration.

Mr. Parker began his civilian career in 1998 as Deputy for HUMINT at USAOMS and later served as Director of the Army HUMINT Operations Center. In 2008, he was appointed to the Senior Executive Service as the first senior HUMINT advisor to the Deputy Chief of Staff, G-2. COL Parker dedicated his civilian career to revitalizing Army HUMINT, particularly in support of Operations Iraqi Freedom (OIF) and Enduring Freedom. He was instrumental in creating the first joint HUMINT operating base supporting the Commander of U.S. Forces Afghanistan. He also directed the creation of new regional collection platforms for full-spectrum HUMINT support to the regional combatant commands. COL Parker was the driving force behind the creation of the HUMINT Training Joint Center of Excellence, which since 2006, has trained more than 20,000 students in advanced HUMINT skills. He also deployed as the CJ-2X, Multi-National Force-Iraq, where he developed initiatives for Iraqi self-reliance and directed counterintelligence and HUMINT activities supporting OIF.

COL Parker's military awards and decorations include the Legion of Merit (2 OLC), Meritorious Service Medal (2 OLC), Army Commendation Medal (2 OLC), Army Achievement Medal (1OLC), Joint Meritorious Unit Award, Meritorious Unit Commendation, Army Superior Unit Award, Expert Infantry Badge, Master Parachute Badge, Ranger and Special Forces Tabs. As a Civilian, he received the first Department of Defense Lifetime HUMINT Achievement Award. Additional Civilian awards include the Global War on Terrorism Civilian Service Medal, Superior Civilian Service Award, and the Knowlton Award.

Chief Warrant Officer 5 James J. Prewitt, U.S. Army, Retired

Jerry Prewitt began his Army career as an imagery interpreter in 1974. He was appointed an imagery intelligence (IMINT) warrant officer in 1985 and his first assignment was to the Defense Intelligence Agency (DIA). In 1989, CW5 Prewitt was assigned as an IMINT platoon leader in the 470th Military Intelligence Brigade in support of Operation Just Cause and El Salvador counterinsurgency operations. The following year, he returned to the DIA as the Counterdrug Branch's senior military IMINT authority on narco-trafficking activities in Latin America. When Operations Desert Shield/Desert Storm began, CW5 Prewitt volunteered for the Joint Intelligence Center, Iraqi Task Force, where his analytical findings shaped perceptions of Iraqi strategy and strength, and critically impacted battlefield success in the Kuwaiti Theater of Operation.

In 1993, CW5 Prewitt was handpicked as the Chief, Exploitation Division, Directorate of Intelligence. During this period, punctuated by Operation Uphold Democracy in Haiti, his analysis at national sensor facilities ensured the success of several extremely dangerous missions.

In 1998, as the CJ2 Operations systems officer in the Assistant Chief of Staff, U.S. Forces Korea, CW5 Prewitt orchestrated a combination of complex and diverse national systems in support of the warfighters. He also created the most robust space-to-mud imagery architecture in 53 years of U.S. commitment to the Korean Armistice by integrating joint and combined theater assets into a seamless reconnaissance and surveillance system of systems.

Heading next to the National Imagery Mapping Agency, he volunteered to deploy as the leader of the National Intelligence Support Team for Joint Task Force Noble Anvil. In extreme weather and near combat conditions, he provided national imagery products and support to the Deep Operations Coordination Cell of Task Force Hawk that led directly to targeting of hostile forces in Kosovo.

From 2001 to 2007, CW5 Prewitt focused his efforts on improving the military intelligence (MI) warrant officer corps. He served as the MI research analyst for the Warrant Officer Personnel Management Study Group, the MI warrant officer career manager in Personnel Command, and was chosen as the Chief Warrant Officer of the MI Corps in 2004, during which time he instituted programs that helped MI meet or exceed accession goals.

In the last seven years of his military career, CW5 Prewitt was assigned to the U.S. Army Special Operations Command and then to the Joint Special Operations Command (JSOC). As the commander of JSOC's Advanced Geospatial Troop, he deployed five times on highly sensitive and classified missions in support of Operations Iraqi Freedom and Enduring Freedom. CW5 Prewitt retired from active duty in 2014 with more than 40 years of active service.

CW5 Prewitt's awards include the Legion of Merit, Bronze Star (2 OLC), Defense Meritorious Service Medal (5 OLC), Meritorious Service Medal (4 OLC), Air Medal (2 OLC), Joint Service Commendation Medal (1 OLC), Army Commendation Medal (2 OLC), Aerial Achievement Medal, Joint Achievement Medal (1 OLC), and the Army Achievement Medal.

Command Sergeant Major Lawrence J. Haubrich, U.S. Army, Retired

Lawrence Haubrich enlisted in the Army in 1976, and during his 30-year career, proved a consummate intelligence technician, linguist, trainer, leader, and advisor for commanders and thousands of Soldiers. After serving four years as a senior aerial observer in Berlin, Germany, he was assigned to the 2nd Ranger Battalion, 75th Ranger Regiment at Fort Lewis, Washington, the first of several assignments in the special operations community. During his three-year assignment, he helped prepare the battalion for its participation in Operation Urgent Fury in Grenada and conducted debriefings of all wounded and returning Rangers to Fort Lewis, Washington.

In 1986, CSM Haubrich moved back to Germany to be the intelligence sergeant of F Company (Long Range Surveillance) (LRSC), 51st Infantry, 511th Military Intelligence Battalion. As the primary intelligence advisor to 18 LRS teams, he took it upon himself to complete the LRSC Leader's Course and then instituted more detailed intelligence products and better instruction for the LRS teams. From 1989 to 1993, he served as First Sergeant for three units: the Military Intelligence Detachment, 3rd Battalion, 5th Special Forces Group (A); the Military Intelligence Detachment, 1st Battalion, 3rd Special Forces Group (A); and A Company, 1st Psychological Operations Battalion. During this time, he took on the duties of detachment commander for a deployment to Operation Desert Storm, graduated from the extremely difficult High Risk, Level III, Survival, Escape, Resistance, and Evasion course, and supported 75 Operational Team Detachment deployments to 12 countries in Central America, South America, and the Caribbean.

CSM Haubrich was then selected to serve with the On Site Inspection Agency Europe in Germany. He was the noncommissioned officer in charge of the Operations and Plans Division of a joint NATO contingent monitoring conventional armed forces in Europe and intermediate-range nuclear forces. He also served as the U.S. liaison officer to the German government for three Ukrainian inspections and as the U.S. government representative on inspection trips in former Soviet Union and Warsaw Pact countries. During this assignment, CSM Haubrich earned the Soldier's Medal for saving the lives of two German civilians whose plane had crashed.

After graduating from the Sergeants Major Academy, CSM Haubrich was assigned as the Deputy Chief of Staff, Intelligence, Sergeant Major for U.S. Army Special Operations Command. He successively served as the CSM of the 519th Military Intelligence Battalion (ABN), then the 525th Military Intelligence Brigade (ABN). Credited as one of the strongest CSMs in military intelligence (MI), in November 2000, he was selected to be the MI Corps CSM. For the next five years, he brought seasoned combat veterans to the school to train young and deploying Soldiers and moved "career instructors" out to deploying units to update their skills. Coining the phase "WE ARE AN MI CORPS OF ONE," he visited Active and Reserve MI Soldiers worldwide to gather lessons learned and personally ensured those lessons were incorporated into programs of instruction to better prepare MI Soldiers to fight the Global War on Terrorism. He also led the successful effort to award the Combat Action Badge to all combat support and combat service support military occupational specialties.

CSM Haubrich retired from the Army in April 2006. His awards include the Distinguished Service Medal, Soldier's Medal, Bronze Star, Meritorious Service Medal (3 OLC), Joint Service Commendation Medal, Army Commendation Medal (4 OLC), Army Achievement Medal (1 OLC), Master Parachutist Badge, German and Royal Australian Parachutist Badge, Jungle Expert Badge, and the coveted Ranger Tab.

Mr. Bill "Rod" Moore, Colonel, U.S. Army, Retired and Senior Executive Service, Retired

Rod Moore was commissioned a second lieutenant of military intelligence in 1974. During his 26-year military career, he commanded at the company and battalion levels and deployed the 101st Military Intelligence Battalion in support of the 1st Infantry Division during Operations Desert Shield/Desert Storm. He also served as the senior intelligence officer at all levels from battalion through army service component command. In December 2000, at the rank of colonel, he culminated his military career as the G-2 for the Third U.S. Army.

Beginning in January 2006, Mr. Moore served with great distinction as the Deputy J-2 at U.S. Central Command (CENTCOM), providing mission continuity during eight changes in both combatant commanders and intelligence directors. He was responsible for intelligence planning and execution for the Global War on Terrorism and subsequent operations in Afghanistan, Iraq and throughout the tumultuous CENTCOM area of responsibility. Collection management; intelligence, surveillance, and reconnaissance (ISR) synchronization; analysis and production; intelligence support to planning; and network architecture all grew exponentially and thrived during Mr. Moore's tenure as the Deputy J-2.

Mr. Moore oversaw the largest buildup of intelligence capacity and capability in the history of the U.S. Army. He worked closely with deployed commands to build a fully integrated ISR architecture and developed unique capabilities to target enemy networks and defeat the threat from improvised explosive devices. He was a major contributor to the successful fielding of the Persistent Threat Detection Systems, Liberty aircraft, and the expansion of Predator and Global Hawk unmanned aircraft systems. To maximize these critical resources, Mr. Moore led an initiative to shift platforms in Afghanistan, Pakistan, and Iraq to other missions in those countries when unable to operate in primary areas. Understanding collection as only one part of the ISR mission, Mr. Moore initiated coordination of production, exploitation, and dissemination systems and increased personnel strength to support expanded automated and manual dissemination of intelligence to coalition and partners.

With CENTCOM's increased mission and associated Operation Enduring Freedom workload, Mr. Moore oversaw the construction of a new CENTCOM Joint Intelligence Operations Center (JIOC) and transformed it into the most effective joint intelligence element within the defense intelligence enterprise. He oversaw a number of reviews of J-2 mission areas, and the lessons learned became the Under Secretary of Defense for Intelligence's model for other combatant commands. His efforts were equally important in the establishment of the JIOC-Afghanistan and in the Afghanistan/Pakistan Intelligence Center of Excellence. The foundation he created will have a positive and enduring impact on the development of the Iraqi and Afghanistan military intelligence services.

Mr. Moore retired from Senior Executive Service in April 2014. His military awards include the Legion of Merit, Bronze Star, Defense Meritorious Service Medal, the Meritorious Service Medal, the Army Commendation Medal, and the Army Achievement Medal. His civilian awards include the Joint Distinguished Civilian Service Medal, National Intelligence Distinguished Service Medal, Defense Intelligence Agency Director's Award, the Presidential Rank Meritorious Executive Award, and the Defense Superior Service Medal.

Mrs. Glenda Griffin, Department of the Army Civilian, Retired (Deceased)

Although Glenda Griffin entered Federal Service in 1958 as a GS-2 Clerk Typist at Redstone Arsenal, by 1965 she had entered the military intelligence arena. As an analyst at the Missile Intelligence Agency, Redstone Arsenal, during the Vietnam War, her understanding of Soviet air defense tactics and doctrine fostered a continuous and immediate exchange between the intelligence community in the United States and U.S. Air Force operating units in Vietnam. Over the next several years, she provided intelligence analytical support to U.S. personnel supporting the Israeli/Arab conflicts and managed a comprehensive translation effort of captured Arab documents that became the basis for an understanding of Arab capabilities to wage air defense combat.

In 1981, Mrs. Griffin transferred to the U.S. Army Electronic Research and Development Command, predecessor of the U.S. Army Laboratory Command (LABCOM). She was instrumental in developing the electronic warfare integrated reprogrammable database and establishing a solid relationship with the Air Force Electronic Warfare Center in San Antonio, Texas. Her next assignment was in the Special Programs Branch of the Deputy Chief of Staff for Intelligence (DCSINT) at Army Materiel Command. During this assignment, she developed policies and procedures for managing intelligence special access programs.

In 1985, Mrs. Griffin returned to LABCOM as the Deputy to the DCSINT and Chief of the Special Programs Branch. She and her staff refined the procedures for protecting special access programs during field-testing. She became the LABCOM DCSINT in 1987, continuing to serve as a bridge between the research, development, and acquisition community and the intelligence community. During Operations Desert Shield/Desert Storm, Mrs. Griffin managed a major foreign exploitation effort that provided previously unknown intelligence to the theater and resulted in changes to a major battlefield system.

In 1990, she became the senior intelligence officer, U.S. Army Research Laboratory (ARL), and was appointed as a special Army observer to the inter-agency Scientific and Technical Intelligence Committee. In addition to her intelligence responsibilities, Mrs. Griffin managed the consolidation and downsizing of the seven independent laboratories of LABCOM into the unified ARL. A champion of fairness and equality, she was commended for the establishment of a women's mentoring program and advancement of women in the intelligence service. During her last year at ARL, she established the first Computer Security and Incident Response Team in the Army. This team successfully developed automated methods for recognizing, identifying, responding to, and reporting computer security intrusions.

Mrs. Griffin culminated her career as Chief, Intelligence and Security, Office of the Chief of Staff, ARL. She managed a staff of 61 intelligence and security professionals who provided myriad services to the laboratory's multiple sites within the United States.

After 37 years of federal service, Mrs. Griffin retired in September 1997. Her awards include the Commander's Award for Civilian Service, which she received in 1980 and upon her retirement in 1997; the Della Whittaker Memorial Award given by the Federally Employed Women (Adelphi Chapter); and the Meritorious Civilian Service Award. Mrs. Griffin passed away in August 2016.

Captain Christopher R. Philhower
2017 Recipient
Lieutenant General Sidney T. Weinstein Award For Excellence in Military Intelligence

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

Originally, from Columbus, Ohio, CPT Philhower commissioned as an infantry officer from Capital University in May 2010 and began Infantry Basic Officer Leader Course in November, graduating on the Commandant's List.

Following Ranger School, CPT Philhower was assigned as platoon leader of the 2nd Platoon, Battle Company in the 2nd Battalion, 503rd Infantry (Airborne), 173rd Airborne Brigade Combat Team. CPT Philhower executed a rotation to the Joint Multinational Readiness Center in Germany and successfully graduated Jumpmaster School, becoming the only second lieutenant jumpmaster in the 173rd at that time. CPT Philhower then led his platoon on a seven-month deployment to Wardak, Afghanistan.

Following redeployment, CPT Philhower was assigned to 1st Battalion, 75th Ranger Regiment. He deployed a second time to Logar, Afghanistan, serving as a targeting officer for Task Force Central. Upon redeployment, CPT Philhower became the platoon leader for 1st Platoon, Delta Company, and deployed a third time to Afghanistan. He then attended the Military Intelligence Captains Career Course (MICCC) at Fort Huachuca, Arizona, graduating again on the Commandant's List after serving in class leadership and being selected to oversee the execution of the Emerging Leader Physical Training (PT) Program, a high-intensity PT program designed to prepare MI officer students for nominative selections in the special operations and intelligence communities.

Following the MICCC, CPT Philhower received his first assignment as an intelligence officer. He was assigned as the battalion S-2 for the 2nd Battalion, 87th Infantry Regiment, 10th Mountain Division at Fort Drum, New York. In April, he met his battalion forward in Helmand Province, Afghanistan, for his fourth deployment, and assumed the role of G-2 for the commanding general of Task Force Forge (now called Train Advise Assist Command–Southwest) in support of Operation Freedom's Sentinel.

By quickly overhauling the organization's intelligence process, he was able to gain an understanding of the tribal threat streams in the Province, which had had no coalition presence for nearly a year. He streamlined the analysis and dissemination of TF Forge's new, thorough assessments. With an unsurpassed ability to articulate threats, CPT Philhower worked tirelessly to build and maintain relationships. He established and led a weekly meeting to synchronize the assessment and targeting efforts of 19 combined, joint, and special operations forces across Afghanistan. He regularly presented the intelligence picture to visiting general officers, coalition partners, and distinguished visitors, providing a thorough, reliable understanding of Helmand Province. CPT Philhower sought every opportunity to reshape the way maneuver commanders view intelligence, increasing the value they find in intelligence and ensuring intelligence drives operations.

As a competent and strong leader, CPT Philhower fostered an environment in which every Soldier was treated as an intelligence professional and expected to contribute to a collective and shared understanding. His versatility and ability achieved results under adverse circumstances and he held himself, his subordinates, and his organizations accountable, always working to make his team the absolute best it could be.

CPT Philhower's awards and decorations include the Bronze Star Medal, Joint Service Commendation Medal, Army Commendation Medal (2 Oak Leaf Clusters), Army Achievement Medal, the Meritorious Unit Commendation, National Defense Service Medal, Afghanistan Campaign Medal (2 Campaign Stars), Global War on Terrorism Service Medal, Army Service Ribbon, Overseas Service Ribbon, NATO Medal, Combat Infantryman Badge, Expert Infantryman Badge, Parachutist Badge, and Ranger Tab.

Chief Warrant Officer 2 Stephen R. Barber

2017 Recipient

Chief Warrant Officer 5 Rex Williams Award

For Excellence in Military Intelligence

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

CW2 Stephen R. Barber was born in San Francisco, California. He enlisted in the U.S. Army as an imagery intelligence analyst in 2004 after graduating from General H.H. Arnold American High School in Wiesbaden, Germany. He graduated from Cochise Community College with an associate's degree in intelligence operations in 2013 and from American Military University with a bachelor of arts degree in homeland security in 2016. His military education includes multiple advanced geospatial intelligence (GEOINT) and imagery intelligence analysis courses, Measurements and Signatures Intelligence (MASINT) Collections and Analysis Course (2005), Requirements Management System Course (2007), GEOINT Information Management System Course (2011), Warrant Officer Candidate School (2011), Warrant Officer Basic Course (2011), Warrant Officer Advanced Course (2015), and the Digital Intelligence Systems Master Gunner Course (2017).

In early 2016, CW2 Barber transitioned from U.S. Southern Command (USSOUTHCOM) to the Combined Arms Center, Army Mission Training Command Program to serve as an intelligence observer coach/trainer for multi-echelon warfighter exercises. His previous assignments include senior GEOINT advisor and GEOINT officer in charge (OIC), Joint Intelligence Operations Center–South, J-2 Intelligence Directorate, USSOUTHCOM; GEOINT OIC and Tactical Exploitation System-Forward OIC, Analysis and Control Element, G-2 Intelligence Directorate, I Corps; Aerial Reconnaissance Support Team mission lead and senior analyst, Task Force ODIN, 21st Cavalry Brigade, Regional Command-South, Afghanistan, for Operation Enduring Freedom; Senior GEOINT and MASINT analyst, Theater Ground Intelligence Center-Central, 297th Military Intelligence Battalion, 513th Military Intelligence Brigade with two deployments as a GEOINT analyst and MASINT liaison officer, Joint Intelligence Support Element, J-2 Intelligence Directorate, 3rd and 7th Special Forces Group (Airborne), Combined Joint Special Operations Task Force, Afghanistan, for Operation Enduring Freedom.

While serving as the G-2 GEOINT OIC at I Corps, CW2 Stephen Barber personally developed a partnership between I Corps, the Training and Doctrine Command Capabilities Managers for Sensor Processing, Geospatial, and Intelligence Sensors, and the Distributed Common Ground System-Army (DCGS-A) program office. This partnership not only allowed I Corps to leverage the latest in DCGS-A architecture but also provided a real world test bed for future developments of the system. CW2 Barber was the first to field the next-generation version of the Tactical Ground Station and led U.S. Forces Command in the development of the Operational Intelligence Ground Station, the successor for the Tactical Exploitation Systems at all Corps and Aerial Exploitation Battalions.

After ensuring the success of DCGS-A integration at I Corps, he utilized that knowledge and experience to ensure effective intelligence communications at the strategic level at USSOUTHCOM. As the senior GEOINT advisor at USSOUTHCOM, CW2 Barber helped shape the development of joint processing, exploitation, and dissemination standards, and he hosted GEOINT and light detection and ranging communities of interest to ensure tradecraft competency and enhance the readiness and analytical capabilities of deployable forces. As the production lead for SOUTHCOM's premier intelligence, surveillance, and reconnaissance platform, he directly contributed to countering terrorism and transnational organized crime, providing humanitarian assistance, and building partner nation capacity in the region. Vacating a spot on the Command Army 10 Miler Team, in October 2016, CW2 Barber led the GEOINT team deployed to Haiti in support of Joint Task Force Matthew—a humanitarian and disaster relief operation that delivered more than 600,000 pounds of supplies.

CW2 Barber's awards and decorations include the Defense Meritorious Service Medal, Meritorious Service Medal, Joint Service Commendation Medal (1 Oak Leaf Cluster), Army Commendation Medal (1 Oak Leaf Cluster), Joint Service Achievement Medal (1 Oak Leaf Cluster), Army Achievement Medal (3 Oak Leaf Clusters), National Defense Service Medal, Afghanistan Campaign Medal (3 Campaign Stars), Global War on Terrorism Service Medal, NATO Medal, Army Service Ribbon, the Military Intelligence Corps Association Knowlton Award, and the National Geospatial-Intelligence Agency's GEOINT Professional Certification–Fundamentals.

Sergeant Angel V. Guanlao
2017 Recipient
Command Sergeant Major Doug Russell Award For Excellence in Military Intelligence

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

SGT Angel Guanlao was born in Pampanga, Philippines, and raised in Seattle, Washington. He enlisted into the U.S. Army in January 2012 and attended basic training at Fort Benning, Georgia. Afterwards, he went on to Advanced Individual Training at Fort Huachuca, Arizona, where he graduated with honors as a 35T, Military Intelligence Systems Maintainer/Integrator.

SGT Guanlao's previous assignment from 2013-2015 was with Headquarters and Headquarters Detachment, 719th Military Intelligence Battalion, 501st Military Intelligence Brigade at Camp Humphreys, South Korea. He was assigned as the lead intelligence systems technician on Forward Detachment J situated on Goryeo-san Mountain along South Korea's Demilitarized Zone. During this assignment, SGT Guanlao participated in multiple exercises and drills with the South Korean Army and Marines. He attended the Basic Leader Course at Camp Jackson, South Korea, in 2014. He graduated on the Commandant's List and was named the Commandant's Inspection winner for his cycle.

In 2015, SGT Guanlao was assigned to Headquarters and Headquarters Detachment, 24th Military Intelligence Battalion, 66th Military Intelligence Brigade, as the intelligence and electronic warfare noncommissioned officer in charge. He maintained intelligence systems in support of unified land operations across the U.S. European Command theater, regionally aligned forces, North Atlantic Treaty Organization, and Allied and partner nations. In the absence of a sergeant first class and despite being resourced at less than 20 percent personnel strength, SGT Guanlao forged a team of systems maintainer/integrator Soldiers, field software engineers, intelligence architecture, and knowledge management personnel that earned accolades from theater-level senior intelligence leaders throughout 2016.

As a result of SGT Guanlao's technical acumen, he led his Intelligence and Electronic Warfare (IEW) Section in improving the 66th Military Intelligence Brigade's operational readiness and theater intelligence posture by providing exceptional Distributed Common Ground System-Army (DCGS-A) brain services. He expanded support to unified action partners, two major Army Service component commands, two multinational headquarters, regionally aligned forces, and the Joint Multinational Readiness Center. His section maintained more than 200 mission critical DCGS-A systems, 550 work stations, 90 servers, and 50 tactical systems across five network domains at an unprecedented 100 percent operational readiness rate. SGT Guanlao's systems maintenance team developed procedures for the remote installation of security software updates and patches that facilitated the transmission of DCGS-A data over the Global Rapid Response Information Package and Broadband Global Area Network Systems. This innovative solution enabled the XVIII Airborne Corps and U.S. Special Operations Command to utilize time-sensitive intelligence to conduct uninterrupted unified land operations in the U.S. Central Command area of operations; a program now implemented Army wide. Additionally, his IEW Section implemented the $28 million dollar upgrade and accreditation of the U.S. Army Intelligence and Security Command's first Joint Worldwide Intelligence Communications System DCGS-A brain system.

In addition to his technical expertise, SGT Guanlao's dedication to his Soldiers was reflected in everyday leadership as he continuously exceeded mission expectations and led his Soldiers to receive Platoon of the Quarter three times in 2016.

SGT Guanlao's awards and decorations include the Army Commendation Medal, Army Achievement Medal, Good Conduct Medal, National Defense Service Medal, Global War on Terrorism Service Medal, Korean Defense Service Medal, Noncommissioned Officer Professional Development Ribbon, Army Service Ribbon, and Overseas Service Ribbon. SGT Guanlao has also been awarded the German Armed Forces Marksmanship Badge qualifying Bronze.

Men Wanted for the Army
I WANT YOU FOR U.S. ARMY
NEAREST RECRUITING STATION
WORLD WAR I CENTENNIAL COMMEMORATION
1916
1919
REMEMBER ★ HONOR ★ EDUCATE

Moments in MI History

World War I Counterintelligence Agents Get Their Man

February 1918

by Lori S. Tagg, USAICoE Command Historian

On August 13, 1917, the U.S. Army's Military Intelligence Section (later elevated to Division) created the Corps of Intelligence Police (CIP) to protect American forces in France from sabotage and subversion. CIP agents also conducted special investigations, including suspected German espionage activities, throughout the United States. The CIP had difficulty apprehending the enemy agents involved because they often fled to Mexico. Several CIP agents were stationed along the United States-Mexico border during this period to investigate and apprehend suspected German spies.

Two CIP agents in Nogales, Arizona, Captains Joel A. Lipscomb and Byron S. Butcher, recruited Dr. Paul B. Altendorf to infiltrate German spy rings in Mexico. Altendorf was an Austrian immigrant to Mexico, where he served as a colonel in the Mexican army. Known to the CIP as Operative A-1, Altendorf managed to join the German Secret Service and established links with several other German spies living in Mexico.

In January 1918, the CIP learned that Altendorf was accompanying one Lothar Witzke from Mexico City to the U.S. border. Witzke was a 22-year-old former lieutenant in the Germany navy, who alternately went by Harry Waberski, Hugo Olson, and Pablo Davis, to name just a few of his many aliases. He had long been under CIP surveillance as a suspected German spy and saboteur. During the trip from Mexico City, Witzke had no suspicion that his companion was an Allied double agent taking note of Witzke's every move and indiscretion. At one point, a drunk Witzke let slip bits of information that Altendorf quickly passed on to CPT Butcher. Specifically, Altendorf informed the CIP that Witzke's handlers had sent him back to the United States to incite mutiny within the U.S. Army and various labor unions, conduct sabotage, and assassinate American officials.

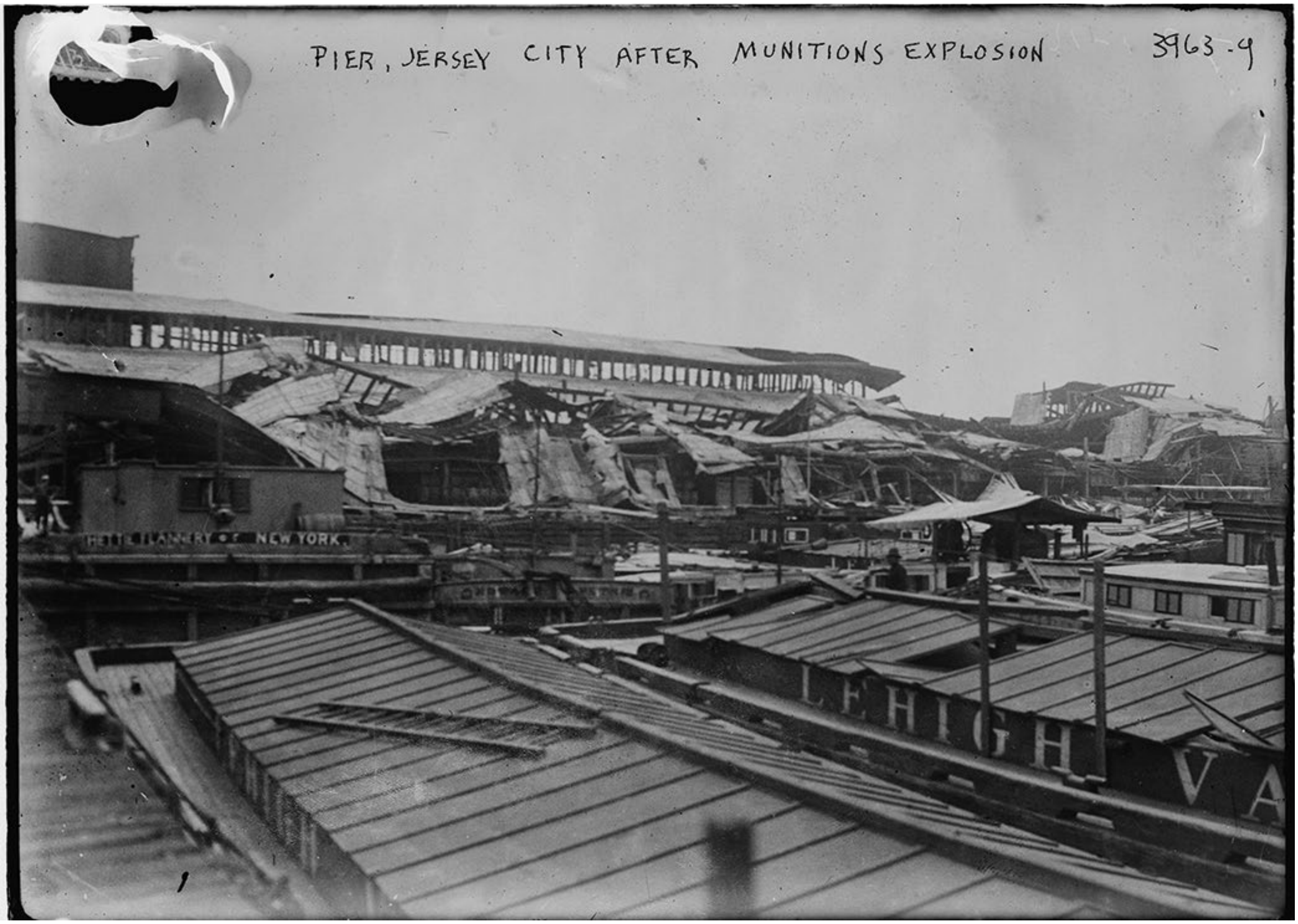
On or about February 1, 1918, CPT Butcher apprehended Witzke once he crossed the border at Nogales, Arizona, and a search of Witzke's luggage revealed a coded letter and Russian passport. CPT John Manley, assistant to Herbert Yardley in the Military Intelligence Division's MI-8 Cryptographic Bureau in Washington, DC, deciphered the letter, revealing Witzke's German connections. The letter stated, "Strictly Secret! The bearer of this is a subject of the Empire who travels as a Russian under the name of Pablo Waberski. He is a German secret agent."

While detained at Fort Sam Houston, Texas, awaiting trial, Witzke was extensively interrogated by CIP agents but refused to provide any details about his contacts, co-conspirators, or alleged espionage. His trial began in August 1918, and witnesses against him included Dr. Altendorf, CPT Butcher, CPT Lipscomb, and CPT Manley. Witzke took the stand in his own defense and spun a fantastical tale of how he was simply a down-on-his-luck drifter framed as a German spy. The military commission found Witzke guilty of espionage and sentenced him to death, the only German spy thus sentenced in the United States during World War I. After the war, President Woodrow Wilson commuted his sentence to life in prison, and he was transferred to Fort Leavenworth, Kansas. In 1923, however, Witzke was pardoned and released to the German government.

A decade later, during the international Mixed Claims Commission hearings into damages related to the war, several American lawyers revealed Witzke's role in the sabotage of the Black Tom Island munitions depot in New York Harbor on July 20, 1916. Ostensibly, he had been one of three collaborators who had placed dynamite on several barges loaded with ammunition causing a blast felt as far away as Philadelphia, Pennsylvania, and Maryland. The explosion lit up the night sky, shattered windows, broke water mains, and peppered the Statue of Liberty with shrapnel. Seven people were killed. Although in 1939 the Mixed Claims Commission found Germany complicit in the sabotage, Witzke and his co-conspirators, allegedly responsible for the worst act of terrorism on American soil up to that time, went unpunished. Additionally, Germany refused to pay the $50 million judgment.

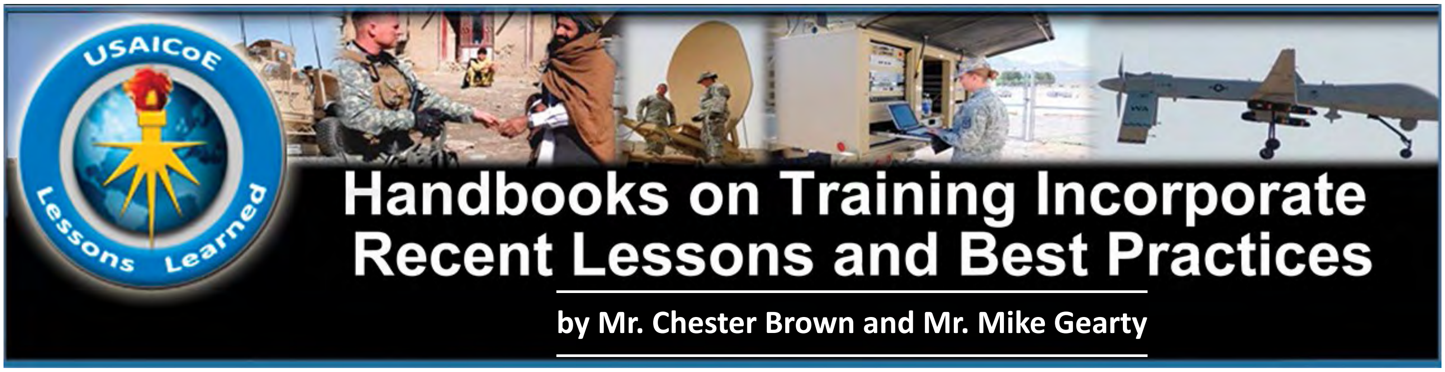
The capture of Witzke and other German spies and saboteurs by the Army's counterintelligence agents undoubtedly prevented many, but not all, planned sabotage activities during the war. Such incidents poisoned relations between the United States and Germany and introduced suspicions and fear in the minds of the American public. Americans could no longer assume complete security from enemy acts of terror on United States soil, a reminder still valid today.

For more information on the Black Tom Island incident, see Michael Warner's "The Kaiser Sows Destruction: Protecting the Homeland the First Time Around," https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no1/article02.html#rfn12.



Library of Congress Photo

Damage to a pier at Black Tom Island caused by German sabotage to prevent American munitions from reaching Germany's enemies.



Handbooks on Training Incorporate Recent Lessons and Best Practices

by Mr. Chester Brown and Mr. Mike Gearty

Concurrent with the publishing of this issue of MIPB, a new handbook that seeks to provide useful military intelligence company (MICO) training and employment tips learned from Army officers, warrant officers, noncommissioned officers (NCO), and Soldiers is available via the U.S. Army Intelligence Center of Excellence (USAICoE) Military Intelligence (MI) Lessons Learned (LL) homepage, Intelligence Leader Development Resource (iLDR) website, and other collaborative sites throughout the LL and intelligence enterprise. This new handbook is the MICO Training Lessons and Best Practices for Leaders Handbook (Version 1.0). For brevity, we will refer to this publication as the MICO Training Handbook from this point forward.

The handbook's content is not written exclusively for MI personnel or limited to MI equipment or capabilities. The information is useful for all leaders involved with planning, directing, leading, and assessing the training of a MICO within a brigade combat team (BCT). The information included in this inaugural version was selected from the experiences and reports provided by leaders, and Soldiers of varying branches, warfighting functions, and operations over the past 24 months.

Updates to the MICO Training Handbook will occur upon receipt of new information. Working drafts of the future versions will only be available on-line through the USAICoE MI LL website.[1] By specifying "Version 1.0" in the current handbook's title, there is an expectation of further development informed by additional topics, experiences, and more recent examples of success. Major content changes to existing, or adding additional, chapters will result in a different version number (Version 1.0 to 2.0). Updates to existing chapters will change the version decimal (Version 1.0 to 1.1). We depend upon you—Soldiers and leaders—to provide us with your lessons and best practices to ensure the handbook is accurate, current, and relevant to your needs.

As an old television crime drama used to state in its opening narration, "Only the names have been changed to protect the innocent."[2] To avoid identifying specific units or personnel we use general descriptions of sources that present composite anecdotes or vignettes to illustrate information from over 200 separate observations. We also use vignettes and best practices derived from—

- Home station training.
- Operational deployments.
- Combat training center (CTC) rotations.
- Center for Army Lessons Learned (CALL) reports.
- USAICoE Lessons Learned Collection Reports.
- Intelligence and Security Command Detention Training Facility after action reports.
- MICO commanders, officers, and NCOs.

Other sources informing the handbook that we have collected or that contributors have provided to us include—

- Field observations.
- Lessons.
- Best practices.
- Insights.
- Concepts.
- Doctrine and emerging doctrine.
- Force design updates.

The MICO handbook will be a useful reference for commanders, intelligence officers, engineer officers, staff planners, and intelligence personnel at all echelons. Additionally, the handbook may provide insights useful for training developers, trainers, and combat developers. The Lessons Learned Team worked closely with senior intelligence trainers, MICO commanders, battalion and brigade intelligence officers, and intelligence professionals throughout the force, to identify and incorporate into the handbook topics they recognized as important for MICO training. The MICO Training Handbook attempts to guide the reader through the planning, resourcing and execution of MICO training as well as providing examples, references and links to other pertinent resources.

The production of the MICO handbook's compilation of lessons and best practices during the year of "Intelligence Readiness" is no coincidence. The driving force behind the handbook is to address the most frequent request for MI LL assistance from company grade officers and NCOs—How do I train my [MICO] Soldiers? This request for assistance topic is becomingly more frequent as unit commanders plan and conduct training to meet their Objective-T (Training) certification being reported to, and tracked at, the Headquarters of the Army level.

Earlier this year the Center for Army Lessons Learned (CALL) published a Home Station Training (HST) Handbook, which you can use to complement the MI specific lessons and best practices in the MICO Training handbook. The CALL Director describes the HST Handbook as, "a practical guide to assist leaders at brigade level and below in planning and executing effective training at home station. This handbook is designed to accompany FM 7-0, *Train to Win in a Complex World,* [5 Oct 16] and is based on observations collected from training events and Soldier and leader interviews from four brigades and eight training support agencies across the Army. It also identifies common issues and potential solutions to the challenges observed during training events." CALL's HST Handbook is available on the CALL website (login required)—https://call2.army.mil/toc.aspx?document=7471&file=true.

Both CALL's and USAICoE's training lessons can be put to good use when determining how to implement MI Gunnery 1.0 and 2.0 in your HST events. The combination of Army and MI lessons and best practices provide insights and tips to plan, resource, and conduct an effective training strategy. Version 1.0 of USAICoE's MICO Training Handbook contains four chapters and two appendices.

The first chapter presents effective techniques and references to help you plan MICO training. Units do not conduct MICO training in isolation. At all echelons, Army intelligence plays a critical role in enabling military decision making within mission command functions and processes. The handbook emphasizes how the MICO must train collectively with all the warfighting functions in order to be fully proficient in providing intelligence support to the BCT. Whether at home station or at a CTC, the intelligence warfighting function performance excellence requires integrated training of intelligence enablers and Soldiers with maneuver elements. The handbook describes how MICO commanders can take advantage of maneuver element's training events to simultaneously, maximize intelligence-specific training.

Issues involving training with various systems equipping the MICO fill the second chapter. The handbook links the most valuable lessons within this chapter to monetary value. Lessons confirm an unexpectedly high number of Financial Liability Investigation of Property Loss (FLIPL) actions for outgoing MICO commanders. We begin the chapter with tips on conducting property inventories and ensuring accountability of complex equipment sets. We want to help you, and your Soldiers, avoid having to undergo a FLIPL. We admit Version 1.0 content related to unmanned aircraft systems (UAS) is relatively sparse compared to other MI system disciplines. We continue to seek more examples of effective UAS HST strategies to share in Version 1.1.

Chapter 3 introduces MI-specific aspects of MICO leader knowledge, roles, and functions. The reader will rapidly identify the synergy in applying our handbook's lessons with those contained in Army training doctrine and CALL's HST Handbook. While our handbook references the same doctrinal products, we provide a MICO perspective on applying these resources. We also introduce the challenges specific to training the Soldiers and elements within a MICO that are not covered in sufficient detail in doctrinal publications, as those publications are intended for an Army-wide audience.

The last chapter in the current version is already under revision based on comments received from those who helped craft and review our initial attempt at producing the handbook. We deemed the role of the NCO in MICO training of such importance that we extracted the topic from Chapter 3 and used it to form the basis of Chapter 4, NCO Role in MICO Training. We delayed releasing the handbook from the original timeline to discuss this crucial role MI NCOs perform in conducting individual and collective training of MICO Soldiers, crews, teams, sections, and squads.

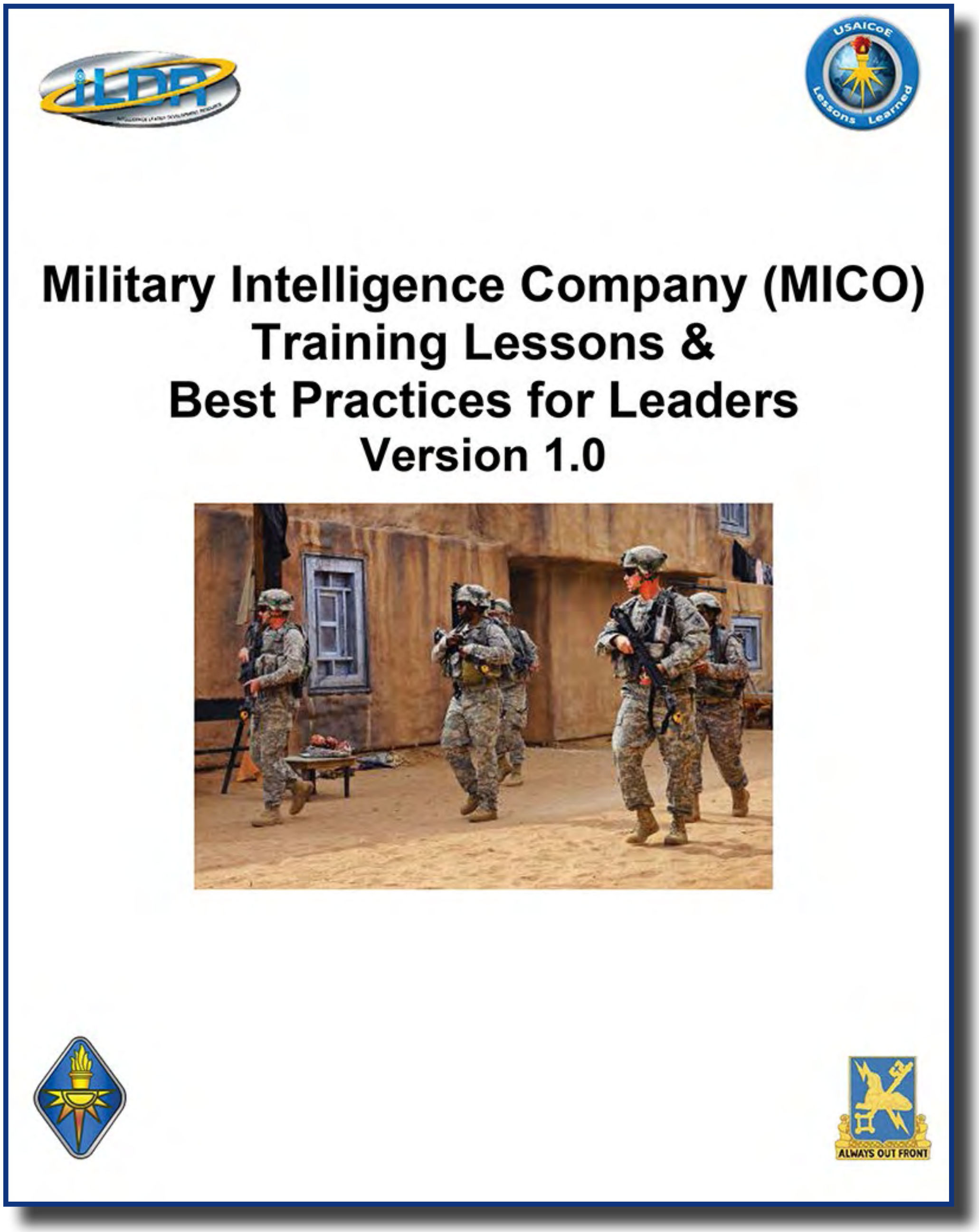
The handbook's appendices contain MI training references, web links, and examples of MICO training products, strategies and tools for planning and assessing training. Most of the products in the appendices are examples successfully used in collective training events by MICO elements. Examples of separate intelligence disciplines and MI systems are included. The seemingly contradictory attributes of detailed yet concise descriptions and assessment criteria are evident in most of the examples contained in Appendix B. You only need to re-name and tailor the examples to your particular situation to provide a starting point on which to build. We will add examples you provide to share with others in future versions.

We are fully dependent upon you—the experts in our profession—to help inform the operating and generating forces of successful techniques and practices. The lessons you share with us help others avoid the pitfalls and problems you may have experienced. We describe our philosophy in the LL email tag line, "The success of ICoE's Lessons Learned Team is determined by how successful we make others." What is missing from that tag line is that we are totally dependent upon those with whom we interact to share their lessons and best practices. Without your support, we cannot accomplish our mission to help others be successful. Visit our website, review the MICO Training Handbook, and send us your lessons and best practices, comments, or recommendations on how we can improve the next version.

Endnotes

[1] Access to the USAICoE Military Intelligence Lessons Learned webpage requires Common Access Card email certificate login. The web address is: https://army.deps/mil/Army/CMDS/USAICoE_Other/LL/SitePages/Home.aspx.

[2] *Dragnet* was an American radio, television, and motion picture series, enacting the cases of dedicated Los Angeles police detective, Sergeant Joe Friday, and his partners. This *Dragnet* hallmark feature is part of the show's opening narration which has undergone minor revisions over time. It has been featured in subsequent crime dramas, and in parodies of the dramas.



Military Intelligence Company (MICO) Training Lessons & Best Practices for Leaders Version 1.0

Proponent Notes

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

35D Critical Task Site Selection Board

by Captain Antonette A. Deleon

The U.S. Army Intelligence Center of Excellence (USAICoE) conducted a Critical Task Site Selection Board (CTSSB) for the MOS 35D, All-Source Intelligence Officer, from February 27 to March 10, 2017. The objective was to discuss and update the critical tasks expected of lieutenants, captains, and majors. Seventeen representatives traveled to Fort Huachuca, Arizona, from the—

- U.S. Army Forces Command.
- U.S. Army Military Intelligence Readiness Command.
- U.S. Army Cyber Command.
- U.S. Army Intelligence and Security Command.
- U.S. Army Special Operations Command.
- U.S. Army National Guard.
- U.S. Army Civil Affairs and Psychological Operations Command.

This is the first CTSSB conducted in person in the past 10 years. The previous CTSSB in 2013 was conducted in a virtual environment. This change resulted in maximum participation from the attendees, which made the CTSSB more efficient than past boards.

In preparation for the CTSSB, personnel from the Training, Development, and Support (TD&S) Directorate sent a survey to 1,500 intelligence officers in grades ranging from second lieutenant to lieutenant colonel. Approximately 10 percent of survey recipients (154 participants) responded to the survey. Previous CTSSB surveys generated a 3-5 percent response.

TD&S also arranged for guest speakers from throughout USAICoE to address CTSSB attendees on significant events occurring within the intelligence community. This included speakers from TD&S, the Office of the Chief, Military Intelligence (MI), and course managers from the MI Basic Officer Leader Course and the MI Captain's Career Course. Subject matter experts presented briefings in the fields of—

- Processing, exploitation and dissemination (PED).
- Intelligence, surveillance and reconnaissance.
- Cyberspace.
- Intelligence Leader Development Resource.

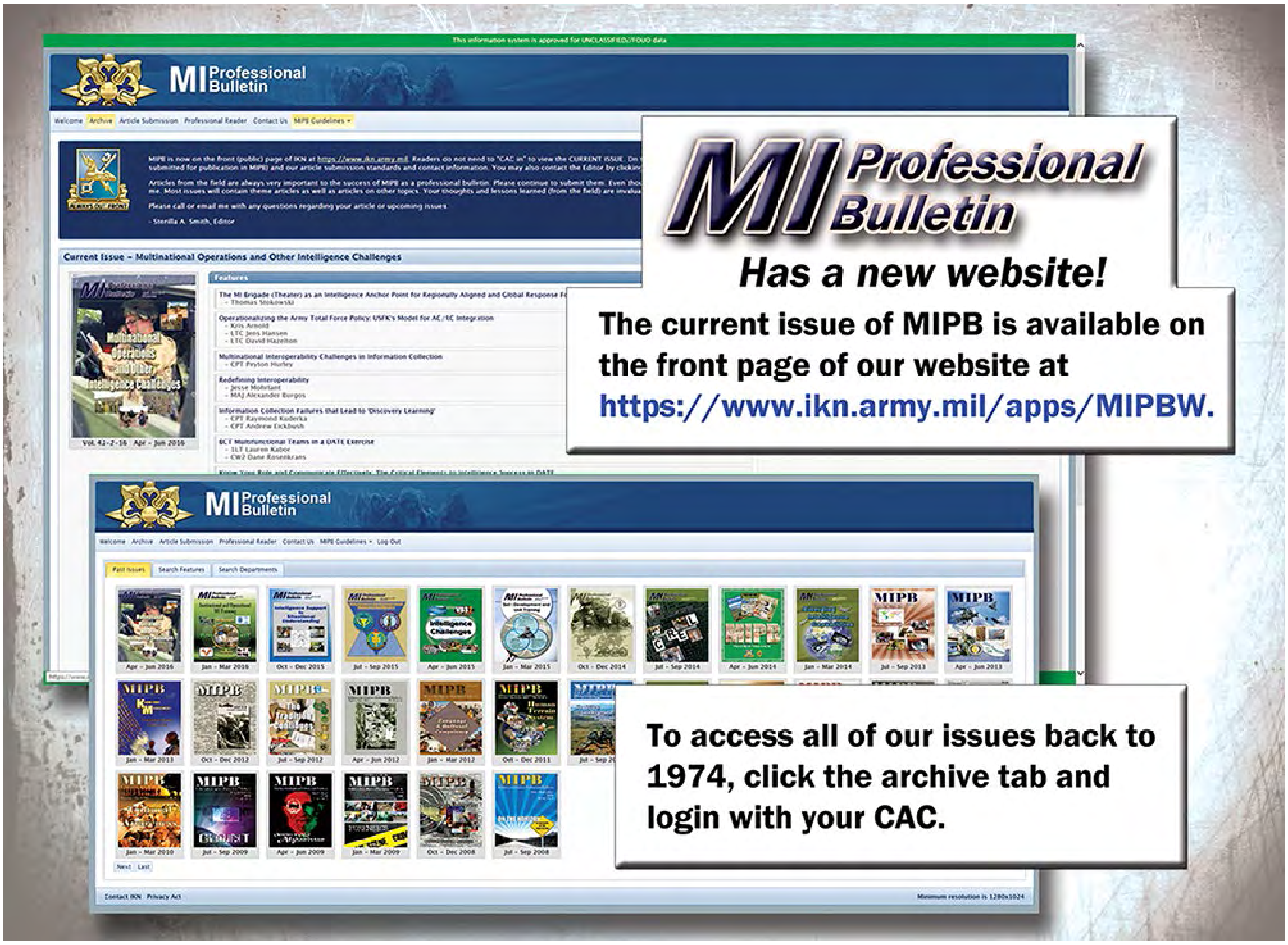
Battalion executive officers, company commanders, battalion S-2s, and PED and MI company platoon leaders were all represented at this year's CTSSB. USAICoE staff supplemented the field supplying additional expertise from civilians, warrant officers, and noncommissioned officers who had experience working for MI officers at various echelons. TD&S staff personnel acted as facilitators, ensuring the groups remained on task and that proper resources and personnel were available to answer questions and address concerns.

After 14 days, the board proposed 18 35D critical tasks, a marked decrease from the previous list, which contained 29 critical tasks. The new critical task list (CTL) is comprised of five critical tasks for lieutenants, six for captains, and seven for majors. All proposed tasks are tied to the intelligence core competencies and are nested with the CTLs for enlisted military occupational specialty (MOS) 35F, Intelligence Analyst, and warrant officer MOS 350F, All-Source Intelligence Technician. Tasks were updated with current doctrinal terms and references; follow the task, conditions and standards template; and included performance steps and measures, skills, and knowledge. Tasks are embedded to build upon each other by requiring a specific level of knowledge at each rank. Introduction of tasks occurs at the lieutenant level with certain conditions and standards. Once promoted to captain, the tasks expand requiring greater responsibility. Each task includes recommendations of frequency and type of training in either institutional, organizational, or self-developmental domains.

This year's CTSSB's critical task lists is expected to have a positive effect on the future of 35Ds by detailing what is needed to become successful MI officers. This experience allowed USAICoE to improve the process for future site selection boards. One of the board's recommendations was to hold the next CTSSB in five years, instead of three, to allow proper distribution of CTL updates to Army components and gauge their effects. Other recommendations for improvements include providing material to all participants prior to their arrival, providing on-site computer access to all participants, condensing the board from 14 days to 5 days, and to initially keep the group together to establish a foundation at the lower level prior to breaking up into separate groups.

CPT Deleon is the Professional Development Officer at the Office of the Chief, Military Intelligence.

Officers from the 10th Mountain Division (Light Infantry), 780th Military Intelligence **Brigade, U.S. Army Special Operations Aviation Command, 17th** Fires Brigade, 1st **Armored Division, U.S. Army Special Force Command, 201st** Expeditionary Military Intelligence Brigade, U.S. Army Military Intelligence Readiness Command, U.S. Army Combined Arms Center, U.S. Army Civil Affairs and Psychological Operations **Command, and the 500th Military Intelligence Brigade take a break from the 35D critical** task site selection board to pose for a group picture.



This information system is approved for UNCLASSIFIED//FOUO data

MI Professional Bulletin

MIPB is now on the front (public) page of IKN at https://www.ikn.army.mil. Readers do not need to "CAC in" to view the CURRENT ISSUE. On
submitted for publication in MIPB and our article submission standards and contact information. You may also contact the Editor by clicking

Articles from the field are always very important to the success of MIPB as a professional bulletin. Please continue to submit them. Even tho
me. Most issues will contain theme articles as well as articles on other topics. Your thoughts and lessons learned (from the field) are invalua

Please call or email me with any questions regarding your article or upcoming issues.

- Sterilla A. Smith, Editor

Current Issue – Multinational Operations and Other Intelligence Challenges

Vol. 42-2-16 Apr – Jun 2016

Features

The MI Brigade (Theater) as an Intelligence Anchor Point for Regionally Aligned and Global Response F
- Thomas Stokowski

Operationalizing the Army Total Force Policy: USFK's Model for AC/RC Integration
- Kris Arnold
- LTC Jens Hansen
- LTC David Hazelton

Multinational Interoperability Challenges in Information Collection
- CPT Peyton Hurley

Redefining Interoperability
- Jesse Mohrlant
- MAJ Alexander Burgos

Information Collection Failures that Lead to 'Discovery Learning'
- CPT Raymond Kuderka
- CPT Andrew Eickbush

BCT Multifunctional Teams in a DATE Exercise
- 1LT Lauren Kabor
- CW2 Dane Rosenkrans

Know Your Role and Communicate Effectively: The Critical Elements to Intelligence Success in DATE

MI Professional Bulletin

MI Professional Bulletin

Has a new website!

The current issue of MIPB is available on the front page of our website at https://www.ikn.army.mil/apps/MIPBW.

To access all of our issues back to 1974, click the archive tab and login with your CAC.

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:

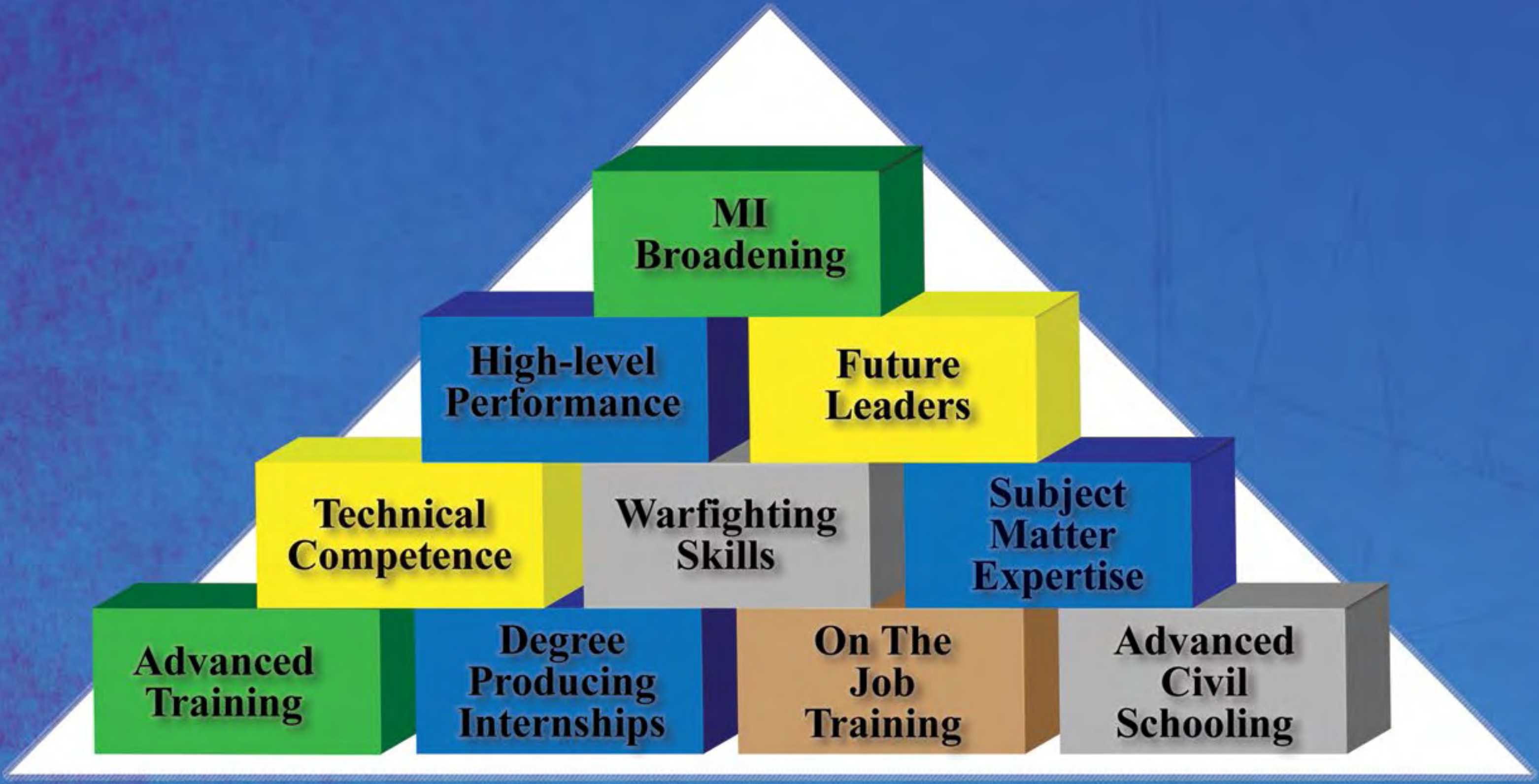
- A release signed by your unit or organization's information security officer/operations security officer/SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain (IAW AR 380-5 DA Information Security Program). A sample security release format can be accessed at our website at https://ikn.army.mil.
- 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

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



MI Broadening

High-level Performance

Future Leaders

Technical Competence

Warfighting Skills

Subject Matter Expertise

Advanced Training

Degree Producing Internships

On The Job Training

Advanced Civil Schooling

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

PIN:201905-000