

# MIPB

Military Intelligence Professional Bulletin  
April-June 2013

PB 34-13-2



Joint Targeting  
and  
ISR

## FROM THE EDITOR

In this issue, MAJ Koehler and Mr. Tatarka discuss the need for additional formal aviation-related intelligence training and increased manning of intelligence soldiers in the Army's combat aviation brigades intelligence sections. The authors specifically offer suggestions for training that are modeled after the U.S. Marine Corps intelligence training portions of its aviation courses. SSG Adair, from NTC, outlines how battlefield support battalion S2s can apply IPB to BSA site selection. 2LT Polek reviews the history and employment of the Shadow TUAS, its future, and the need for a rethink on possible alternative TUAS as the Shadow fleet ages and we enter a time of severe budget constraint.

MAJ Spahr offers lessons learned from his time as a combat BCT S2 on how to build intelligence teams within the BCT at all levels and how to develop healthy working relationships within the brigade staff by leading the intel effort. LTC Morrow discusses some misconceptions about OSINT that lead to its underuse as a source of intelligence and its perceived lack of credibility. How the synchronization of targeting and ISR to accomplish the commander's desired effects on the battlefield in the Joint environment is reviewed by MAJ Fair. Mr. Lint and Mr. Coleman address the need for vigilance and threat awareness in the uncertain climate brought about by sequestration. Finally, an article on a new software that will aid translators and linguists in locating and translating names and places in non-English documents.

Also included is the *Leader's Information Assurance/Cybersecurity Handbook* by the Army CIO/G6. It is a good tutorial for basic cyber security and offers many helpful links for training and contact information.

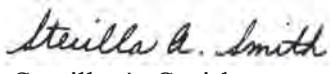
You will notice in the CG's *Always Out Front* column that the MI Corps Hall of Fame selectees for this year are named. As there will be no Hall of Fame ceremony this year due to budget constraints, these four individuals will join the Class of 2014 in a June 2014 Hall of Fame ceremony and induction. I have included their photographs on the inside back cover of this issue. Look for their biographies in our next issue (July September 2013.)

In an effort to improve the relevance, accessibility, and distribution of the Military Intelligence Professional Bulletin (MIPB) we are conducting a survey. For those of you who participated in the 2010 survey, some of the questions will be familiar. This will take no more than 5 minutes out of your schedule, and this time, there is a section for free form comment. I urge you to take this short survey. We respect our readers' feedback and want to make this publication as relevant and as accessible as we can. To take the survey, go to: <http://www.surveygizmo.com/s3/1190434/MIPB-Survey-March-13-2013> .

**REMINDER: If your organization/unit has moved or has been re-addressed, please send me an updated address at [sterilla.smith@us.army.mil](mailto:sterilla.smith@us.army.mil).**

Suspenses for MIPB are:

October-December 2013	S: 30 November 2013
January-March 2014	S: 28 February 2014
April-June 2014	S: 31 May 2014
July-September 2014	S: 30 April 2014



Sterilla A. Smith  
Editor

# MILITARY INTELLIGENCE

April-June 2013

Volume 39 Number 2

PB 34-13-2

## FEATURES

- Commanding General**  
Major General Robert P. Ashley  
**Deputy to the Commanding General**  
Mr. Jerry V. Proctor  
**Deputy Commander for Training**  
Colonel Lisa K. Price  
**Chief, Doctrine Division**  
Mr. Stephen B. Leeder

- MIPB Staff:**  
**Editor**  
Sterilla A. Smith  
**Design and Layout**  
Gary V. Morris  
**Cover Design**  
Gary V. Morris  
**Issue Photographs**  
Courtesy of the U.S. Army

**Purpose:** The U.S. Army Intelligence Center of Excellence (USAICoE) 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.

**Disclaimer:** Views expressed are those of the authors and not those of the Department of Defense or its elements. The contents do not necessarily reflect official U.S. Army positions and do not change or supersede information in any other U.S. Army publications.

By order of the Secretary of the Army:  
Official:



**Joyce E. Morrow**  
Administrative Assistant to the  
Secretary of the Army

1315601

**RAYMOND T. ODIERNO**  
General, United States Army  
Chief of Staff

- 4** **Intelligence Support in Combat Aviation Brigades**  
by Major Corby Koehler and Christopher Tatarka  
**13** **S2 IPB for BSA Site Selection**  
by Staff Sergeant Christopher Adair  
**15** **Supplementing Shadow's ISR Capabilities with an Expeditionary TUAS**  
by Second Lieutenant Matthew Polek  
**23** **S2 Leadership: 10 Lessons Learned from a Combat BCT S2**  
by Major Thomas W. Spahr  
**31** **OSINT: Truths and Misconceptions**  
by Lieutenant Colonel Craig D. Morrow  
**35** **The Targeting-ISR Relationship**  
by Major Jeffrey Fair  
**38** **Sequester and Furloughs: Discount Espionage Time**  
by James R. Lint and Timothy W. Coleman  
**41** **Leader's Information Assurance/Cybersecurity Handbook**  
by Army CIO/G-6  
**50** **Words and Action: How Text Analysis is Transforming the War on Terror**  
by the *HIGHLIGHT* Team  
**54** **Combined Arms Center: Doctrine Update, 3-13**

## DEPARTMENTS

- 2** **Always Out Front**  
**59** **Professional Reader**  
**60** **Contact and Article Submission Information**

**Inside Back Cover: 2013 Military Intelligence Corps Hall of Fame**

# ALWAYS OUT FRONT

by Major General Robert P. Ashley  
Commanding General  
U.S. Army Intelligence Center of Excellence



It is a great honor to accept command of the Intelligence Center of Excellence (CoE) at this time of significant change in our nation and across the Department of Defense (DOD). One task I am working on, in conjunction with the Army G2, the U.S. Army Intelligence and Security Agency (INSCOM), and the larger Army Intelligence Team is to provide the Chief of Staff of the Army (CSA) with a road map for Army Intelligence 2020 and beyond. This task is a tremendous undertaking and requires one voice for Army Intelligence across many organizations to include Department of the Army G2, INSCOM G2, the U.S. Army Forces Command G2, the Program Executive Office-Intelligence Electronic Warfare and Sensors, the Military Intelligence Readiness Command, the Army National Guard, and many others.

The road map will optimize intelligence support to an emerging Army 2020 that is ready to tackle the expeditionary challenges of the future hybrid threat in an environment of ever increasing change and complexity. Our purpose is to:

- ◆ First and foremost build agile leaders that understand the Army Profession, can leverage the Intelligence Enterprise, and can apply the attributes of mission command in the future operational environment in support of Unified Land Operations.
- ◆ Continue to adapt to the Army Learning Model 2015 as we modernize training initiatives aimed at enhancing our ability to support a globally and regionally aligned Army in a resource constrained environment.
- ◆ Gain CSA concurrence on a proposed way ahead for upcoming force structure and modernization decisions concerning the Expeditionary Military Intelligence Brigade, Aerial ISR Brigade, Theater Intelligence Brigade, Signals Intelligence, and CYBER.

*"I think [it's] very clear that... [our] main objective... is to preserve this magnificent land force that's been built over the last 10 years, and ensure we remain in the future what we are today: the greatest land power the world's ever seen."*

- Hon. John McHugh

*"Our Army is the Nation's Force of Decisive Action, A Relevant and Highly Effective Force for a Wide Range of Missions."*

GEN Raymond Odierno, CSA



- America's Force of Decisive Action
- Globally Engaged, Regionally Responsive
- Capable of Rapidly Dominating Any Operational Environment
- Interoperable with Joint/Multi-National/Interagency Partners



## Army Intelligence 2020 Priorities

- ✓ Provide the Best Trained, *Multi-Disciplined Intelligence Force* to Enable Decisive Action For the Nation's Current and Emerging Contingencies.
- ✓ Build the MI Force of the Future with a *Versatile Mix of Capabilities* to Meet the Current and Future Demands of a Robust, Ready, *Regionally Engaged and Responsive Army*.
- ✓ Keep our Army Intelligence Force in the Fight – Provide the Resources and Direction to Ensure *No Cold Starts, No MI Soldier at Rest*.
- ✓ Provide Solutions that Allow Our Soldiers on Point to Leverage the Technology, Expertise, and Intelligence in the Intelligence Enterprise.

Figure 1. Army Intelligence 2020 Priorities.

Major General Potter discussed the basics of Army Intelligence 2020 in the October December 2012 issue. The basics remain unchanged. Figure 1 does a good job of visually listing the Army Intelligence 2020 priorities within the context of Army 2020. The Army Intelligence community is on its way to a significant transformation that will result in improved capabilities and a stronger intelligence enterprise.

The mission of the Intelligence CoE during this transition is develop and educate our Army's Intelligence Soldiers, Civilians, and Leaders and design, develop, and integrate intelligence capabilities, concepts, and doctrine which supports unified land operations in a Joint, Interagency, and Multi-national environment. In executing this mission we plan to focus on four priorities/opportunities over the course of the next year. Figure 2 lists those four priorities as well as some tasks associated with each priority.

<input checked="" type="checkbox"/> <b>Invest in our Human Capital.</b>
<ul style="list-style-type: none"><li>• Focus on Leader Development and Reduction of Sexual Harassment/Sexual Assault</li><li>• Renew Focus on People during this Year and Next Year's Times of Fiscal/Resource Uncertainty</li></ul>
<input checked="" type="checkbox"/> <b>Support the Operational Army.</b>
<ul style="list-style-type: none"><li>• Provide Future Focused MI Soldiers through Strong Coordination with FORSCOM, DA G2, INSCOM, and TRADOC</li><li>• Increased Emphasis on Analytics, ISR Synchronization, Multi-disciplined Context and Writing Skills</li><li>• Drive Solutions for SIGINT Modernization, Big Data, Evolution of the COE</li></ul>
<input checked="" type="checkbox"/> <b>Modernize the MI Force, CYBER Integration.</b>
<ul style="list-style-type: none"><li>• Force Design in Support of Army/Intel 2020</li><li>• Support Cyber Institutional Unity of Effort</li><li>• DCGS-A Efficiencies and Ease of use, 35T, Proficiency on Intelligence Systems.</li><li>• Doctrine 2015</li></ul>
<input checked="" type="checkbox"/> <b>Transform and Sustain the Institution for the Army of 2020.</b>
<ul style="list-style-type: none"><li>• Leverage the Army Learning Model and Technology to Increase Academic Rigor for both AC and RC</li><li>• Transition to Decisive Action Training Environment (DATE), Work Cross-COE Collaboration</li><li>• Reduce Contract Support/Maximize Efficiencies across ICoE and Fort Huachuca.</li></ul>

Figure 2. USAICoE Priorities/Opportunities for the Upcoming Year.

the next Hall of Fame in June 2014, at which time we will honor both the Class of 2013 and the Class of 2014.

I am pleased to announce the names of the Class of 2013. Representatives across the force considered 35 nominations. The following were chosen: Mr. Robert Winchester, COL (R) William (Jerry) Tait, CSM (R) Franklin Saunders, and Brevet BG George Sharpe (Deceased). Please see a more extensive discussion of the Class of 2013 and their significant contributions in the July September 2013 issue of MIPB.

We also recognize and thank CW5 (R) Lon Castleton for his excellent service over the past six years as the Honorary Chief Warrant Officer of the MI Corps. He will become a Distinguished Member of the Corps as he turns over the reins to our new Honorary Warrant Officer, CW5 (R) Rex Williams. He will join COL (R) Al Elliot and CSM (R) Art Johnson who were installed as the Honorary Colonel and Sergeant Major, respectively, last year. Finally, I am extremely honored to have the opportunity to confer Honorary Membership in the MI Corps upon Mrs. Pauline Weinstein.

Please extend your congratulations to the Class of 2013. I look forward to seeing many of you during the 2014 MI Hall of Fame. More information about the very special event and our soon-to-be determined Class of 2014 will follow in a future issue of MIPB.



**Always Out Front**

# Intelligence Support in Combat Aviation Brigades



by Major Corby Koehler and Christopher Tatarka

## Introduction

Army aircraft are the single most expensive piece of Army equipment operating on the battlefield, with the cost of replacing individual airframes ranging from \$9.5 million for a UH-60L Blackhawk to \$28 million for an AH-64D Apache. Along with personnel and unit impacts, the loss of a single aircraft can have a substantially negative strategic level impact on operations due to loss of life of aircrews and the passengers onboard.

The impact of Army Combat Aviation is critical. During the War on Terrorism U.S. Army aircraft flew the most flight hours in combat zones and had the greatest number of aircraft hit and lost due to enemy action of any U.S. military service. Despite this there have been few institutional efforts made by the U.S. Army to substantially improve intelligence support to Army Aviation. That is not to say that individual aviators and intelligence professionals have not adjusted tactics, techniques, and technology or made, in some cases, impressive efforts to overcome these challenges. Rather the Army, as an institution, has not made the changes needed to enhance intelligence support to Army Aviation in a way that can reduce the risk to this critical capability.

In order to provide effective intelligence support to the combat aviation brigades (CABs) and their battalions that will help mitigate this risk, assigned S2 (Intelligence) sections need:

Airframe	Cost
UH-60A/L Blackhawk	\$ 9.4-9.5 million
UH-60M Blackhawk	\$ 15.5 million
CH-47D Chinook	\$ 10.6 million
CH-47F Chinook	\$ 24.1 million
OH-58D Kiowa Warrior	\$ 10.9 million
AH-64A Apache	\$ 20 million
AH-64D Apache Longbow	\$ 18-28 million

• The aircrew numbers differ for each air frame:  
–AH-64 & OH-58 (2 pilots), UH-60 (2 pilots and 2 crew chiefs), CH-47 (2 pilots, 1 flight engineer, and 2 crew chiefs).

• The majority of the catastrophic shoot downs have had a Chief Warrant Officer 3 (CW3) or CW4 in the aircrew.

• The Army has been able to absorb the monetary costs but the Aviation community has struggled to replace the experience lost in the catastrophic shoot downs.

Aircrew Experience	Cost
Flight School (IERW)	\$ 1.5 million
1000 flight hours for CW3/CW4	\$ 6 million
* Figured at \$6000.00 an hour for a UH-60 Blackhawk ** 1000 hrs estimated as a low minimum for CW3/CW4 with multiple combat tours	
<b>Total Cost of a Single Pilot</b>	<b>\$ 7.5 million</b>

Figure 1. Army Aircraft and Aircrew Costs

1. Formal aviation related intelligence training.
2. Qualified and trained dual track aviation and intelligence professionals (Area of Concentration (AOC) 15C, Aviation and 35D, All-Source Intelligence).
3. Adequate manning.

We will discuss these shortfalls and propose solutions to fill these gaps in order to substantially reduce the probability of costly aviation losses from enemy activity.<sup>1</sup>

## **Why Intelligence Support to Aviation is Different**

Inherent to any discussion of intelligence support in Aviation is to briefly compare the significant differences between this support and intelligence support to other types of ground based units. While complex, for the sake of this article, the differences can be separated into conceptual differences and more specific disparities in process and technique.

As any intelligence professional who has ever been assigned to an Aviation S2 section can attest, there are fundamental conceptual differences between intelligence support to Army Aviation versus support to ground based units. These differences are attributable to the complexities of an area of operations (AO) for Army Aviation as well as the requirements for analytical confidence in supporting these operations.

***“The dangers posed to Army aircrews by enemy Surface to Air Fires (SAFIRE) are nothing new. During the Vietnam war the U.S. Army lost in excess of 2,000 helicopters to hostile fire; 95% of which were due to small arms fire (14.5mm and below).”***

***“The mission profile of Army aircraft demands that, just like the soldiers in the HUMVEEs, have to go into harm’s way every day.”***

***“The reality of counterinsurgency warfare is that our aircraft fly in contested airspace and remain well within the enemy’s Weapons Engagement Zone (WEZ) 24 hours a day /7 days a week.”***

***“To optimize our survivability we can study the enemy’s patterns and use his tactics, weapons signatures and characteristics against him. To select the optimum counter tactics we must be able to answer two key questions, what weapon is the enemy firing at me and where is he firing from.”***

***—SAFIRE’s Two Biggest Questions, Tactics Division Newsletter, March 2007.***

The basic mathematics of the operational capabilities of Army aircraft translate into a fundamental difference between air and ground intelligence support. The speed of Army aircraft (typically 138 mph), the range of Army aircraft (typically over 250 miles), and the altitudes (three-dimensional battlespace) Army aircraft operate at (typically 0-2,000

feet AGL) immediately suggest that the S2 section must assess a large area along three dimensions (the volume of a massive area) vice the comparatively smaller linear AO of their ground counterparts. For example, in Operation Iraqi Freedom, it was not unusual for an Aviation battalion to have aircraft operating in every corner of the country on a daily basis, requiring their S2 sections to have a detailed understanding of the *entire theater’s* threat environment, not just a single localized area.

These conceptual differences create a cascading set of processes and techniques for intelligence support to Aviation that are well understood by the intelligence professionals assigned to these units. These include:

- ◆ Understanding the capabilities and vulnerabilities of friendly Aviation assets.
- ◆ A detailed understanding of enemy air defense capabilities.
- ◆ Adapting collection and targeting processes that account for the speed and range of aircraft.
- ◆ Analyzing terrain to support Aviation operations.

The fact that these areas are not covered in any detail in any formal Army intelligence training means that the adjacent and higher echelon ground based S2/G2 sections have little to no understanding of Aviation operations nor the threats to Aviation assets

which means that while their products are useful, they do not instantly result in an effective and useful Aviation threat picture.<sup>2</sup>

The existence of AOC 15C/35, which will be covered in greater detail later in this article, indicates that even the institutional Army supports the notion that intelligence support to Aviation is far different

than intelligence support to ground units since this formally defined, dual qualified position does not exist in any other Army intelligence section.<sup>3</sup> However, despite these differences, the current manning and institutional training emphasizes ground intelligence and reflects a general lack of understanding of intelligence support to Army Aviation.

## Aviation S2 Personnel Lack Formal Training

There is currently no formal Army training to teach the basics of intelligence support to Aviation to Military Intelligence (MI) personnel assigned to these units. As such, intelligence soldiers assigned to these S2 sections are left to their own initiative, research, and informal “on the job training” (OJT) to develop an understanding of how to support Aviation units.

All S2 sections must understand BLUE (Friendly) operations to be able to predict RED (Threat) actions and reactions. In addition, for Army Aviation intelligence sections to be successful they must know the different Aviation airframes; the unique aspects of Aviation missions; Aircraft Survivability Equipment (ASE), and Aviation tactics at a minimum to effectively analyze and predict the threat activity. Due to the complexity of Aviation operations few soldiers assigned to these S2s will be able to quickly and adequately gain this understanding through OJT.

Providing institutional training in these areas will provide soldiers the information and knowledge they require to support complex aviation operations.

## Existing Training

The MI branch offers numerous Military Occupational Specialties (MOS), AOC and Additional Skill Identifiers (ASI) producing courses across the intelligence disciplines. According to the 2012 Foundry

Manual of Training Opportunities there are 103 MI related courses that cover virtually every nuance of intelligence. However, none of the training focuses on, emphasizes, or is even marginally related to Aviation intelligence.

This lack of training is rooted in a belief which assumes that there is no difference between all-source intelligence in a ground unit and all-source intelligence in an Aviation unit. “All-source, is all-source, is all-source” is a common response when discussing the lack of training for Aviation S2 sections. However, the Army is the *only* service that holds this view. The Air Force, Navy, and Marine Corps all provide additional training on the specifics of Aviation intelligence to personnel assigned to these units.

The Air Force’s initial intelligence training (4-6 months) is focused on Aviation intelligence, af-

## Specific Aviation Intel Training (in weeks by branch)



\* Air Force Training metric derived from the average of min and max training durations ((18+28)/2) and includes initial training.

- The Navy offers several different specialized courses for intelligence officers serving in air wing intelligence positions (total of 7 weeks of training)
  - Naval Strike and Air Warfare Center (NSAWC) runs the courses
  - 1 week Basic Air Intelligence Course taken immediately after initial intelligence training
  - 2 week Strike Fighter Intel Primer taken prior to a carrier tour
  - 4 week Intelligence pre-deployment course
  - Have a greater Fixed Wing mission (Air Superiority, deep strikes, etc...)



- Marine Corps Aviation intelligence is covered in the initial training for intelligence personnel.
- Aviation intelligence is also treated as a separate intelligence discipline or track in the Marines.



- Marine intelligence officers that are assigned to aviation intelligence sections must attend the Air Intelligence Officer Course (AIOC/0207 course) after their initial intelligence training.
  - The AIOC/0207 course is a 12 week course that covers all the specifics of aviation intelligence.

- Enlisted Marine intelligence personnel assigned to aviation units attend the Aviation Specific Intelligence Training Program (ASITP) which is a 4 week course that covers required topics in aviation intelligence and information on the specific airframes they are supporting.

Unclassified

Figure 2. Navy and Marine Corps Aviation Intelligence Training.

ter which Airmen attend an additional course (2-4 weeks) for the specific airframe they will be supporting. The Navy offers several different specialized courses for intelligence officers serving in air wing intelligence positions for a total of 7 weeks of training at the Naval Strike and Air Warfare Center (NSAWC).

Perhaps most noteworthy given the similarity between mission and roles, is the Marine Corps where Aviation intelligence is taught in initial training for all intelligence personnel. In addition, Aviation intelligence is also treated as a separate track or intelligence discipline in the Marines. Officers assigned to Aviation intelligence positions attend the Air Intelligence Officer Course (AIOC) after their initial intelligence training. The AIOC, often referred to as the 0207 course, is a 12 week MOS producing course that covers all the specifics of Aviation intelligence. Enlisted Marine intelligence personnel assigned to aviation units attend the Aviation Specific Intelligence Training Program (ASITP), which is a 4 week course covering topics in Aviation intelligence and information on the specific airframes they are supporting.

The only course the Army has which links specifically to Aviation intelligence is the Tactical Operations (TACOPS) course, a 5½ week course for Aviation warrant officers at Fort Rucker. However, only the first 15 days (3 weeks) of the course cover applicable Aviation intelligence topics such as threats, weapon systems, aircraft survivability, and tactics.

In order to help bridge the gap in training for the officers assigned to Aviation intelligence sections the TACOPS course has, since 2010, occasionally and selectively allowed Aviation and MI officers to attend this course (enlisted soldiers are not authorized). While this information was not generally known to the CAB S2s and their battalion S2s, the effort has been an informal approach with a relatively small number of intelligence section attendees (approximately 20 in two years). While this is a move in the right direction, a permanent solution to this training shortfall that preferably includes all the personnel assigned to Aviation intelligence sections needs to be developed.

Army MEDEVAC aircrews are in a unique position to judge the effectiveness of formal Aviation in-

telligence training since many of these units have worked for both the Army and the Marines during the current conflict. Every MEDEVAC pilot interviewed with such experience stated that Marine Aviation intelligence support was vastly superior to that of the Army. Specifically, Marine intelligence sections understood Aviation operations, the threat, and the ASE vastly better than the *untrained* Army Aviation intelligence sections, which resulted in greater analysis and support from the perspective of the aircrews.<sup>4</sup>

In summary, the Army, unlike the other service components, offers no formalized Aviation intelligence training other than the TACOPS course. This has meant that these Soldiers, their sections, and their commanders are left to their own devices to “figure out” how to effectively operate. This situation creates a significant risk that a section may not be able to “figure it out” in a timely, efficient, and effective manner. This can result in the S2 section’s credibility being undermined in the eyes of its primary customers (the commander, staff, and aircrews) and/or worse, the loss of aircraft and personnel.

## **Aviation S2s Lack Trained Dual Tracked Professionals**

Within the U.S. Army personnel management structure is the rare hybrid AOC 15C/35 Aviation, All Source Intelligence Officer. To receive this AOC an individual must be qualified as both an Aviation officer and an MI officer. Aviation officers must complete the MI Officer Transition Course (MIOTC) and the MI Captains Career Course (MICCC). Reserve Component (RC) Aviation officers are required to complete the MICCC-RC.

By Modified Table of Organization and Equipment (MTOE) every CAB S2 and subordinate Aviation Battalion S2 should be a 15C/35. These officers also pilot the rotary wing airframes assigned to the CAB. The concept is that Aviation unit S2 sections are led by an Aviation branch officer who also understands MI. Ideally this officer should be an experienced aviator with Pilot-in-Command experience who can translate aviation operations and provide an invaluable perspective to the MI personnel within the sections. Each CAB is required to have five 15C/35s (Brigade S2 and four Battalion S2s). The Army currently has 20 CABs, so this adds up to a total CAB 15C/35 requirement of 100 personnel.

Type Org	15C/35 Req.	Units	Total	
CAB (AC)	5	12	60	100
CAB (RC)	5	8	40	
TAB (AC & RC)	Varies (7-8)	2	15	
AEB (AC & RC)	Varies (8-14)	7	69	
UNCLASSIFIED				184

Figure 3. Army Aviation AOC 15C/35 Requirements.

## The AOC 15C/35 Dilemma

The concept of the AOC 15C/35 suggests that within the Army and the MI and Aviation communities the notion that “all-source” intelligence techniques apply across the board to all units is not a universally held construct. Likewise, the combination of having a skilled aviator who also has detailed and extensive intelligence training has, in theory, the possibility of serving as a remedy to many of the Army Aviation intelligence issues. However, in reality, the unique AOC has not met the CABs’ needs for a number of reasons.

15C/35s are so few in number such that positions that are coded for these professionals are being filled by non-15C/35s. Likewise, the priority of filling 15C/35 positions is given to the aerial exploitation battalion (AEBs) over the CABs. Per Department of the Army Pamphlet 600-3, 15C/35 officers within AEBs are engaged in the employment of Special Electronic Mission Aircraft (SEMA) in support of tactical and strategic intelligence information collection. These SEMA aircraft are typically fixed wing intelligence collection platforms. These 15C/35 officers must complete the Fixed Wing Multi-Engine Qualification Course (FWMEQC) and the SEMA course to be qualified in their AEB positions.<sup>5</sup>

The result is that in CABs and their battalions it is common to find no 15C/35 serving as an Aviation S2. In fact, 15C/35 assignments to these billets have been so rare that many CABs and Aviation battalion commanders have given up on ever having a 15C/35. Instead they have formally requested to permanently change their MTOEs to replace the 15C/35 with a 35D so that their manning roster reflects reality. Occasionally an Aviation unit will assign a 15B (Aviation Combined Arms Operations) or 15A (General Aviation) officer as the S2 “out of hide,” but these individuals are aviators who are not trained in MI and often have little desire to do the job. Neither the 35D nor the 15B/15A is an ad-

equate interim solution since both are missing a requisite portion of understanding of Aviation operations or MI.

Considering that few of the CAB 15C/35 positions are filled with qualified officers, it would appear that not enough 15C/35s are being produced to meet Army requirements. In curious contradiction, the Army has formally acknowledged the importance of having intelligence trained aviators, but has not made this a priority. Whether this is due to the Aviation branch not identifying enough aviators to attend the MIOTC and MICCC or the MI branch not offering enough slots in these courses to aviators is beyond the scope of this article, but a cursory review suggests that AOC 15C/35 is likely stuck in a seam in the bureaucratic boundaries between Aviation Branch, MI Branch, the U.S. Army Training and Doctrine Command (TRADOC), and the Human Resources Command (HRC) with each entity assessing that this problem is in the bureaucratic battlespace of the others.

## Inadequate Manning Levels

Along with the issues of training and the availability of AOC 15/C35 personnel, CAB and Aviation battalion S2 sections suffer from inadequate manning levels. On the 2011 MTOE each CAB S2 section had 14 personnel. On the 2012 and 2013 MTOEs the CAB S2 sections were reduced by three MI personnel (a loss of an MI O-3/CPT, an MI E-6/SSG, and an MI E-4/SPC).<sup>6</sup> While the individual CAB S2 sections are reduced from 14 to 11 personnel, the total strength of the CABs actually grows from 128 personnel on the 2011 MTOE to 139 personnel on the 2012 MTOE and to 144 personnel on the 2013 MTOE

When asked about this reduction, the office of the Department of the Army (DA) G2 stated that the MI branch is responsible for intelligence support to the CABs and provides recommendations to the Aviation branch on the composition of Aviation S2 sections based on mission analysis and functional requirements. However, it is ultimately up to Aviation branch and TRADOC to “make a decision on the size of each staff section taking into account the overall size of the organization and what is affordable and what level of risk they are willing to assume.”

It appears that the Aviation branch used these three intelligence billets to pay for additions in other

2011 Combat Aviation Brigade (CAB)				
UNIT	POSITION	MOS/AOC	GRADE	
2011 MTOE	EDATE: 1 SEP 11			
HHC, CAB	S2	15C35	O4	
15 personnel	PLANS OFFICER	35D	O3	
	ASSISTANT S2	35D	O3	
	ALL SOURCE INTEL TECH	350F	W2	
	SR INTEL SGT	35F	E7	
	INTEL SGT	35F	E6	
	INTEL ANALYST	35F	E5	
	INTEL ANALYST	35F	E4	
	INTEL ANALYST	35F	E3	
NON-LETHAL	ELEC WARFARE SPT OFF <small>NOTE1</small>	35G	O3	
	INTEL SGT	35F	E6	
CP1 TAC	TAC INTEL OFFICER	35D	O3	
	INTEL SGT	35F	E6	
	INTEL ANALYST	35F	E5	
CP2 TOC	INTEL ANALYST	35F	E4	

#### Total CAB Intelligence personnel

12x Active Duty CABs 456 MI personnel

8x ARNG CABs 304 MI personnel

**20x CABs total 760 MI personnel (REDUCED TO 700)**

loss of 60 MI personnel from CABs with 2012/2013 MTOE

2013 Combat Aviation Brigade (CAB)				
UNIT	POSITION	MOS/AOC	GRADE	
2013 MTOE	EDATE: 1 SEP 13			
HHC, CAB	S2	15C35	O4	
11 personnel	PLANS OFFICER	35D	O3	
	ASSISTANT S2	35D	O3	
	ALL SOURCE INTEL TECH	350F	W2	
	SR INTEL ANALYST	35F	E7	
	INTEL SGT	35F	E6	
	INTEL ANALYST	35F	E5	
	INTEL ANALYST	35F	E4	
	INTEL ANALYST	35F	E3	
NON-LETHAL	INTEL SGT	35F	E6	
CP2 TOC	INTEL ANALYST	35F	E4	

\* Reduced by 4 personnel from 2011 MTOE

\* Reduced by 1 personnel from 2012 MTOE (30A conversion)

Note 1: 35G O3 position converted to 30A

Note 2: 2012 MTOE identical to 2013 MTOE for the CAB MI personnel.

Unclassified

Figure 4. 2011 MTOE vs. 2013 MTOE.

staff sections within the CABs, and felt the risk was acceptable. While developing resource solutions is always an extremely difficult task, given the major issues with a lack of specific training and the lack of 15C/35 officers in the CAB, at a minimum the manning in the CAB S2 sections should return to the 2011 MTOE levels. The decision to reduce the number of intelligence personnel given these functional problems exacerbates an already serious problem internal to the CABs and results in a significant operational risk.

The last decade has *clearly demonstrated* the ongoing threat to Aviation assets in the current operational environment, the extremely high cost of Aviation losses, the lack of adequate formal training for Aviation S2 sections, and the lack of qualified 15C/35 personnel in the CABs. Therefore, the decision to assume even more risk in the CABs by reducing the number of intelligence personnel is neither logical nor wise, given the possible outcomes.

## Improving Intelligence Support to Army Aviation

Given the three key problem areas regarding intelligence support to Army Aviation, we propose a set of suggestions and improvements which will substantially assist the Army in this area. These are separated into three distinct areas: training solutions, improving AOC 15C/35 levels, and overall manning.

**Training Solutions (This area should take priority.):** A formal Army Aviation intelligence ASI producing course must be developed jointly by the Aviation branch and the MI branch modeled on the TACOPS course and the U.S. Marine Corps aviation courses. At a minimum the course content should address these topics:

- ◆ Hybrid threats to Aviation.
- ◆ Opposing Forces Air Defense tactics.
- ◆ Threat weapon systems.
- ◆ Aircraft survivability and ASE equipment.
- ◆ Army airframes and capabilities.
- ◆ Aviation mission sets (attack, recon, lift, and heavy lift).
- ◆ Aviation tactics.
- ◆ Intelligence Preparation of the Battlefield from an Aviation perspective.
- ◆ Electronic warfare.
- ◆ Aviation Survivability Development and Tactics team historical aviation combat loss reviews.
- ◆ Targeting for attack Aviation.
- ◆ Collection planning.
- ◆ Intelligence support to Survival, Evasion, Resistance, and Escape, and Personnel Recovery.
- ◆ Aircrew briefing techniques.

- ◆ Analysis of helicopter landing zones and battle positions/engagement areas.
- ◆ Army Aviation Mission Planning System/Falconview training.

As the parts of the TACOPS course relevant to Aviation intelligence add up to 15 days (3 weeks), this course should be a minimum of 20 days (4 weeks) and would be appropriate for a TRADOC live environment course.

All MTOE Aviation S2 section positions must be coded with this ASI and tracked as a personnel measure in Unit Status Reports. This will ensure units send their personnel to this course. This will also allow a return on investment as HRC will be able to track and identify trained individuals throughout their careers for follow-on assignments.

In the near term, interim solutions which would help alleviate the training problem until such a course could be created include leveraging additional slots in the TACOPS course, securing slots in the Marine AIOC and ASITP courses for Army Aviation intelligence personnel, and seeking slots in the Air Force and Navy Aviation intelligence courses. An informal communication between one of the authors and the Director of the Marine AIOC course indicated that AIOC personnel would be willing to conduct mobile training teams (MTTs) for deploying Army Aviation S2 sections. Potentially the TACOPS course instructors could also be utilized to conduct MTTs to provide a near term solution as well. A potential funding mechanism for these MTTs could be created through the U.S. Army Foundry intelligence training program.

**15C/35 Solutions:** With an estimated 100 plus 15C/35 positions vacant in the CABs and their battalions there is no doubt that the Aviation and MI branches must recruit and train more aviators for these shortfalls.<sup>7</sup> In order to do so, the first thing that must happen is that the CAB S2 and battalion S2 billets should be the highest priority of fill for 15C/35s graduating from the MICCC.

This change would mean that filling AEB positions would need to be lower on the priority of fill. In addition, the requirement that AEB Aviation officers must be Aviation all-source Intelligence officers should be examined for modification.<sup>8</sup> For example, since the MICCC is used primarily as a

means to familiarize AEB officers with MI and the Intelligence Community (IC), such familiarization could be done in a significantly more cost effective manner by creating a short IC familiarization course and utilizing 15B aviators while maintaining the FWMEQC, SEMA course, and Top Secret clearance requirements.

This would then free up MICCC slots for the AOC 15C/35 officers in the CABs who have a real need to understand the type of tactical intelligence taught in that course. Further, by dropping the AEB/SEMA emphasis on the AOC 15C/35, the focus would return to its Aviation all-source intelligence roots and get the proper “need to have” training to the right aviators, vice “nice to have” training to AEB SEMA aviators.

**Manning Solutions:** The fix to the CAB S2 manning issue is simple. Return to the 2011 MTOE numbers by restoring the three reduced MI personnel (MI O-3/CPT, an MI E-6/SSG, and an MI E-4/SPC) to future MTOEs. This recommendation will inevitably require an assessment and difficult decision of determining who the “bill payer” will be within the CAB. Given that the 2012 MTOE increased the total number of personnel in the CAB from previous MTOEs, this decision should be less difficult than it could otherwise be.

Worth noting regarding all of the recommendations and solutions above is that in an upcoming era of what is likely stagnant or even shrinking Army budgets, the argument against these types of training and manning changes will be a perceived lack of funds for such initiatives. There is no doubt that the creation of an ASI course and fully training and filling 15C/35 slots will incur additional costs for personnel, temporary duty pay, and instructor pay. However, the case can be made quite easily that the cost of this training has the very real potential of reducing future costs associated with Aviation shoot downs as well as improving the effective use of already purchased and high cost Army Aviation assets. The argument that there are limited funds for new projects such as those described above is an empty one, as an era of stagnant or reduced budgets should lead to an emphasis on spending in areas that allow for reducing risk to existing assets, as well as those that have a high return on investment for future conflicts. These solutions do both.

## Conclusion

Despite lacking formal training, qualified personnel, and adequate manning, personnel assigned to Army Aviation intelligence sections have performed superbly during the current conflict. However, they have often had to do so *in spite of*, and not due to, the institutional Army's support to their efforts. The lack of institutional support has meant that S2s in the CABs seriously lack formal Aviation related intelligence training, lack qualified and trained dual track aviation and intelligence professionals (AOC15C/35), and suffer from inadequate manning levels required to sufficiently provide high quality intelligence support to aviation. While the solutions to these major problems are not without cost, they are certainly manageable from a budgetary and personnel standpoint.<sup>9</sup>



### Endnotes

1. Three products were drafted by the authors. This article focused on the facts and circumstances of the three main issues. A longer paper goes into greater detail on all the concerns the primary author has with intelligence support to Army Aviation and contains more details, personal opinions, and perspectives within the document. The third product (PowerPoint) supports both papers. These products can be requested from corby.a.koehler.mil@mail.mil.

2. It could be argued that the branch detail program of assigning combat arms officers (specifically Infantry and Armor officers) to the MI branch is the ground unit counterpart to the formally defined AOC 15C/35.

3. The requirements for IPE and the risk calculus for aviation creates a significant difference because the aviation intelligence section's customer has a greater need for analytical confidence than do most maneuver operations in which more risk can be assumed.

4. Marine Air Wing (MAW) intelligence sections are significantly larger (personnel wise) than CAB Intelligence sections and support fixed-wing and rotary-wing operations.

5. The DA Pam 600-3 description of the AOC 15C/35 (Chapter 11-1d(1)(a) 3.) focuses on the AEB/SEMA requirements. This Pam is currently being rewritten with some of the approved changes being the elimination the Aviator and MI officer status which drops the 35D connection, changes 15C/35 to 15C and SEMA positions will no longer be required to serve in MI coded positions or be qualified MI officers. Only the AEB MTOEs currently reflect the 15C change, 2013 CAB MTOEs still show 15C/35. SEMA Aviators will still continue to take the MICCC and SEMA courses but MICCC may become more of an option than a requirement. The CAB 15C/35 positions will still be required to attend MIOTC and MICCC.

6. This change resulted in a loss of 60 MI personnel across the 20 AC and RC CABs (760 MI personnel to 700 MI personnel).

7. The current regulations do not allow this but 15C/35s should also be recruited from the MI community. If an MI officer has a few years of MI experience and can meet all the physical requirements,

this individual should be afforded the opportunity to attend to the Initial Entry Rotary Wing (IERW) course and the Aviation officer Basic Course (AVOBC). This would increase the pool to recruit 15C/35s from and would have the added benefit of having an officer that likes and wants to do intelligence work. Another option for recruiting MI officers for the 15C/35 positions would be to adopt and apply the Medical Service Corps (MSC) process for recruiting Aero-medical Evacuation (67J) officers (MEDEVAC pilots) where officers (if selected) must be branched MSC and attend MSCOBC before attending the IERW course.

8. Serious consideration should be given to whether the AEB Aviation officers need to be Aviation all-source intelligence officers. The future changes to DA PAM 600-3 are taking the AEB SEMA positions further away from the Aviation all-source intelligence basics by no longer requiring them to be qualified MI officers. Since AEB SEMA Aviators are not doing Aviation all source intelligence work/production and the MICCC may become more of an option than a requirement there is little difference between them and their Aviation officer peers in the 15A and 15B AOC other than the Top Secret clearance requirements and the ASI/SI producing FWMEQC and SEMA courses.

In contrast, the 15C/35 in the CAB S2 billets are still required to attend the MICCC and must do all source intelligence, thus these 15C/35s have a significantly different skill set from their 15B peers and require a separate AOC designation. Additionally, Aviation flight courses produce ASIs, they do not produce an AOC. The 15B in an Attack Reconnaissance Battalion is the same as a 15B in an Assault Helicopter Battalion, which is the same as a 15B in General Support Aviation Battalion. The difference for these 15Bs is the airframe they fly and that is differentiated by the ASI for the position on the MTOE. For these reasons it would make sense to separate the CAB 15C/35 from the AEB SEMA 15C by either designating the AEB SEMA positions as a new separate AOC or by leveraging 15B Aviation officers (the predominant Aviation officer AOC) while maintaining the FWMEQC, SEMA course, and top secret clearance requirements.

9. Estimated cost of a TRADOC Aviation intelligence course is well below that of even a single airframe lost to a shoot-down. Assuming the course would be four weeks in length, require at least two instructors in addition to the TACOPS instructors, and that the training would take place at an Army post with lodging and classrooms available, the rough estimate is that it would cost \$1.4 million to train all 700 CAB intelligence personnel. The estimated annual cost after the CAB personnel are trained would be \$550,000 with an estimated annual demand of 200 students due to transfers, ETS, and other losses.

### References

CBO. (2007). Modernizing the Army's Rotary-Wing Aviation Fleet, Congressional Budget Office Paper, The Congress of the United States, Congressional Budget Office, Pub. No. 2898, November 2007.

DA Pamphlet 600-3. Personnel-General, Commissioned Officer Professional Development and Career Management, 1 February 2010.

ALARACT 231-2005. Clarification for Award of the Aviation Badge. Aylworth, Warren. SAFIRE's Two Biggest Questions, Tactics Division Newsletter, March 2007.

AR 600-8-22. Personnel-General, Military Awards, 11 December 2006 (Rapid Action Revision 15 September 2011).

DA Pamphlet 611-21. Personnel Selection and Classification, Military Occupational Classification and Structure, 22 January 2007.

DA PAM 611-21 Smart Book online.

FMSWeb. Data retrieved from FMSWeb on October 23, 2012 from: <https://webtaads.belvoir.army.mil/protected/WebTAADS/tools.asp>

Foundry Manual of Training Opportunities, June 2012,

Sloman, Jesse. September 2012. Fixing Intelligence Analysis: From Specialists to Experts. *Small Wars Journal*, 8, 9. Retrieved from <http://smallwarsjournal.com/jrnl/art/fixing-intelligence-analysis-from-specialists-to-experts>.

**The views expressed by the authors do not reflect the official policy or position of the departments of the Army and Defense, or the U.S. Government.**

Major Corby Koehler is currently the ACE Chief for the 34<sup>th</sup> Infantry Division. He has served as a Deputy G2, 34<sup>th</sup> Infantry Division; S2, 34<sup>th</sup> Combat Aviation Brigade, and as the S2, 2-147<sup>th</sup> Assault Helicopter Battalion deployed under the 12<sup>th</sup> CAB and Task Force 49 during OIF 07-09. He has experience in the attack, scout, and lift aviation mission sets. He is a qualified 15C/35 Officer and a qualified UH-60 A/L Blackhawk Instructor Pilot. He holds a Master's degree in Police Leadership as well as separate Bachelor's degrees in Criminal Justice, Sociology, and Psychology.

Christopher Tatarka, PhD, currently serves as Supervisory Intelligence Analyst in the U.S. Intelligence Community. A retired Army Lieutenant Colonel with over twenty years of active service, his military assignments included G2, 34<sup>th</sup> Infantry Division during OIF 09-10, Assistant Professor, Department of Behavioral Sciences and Leadership at the U.S. Military Academy, and a variety of intelligence and infantry assignments. He holds Bachelor's and Master's degrees in Psychology, a Master's Degree in Public Administration and a Doctorate in Business Administration.

# GREAT SKILL Program

Military Intelligence Excepted Career Program

## Our Mission

The GSP identifies, selects, trains, assigns, and retains personnel conducting sensitive and complex classified operations in one of five distinct disciplines for the Army, DOD, and National Agencies.

## Who are we looking for?

Those best suited for this line of work do not fit the mold of the "average Soldier." Best qualified applicants display a strong sense of individual responsibility, unquestionable character, good interpersonal skills, professional and personal maturity, and cognitive flexibility. **Applicants must undergo a rigorous selection and assessment process that includes psychological examinations, personal interviews, a CI-scope polygraph and an extensive background investigation.**

## Basic Prerequisites:

- ◆ Active Duty Army.
- ◆ 25 years or older.
- ◆ Hold a TS/SCI clearance.

For a full list of prerequisites, please visit our website (SIPRNET <http://gsd.daiis.mi.army.smil.mil>) or contact an Accessions Manager at [gs.recruiting@us.army.mil](mailto:gs.recruiting@us.army.mil) or call (301) 833-9561/9562/9563/9564.





## S2 IPB for BSA Site Selection

by Staff Sergeant Christopher Adair

### Introduction

When brigade support battalion (BSB) S2s arrive at the National Training Center they often find themselves at a loss with regard to identifying a location that lends itself to use as a brigade support area (BSA) in a decisive action (DA) environment. Formal Military Intelligence (MI) training primarily focuses on teaching MI professionals how to select a tactical assembly area for combat arms forces. While this knowledge is also critical in finding a suitable BSA location, additional considerations must be taken into account due to the unique nature and vehicular capabilities of a BSB. In this article I will cover the unique requirements and the procedures to help a BSB S2 identify acceptable BSA site locations utilizing Intelligence Preparation of the Battlefield.

### Site Considerations

The first step to consider when looking for a suitable BSA location in a DA fight is the proposed location of brigade (BDE) or brigade combat team elements for the next phase of the battle. As a general rule, the ideal distance for a BSA location is approximately 30 kilometers behind the forward line of troops (FLOT), or two terrain features towards the rear. If a FLOT will move too quickly to allow for a full movement of the BSA, a forward logistics element will be pushed forward to bridge the gap between the BSA and the FLOT. Knowing this, an S2 section can begin conducting a map reconnaissance of possible sites by plotting the proposed locations and movements of the BDE elements, which are spelled out in the BDE Operation Order.

The next consideration in the selection of a suitable BSA is the terrain. Consider terrain for an assembly area that is easily defensible and lends itself for use in the next phase of the battle. When selecting a suitable BSA location an area must be identified that is also relatively level, generally free of large boulders and other obstructions, does not contain soft pack sand or swamp lands, lacks large vegetation that is not easily removed, and should typically cover an area of no less than two kilometers by two kilometers. Use the BDE geospatial intelligence assets to produce maps which display pertinent BSA site information. To the maximum extent possible, locations immediately near population centers should be avoided to assist in protection against possible pilferage and overwhelming requests for medical support. A keen understanding of the local climate and weather patterns is also key to mission success; care should be taken not to place a BSA in a location that is prone to flash flooding.

Special consideration should be paid to ensuring that attached aerial assets have adequate landing zones (LZ). One LZ should be located next to the role II medical facility to ensure that proper medical evacuation (MEDEVAC) procedures can be initiated with no unnecessary delays due to inadequate LZ considerations. A second larger LZ should also be identified to allow for the sling loading of assets without interfering with MEDEVAC operations. An important and often overlooked consideration regarding rotary wing assets is ensuring the BSA is located in an area that allows for an adequate and safe approach by these aircraft.

## Selecting the Site

After indentifying all areas with suitable terrain that are the appropriate distance from supported units, the process of selecting the most suitable BSA site can begin. Taking into consideration the limited maneuverability of logistics vehicles, all areas requiring movement through terrain less than twelve and a half feet wide or fifteen feet high should be avoided as they pose unacceptable mobility restrictions on logistics transport vehicles. Areas that require logistics vehicles to move across soft sand or swamp lands, boulder strewn terrain, urban environments, or inclines/declines in terrain greater than 15 degrees to access the BSA should not be considered as viable locations due to the restricted mobility of logistics vehicles in these environments. Additionally, proximity to an alternate supply route (ASR) or main supply route (MSR) is a high priority consideration; this will aid in the ability to resupply the BSA and supported units more rapidly and efficiently.

Special consideration must be given by S2s in the planning of all BSB movements and tactical convoy operations in the BSB. Logistics vehicles have unique mobility limiting factors that must be planned for with regards to their armor, fire power, recoverability, and the terrain they can effectively traffic. When planning movements that may at some point require a large section of the BSB to move, a good rule of thumb to determine if the BSB can safely make the move is to determine if a HET would be able to pass the roads and defiles and if it could be recovered in the event of an emergency.

Once areas have been identified that are appropriate for BSA site selection due to their location with respect to supported units, terrain features, accessibility, and proximity to MSRs/ASRs, these areas must be compared against proposed enemy courses of action. BSBs organically have relatively little fire power and armor capabilities. If during the analysis of the selected potential BSA sites, it is determined that a BSA site is likely to be in the axis of advance of an enemy unit, the area should only be considered as a last resort in an effort to aid in force protection.

Enemy indirect fires and direct fires (DF) are also a large concern when selecting a site. It would be very easy for an enemy artillery barrage or even a

single tank to neutralize a BSB, thus preventing an entire BDE from conducting its mission. A preferred location for the BSA would be on the reverse slope of a mountain or large hill, using the surrounding terrain to the advantage of the BSB, providing protection against artillery fire, DF, and obscuration from observation. As the BSB moves further forward of the line of departure (LD) the inherent risk of enemy contact increases. Elements of a BSB face a wide array of threats and vulnerabilities forward of the LD that need to be identified and planned against by the S2 section. These threats include but are not limited to criminal and insurgent threats, hostile enemy forces, and terrain.

Once the best sites are selected the S2 should highlight the areas on a map, and when possible provide imagery of the proposed area for presentation at the mission analysis (MA) brief. It is imperative the S2 give the staff the best analysis and information possible when conducting MA in order to ensure assets are utilized in the best manner possible, and to reduce the amount of unnecessary risk to the BSB. When possible, S2s and other key leaders in the MA process should make a physical or aerial reconnaissance of the proposed areas. It is not uncommon for an area that appears to be free of obstructions on topography or even imagery to actually be unusable as a BSA. As a BSB S2 it is important to make sure your inputs are taken into consideration when planning a BSA movement.

## Conclusion

Taking all these considerations into account when planning a BSA jump will help ensure that support to the brigade is not compromised due to a BSA movement. Providing effective intelligence to support a sustainment organization is not as simple as it first appears. A BSB is susceptible to many additional threats that traditional combat arms units are not; these threats require an in-depth plan and full understanding of the capabilities of the organization in order to provide the most effective intelligence support possible.



*SSG Adair is currently assigned as the Sustainment Intelligence Trainer at the NTC. Prior positions include Assistant Reconnaissance Squadron Intelligence Trainer at the NTC and ANCOIC S2 while assigned to 1-63 AR, Fort Riley, Kansas.*

# Supplementing Shadow's ISR Capabilities with an Expeditionary TUAS

by Second Lieutenant Matthew Polek



*The views expressed in this article are those of the author and do not reflect the official policy or position of the Departments of Army and Defense, or the U.S. Government.*

## Introduction

The U.S. is a worldwide leader in TUAS (tactical unmanned aerial system) research, development, and production. The U.S. Army has benefited from this by having access to some of the most capable TUAS being developed by some of the most innovative manufacturers of unmanned technologies. One of the most prolific TUAS is the RQ-7 Shadow 200, which was first flown in the early 1990s. All variants of the Shadow 200 (there are technically four) are rapidly approaching their one millionth hour of unmanned flight.

Army UAS operators and technicians have proven time and again that manufacturer imposed limitations can be breached. Operator creativity and innovation have led to many improvements to Army UAS operations. However, despite Shadow's successes, Army TUAS requirements have exceeded what this system is able to offer. Presently there are preparations underway for another Shadow upgrade so this system can get closer to meeting the Army's intelligence, surveillance, and reconnaissance (ISR) goals.

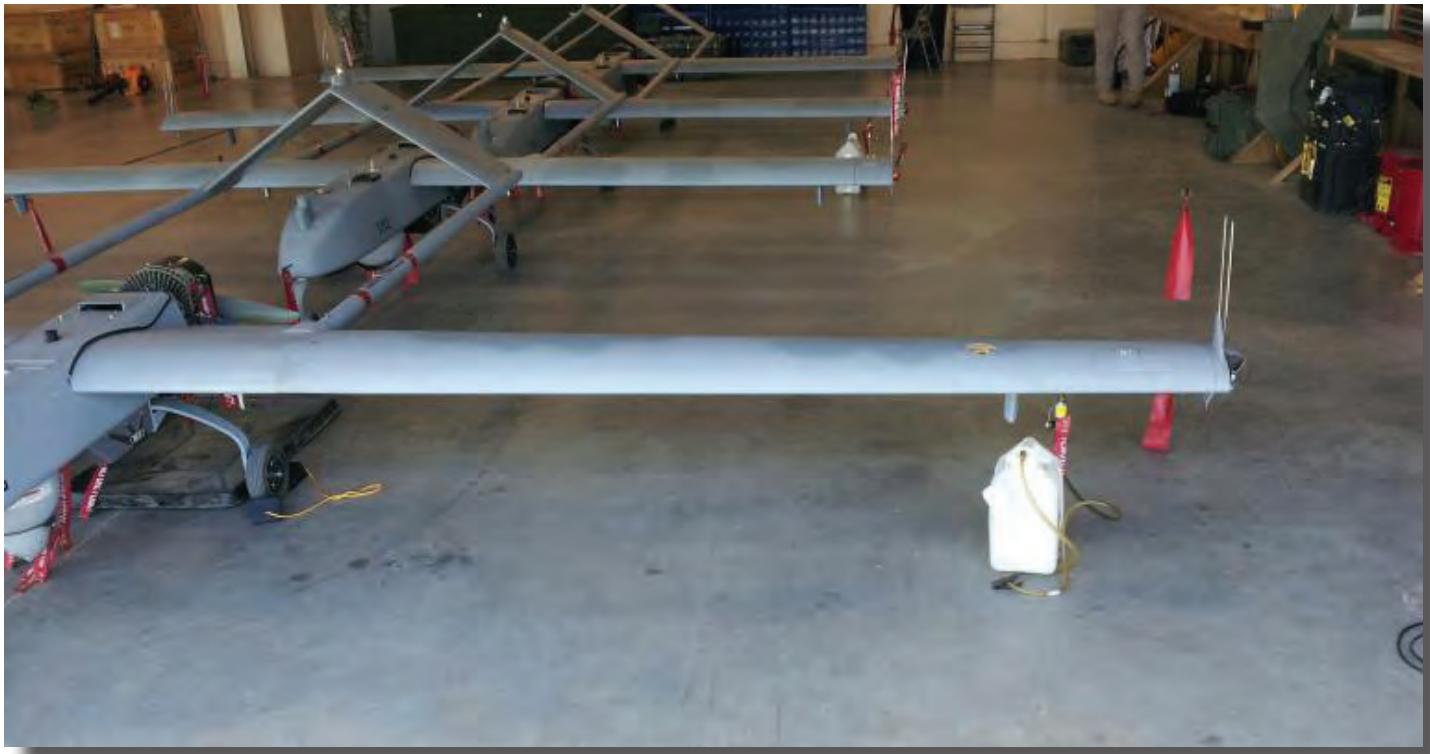
Overall, the Army appears to have lacked strategic direction and focus with the Shadow, which is evident when we assess the modifications and upgrades to this now multi-billion dollar program. The Army's tactical intelligence collection mission requires a longer-enduring TUAS and one that is more deployable than the Shadow. It needs to assess whether the Shadow alone is capable of fulfilling its tactical and collection needs. For some time the Army has been ignoring those TUAS that have been matching or exceeding the collection capability and cost-effectiveness of the Shadow. This

is the wrong path and one that may soon put us in a financial bind that could significantly reduce our future UAS purchase options and overall mission effectiveness.

## Endurance Concerns

Since its inception, flight endurance has been a concern for the Shadow. It has not been uncommon in the past 12 years of OIF/OEF for Shadow operators to break contact with a target during an operation to refuel. While much has been done to improve the performance and fuel capacity of the Shadow in an attempt to meet Army demands, these efforts have yet to fully satisfy requirements. Upgrading the RQ-7A to the RQ-7B in 2004 improved Shadow's endurance by approximately two hours for a total of six. In the Shadow, fuel is held in the two outer wings and the center wing. An upgrade to flight time typically correlates to an increased wingspan. The original RQ-7A grew from approximately 12 to 14 feet after the RQ-7B upgrade. The RQ-7C, Shadow's newest variant, also referred to as the RQ-7BV2 (Version 2), has an approximate 20 foot wingspan and is expected to achieve between 5 and 10 hours depending on the payload weight.<sup>1</sup>

The RQ-7C's payload capacity will be 110 pounds, which is nearly twice that of the RQ-7B. At capacity, the RQ-7C's payload has the potential to turn the Shadow into an over 500 pound UAV. Additionally, the 7C will have many software and hardware improvements to Shadow's mission shelters and launch and recovery computers. The Army originally had this variant scheduled to be fielded in FORSCOM units later in fiscal year (FY) 2013 but there is concern that this upgrade may now be put on hold or only partially fielded due to budgetary concerns. As the Army decides the fate of this new variant, many Shadow platoons have been receiving an extended wing upgrade, referred to as the "re-wing," which gives a standard RQ-7B an increased wingspan like the RQ-7C but without additional upgrades. Shadow's re-wing variant is said to provide nine hours of flight time.



An RQ-7B Shadow with extended wings and three other RQ-7Bs sit in the UAS platoon's hangar of B Co, 4<sup>th</sup> BSTB, 4/10 MTN DIV, Fort Polk, Louisiana.

### Losing Tactical Focus

The Shadow is a TUAS that has lost some of its ability to operate tactically and expeditionary. Note that the Shadow was originally chosen by the Army for its ability to be rapidly deployed and land on unimproved surfaces. RQ-7Bs that have already received the re-wing upgrade are still as tactical as the RQ-7As and do a great job landing on unimproved surfaces. The re-wing Shadows flown here at Fort Polk regularly land on a hard-packed gravel and dirt runway with a high degree of success. But keep in mind that Fort Polk's Shadow runway, despite being "unimproved," was still built by Engineers.

If a Shadow platoon was rapidly deployed and a predetermined operational site did not yet exist, a recon would have to be performed to find a suitable surface on which Shadow could land. This takes invaluable time and that is why the Army regularly defaults to existing airfields during fast-paced operations. At this point in time the Army has been lucky that our deployments have hinged on one Shadow platoon falling in on the already emplaced equipment of another. The logistics of having to move a Shadow launch and recovery site hasn't really been tested much in Iraq or Afghanistan for this reason.

Regardless, there is serious doubt that the upcoming RQ-7C variant will ever be flown out of any place where a paved runway doesn't exist. The reason for this is the increasing cost and weight of the Shadow. The maximum fueled weight of the RQ-7B is 375 pounds, which is approximately 50 pounds heavier than the 7A. The 20 foot re-wing RQ-7B variant weighs approximately 460 pounds fully fueled. If the RQ-7C's 110 pound payload capacity is utilized this UAV may far exceed 500 pounds at its maximum launch weight. Shadow's launcher will also have to be altered to support the weight of the new variant.<sup>2</sup> It is yet to be seen if a greater than 500 pound Shadow would be capable of operating on an unimproved surface.

Additionally, it is not known how well Shadow's landing gear is reacting under the added weight of the RQ-7C. When first introduced, the RQ-7A's tactical automated landing system (TALS) had a tendency to overcorrect in windy conditions which resulted in hard landings and cracked landing gear. A TALS upgrade and landing gear adjustment mostly eliminated hard landings for the RQ-7B, even with the extended wings. But the landing gear may very well need to be improved for a RQ-7C that houses an additional payload.

One concern is that Shadow's new laser designator, which sits approximately two inches from the ground, risks being damaged should a hard landing result from the RQ-7C's additional weight.

If the Army possessed an expeditionary capable TUAS that could be launched and landed without ever touching the ground, much time could be saved by avoiding runways altogether. The additional time it takes to coordinate with manned aircraft operating on the same airfield as a Shadow platoon has the potential to constrain mission times even further.

Future battlefields may not have improved surfaces conveniently located from which the Army can operate and units downrange could find themselves choosing operational sites solely because they have the paved landing surface the Shadow may soon require. This scenario is becoming a reality and the end result is an Army with a more versatile Shadow but with limited tactical maneuverability.

## Beyond Our Shadows

There will most likely be no further upgrade after the RQ-7C. Currently a heavily modified Shadow (Shadow M2) is being tested. The M2 is essentially a 500 pound Shadow variant that has a new fuselage and engine. The M2 will be able to carry multiple payloads and has a 25 foot wingspan that holds enough fuel for 15 hours of flight. By comparison, the M2 is to the Shadow what the Reaper is to the Predator: a larger, more capable variant. But due to the Army's budget problems this system may have arrived too late for the Army to seriously consider as a replacement for the Shadow. The Army could have the M2 for a "very modest incremental cost."<sup>3</sup> However, the Congressional Budget Office estimates that acquiring 20 RQ-7 Shadows and upgrading our entire fleet to the RQ-7C over the next five years will cost nearly \$2 billion.<sup>4</sup> \$358 million of this estimation was already set aside in FY 2012 by the Army to upgrade 172 Shadows to the RQ-7C variant.<sup>5</sup> This comes out to over \$2,000,000 per Shadow in upgrades, which is far more than the original total cost of the RQ-7A.



Approximately 2 inches from the ground, the Shadow's IR laser designator as it appears on a RQ-7B.



A Shadow M2 displayed in Farnborough, UK in July 2012.

Courtesy of the author.

Courtesy of Steve Flint, UK.

There are unmanned systems on the market right now that cost a fraction of the Shadow, get two to three times its flight endurance on half the fuel, have multi-sensor payload bays, and are also compatible with the One System Ground Control System (OSGCS). If more efficient, expeditionary, and cost-effective UAS options exist it would be in the Army's best long-term interest to aggressively pursue and field these systems in a select unit or two to test their integration and combat efficiency.

## A Capable Testbed

Despite any negative perceptions I have portrayed, I do not propose the Army get rid of the Shadow altogether. On the contrary, its growing payload and fuel capacity will allow it to transcend beyond typical ISR missions and will provide the Army an intelligence outlet typically only available on much larger platforms. However, just as smart phones and personal computers have become smaller, more capable, and more affordable, the same innovation has been applied for miniaturized UAV optics and sensors as well. The development of smaller UAS payloads is a growing market and miniaturized versions of current payloads on our larger platforms are actively being developed for smaller airframes.

The Army will certainly benefit from these developments by expanding its own collection capability through smaller payloads with the Shadow. The RQ-7C will be able to carry 110 pounds of any sensor we can stuff in the fuselage. Among these sensors are synthetic aperture radar, improved communications relay packages, and Electronic Intelligence and Signals Intelligence sensors developed specifically for smaller UAS. On the horizon there are lighter, higher definition cameras and stabilizing systems that will exceed all full motion video (FMV) expectations for our TUAS.

Additionally, the Shadow's payload capacity is not limited to sensors in the fuselage. As of 2011 the U.S. Marine Corps (USMC) has been leading the way in arming the Shadow and is engaged in a classified multi-million dollar weapons procurement program for part of their fleet. Each wing of the RQ-7C can be outfitted with a hard point capable of carrying 25 pounds. However, with this course of action the capability of the Shadow expands to that of hunter/killer and the argument regarding intelligence collection is being lost.

Marine commanders of the 1<sup>st</sup> Marine Expeditionary Force argued for munitions after they complained that during a six-month deployment in 2009 to Afghanistan Shadow operators lost track of 90 insurgents involved with improvised explosive device (IED) emplacement.<sup>6</sup> They stated that armed Shadows could have taken these IED teams out. Regardless of their excuses for losing track of 90 insurgents, the Marines may find out that with this path IEDs will still be emplaced and their Shadows will find even fewer of them thanks to the effect the added weight of munitions and associated electronics will have on fuel economy.

Courtesy of Lockheed Martin.



A test flight of a Shadow UAV with Lockheed Martin's 11 pound Shadowhawk munition. This weapon was first dropped from a Shadow in May 2012. The Shadow is reported to be capable of carrying a munition over twice this size.

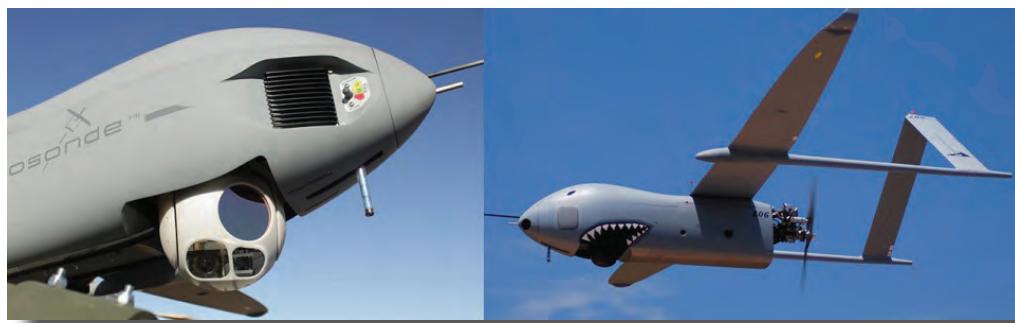
If Army commanders are also looking to enhance our Shadows with weaponry they should take a hard look at this path and consider whether or not current and future missions will require this capability.

Weapons may yet have their place in Shadow's mission. But if the Army is concerned with attacking the networks of our enemies then a better payload on a longer-enduring airframe, along with more payload training for our operators may be a more suitable answer at this time than munitions.

## Aerosonde and Capabilities/Landing

Until recently, the U.S. Special Operations Command (SOCOM) had been heavily invested in the ScanEagle TUAS for its operations. However, since the ScanEagle was ultimately unable to provide adequate breadth of collection for operations, SOCOM transitioned to the Aerosonde 4.7G TUAS in March 2012.<sup>7</sup> Like the Shadow, Aerosonde is compatible with the Army's OSGCS. It weighs approximately 70 pounds and has a 12 foot wingspan.<sup>8</sup> Since this UAV has a heavy fuel (JP-8) engine, flight endurance is expected to be 15 hours or longer depending on the payload configuration. Aerosonde's heavy fuel engine also allows it to carry payloads with higher electricity demands and results in performance improvements such as an increased climb rate, speed, and altitude ceiling.<sup>9</sup> Aerosonde lands by flying into a net, much like the Pioneer UAV but also has the option of a belly landing. Another selling point of the Aerosonde is that its launch site takes a fraction of the time to emplace than the Shadow.

A justifiable criticism of smaller TUAS like the ScanEagle is that it can carry only one electro-optical (EO) or infra-red (IR) camera at a time. The Aerosonde will carry Cloud Cap's TASE400 payload that can carry both EO and IR cameras. The TASE400 also has a third bay for an additional IR sensor, rangefinder, or laser pointer.<sup>10</sup> Aerosonde's payload weighs 14 pounds and is as capable as the 40 pound payload Shadow had 6 or 7 years ago.<sup>11</sup> Considering the Aerosonde weighs just 70 pounds, this is a major advancement for smaller TUAS payloads. It is just a matter of time before technology advances enough to allow a smaller UAV like the Aerosonde to have the highest quality FMV capability.



Courtesy of Goodrich Corporation and AAI.

At only 14 pounds, Aerosonde's retractable multi-bay payload is as capable as Shadow's 40 pound payload was 6 years ago. As technology advances, smaller TUAS will become more feasible options for Army intelligence collection missions.



Photo courtesy of the U.S. Navy.

Aerosonde's arresting net is combined with its launcher, making this platform capable of being mounted to virtually anything. Pictured is the U.S. Navy Stiletto. Shadow's logistical requirements prevent it from being as rapidly deployable as other TUAS.

The Aerosonde's cost is estimated to cost between 300 to 400 thousand dollars. Putting this cost into perspective, the Army signed a contract for \$70.7 million to provide 142 Shadows with laser designators.<sup>12</sup> That makes each of these designators worth about \$500,000 each. This should provide a little insight into the explosion of funds for the Shadow program.

## Transition

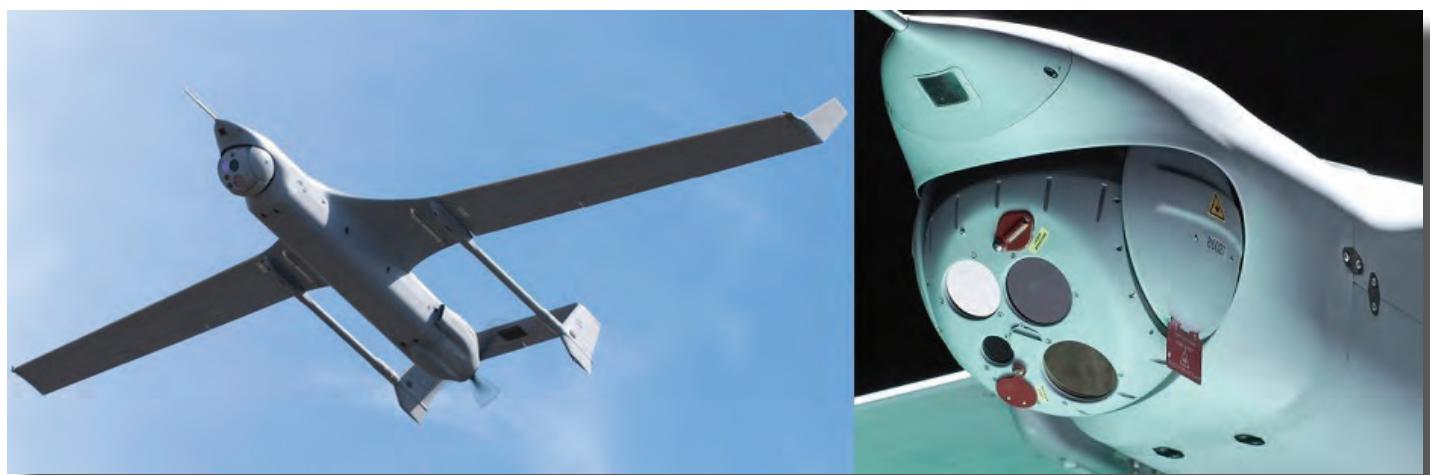
Expanding the Army's UAS fleet with a more tactical, longer enduring, and cost effective system could solve many of our ISR request issues. This could also help with the Army's budgetary shortfalls. I propose the Army outfit some of its most expeditionary reconnaissance, surveillance, and target acquisition squadrons; battlefield surveillance brigades, and intelligence brigades with TUAS that are capable collec-

tors but do not require the logistical ground support of the Shadow. Shadows in these units can be sent to those that are waiting for replacements. The Army could begin transitioning with the Aerosonde since this system is compatible with the OSGCS and is already being utilized by SOCOM.

According to the Department of Defense (DOD), the MQ-5B Hunter UAS is scheduled to retire in FY 2013 with the possibility of the retiring process spilling over into January 2014. As the area currently occupied by the MQ-5B Hunter becomes vacant, the Aerosonde or a similar UAS can take its place. If outfitting units with another TUAS isn't contractually possible, we should at least monitor SOCOM's success with Aerosonde and make an assessment based on that. When the time comes to make difficult budget decisions we will already have an idea of where money could be saved and where our needs can be met.

The Marines are already leading the way with TUAS diversification. Aware of the effects of Shadow's reduced tactical capabilities, they are mitigating them by contracting the Integrator UAS to operate alongside their Shadows. The Integrator is a 135 pound TUAS with a 16 foot wingspan that uses the same launch and recovery systems of the much smaller ScanEagle. This TUAS also carries a multi-sensor payload bay like the Aerosonde. The USMC's Small Tactical UAS (STUAS) Program Manager said the Shadow is "expeditionary to a point, but requires an improved runway for recovery."<sup>13</sup> The Marines are proactive and have acted to mitigate the tactical limitations brought about by Shadow's upgrades.

Photos courtesy of Insitu.



Due to its tactical capabilities, the Integrator UAS has been contracted by the USMC to supplement Shadow's intelligence collection mission.

## Electronic Warfare Concerns

The Shadow is the only UAS the Army has below corps level capable of providing tangible FMV for our battlefield commanders. Our fleet of Shadows is approaching 500 and, in essence, all of our eggs are in one basket at this level. It isn't discussed much, but the Shadow has already had at least two instances in recent years in which the whole fleet was grounded for mechanical and production flaws. Throughout the entire Armed Forces, there have been about a dozen instances in the past two years where an entire aircraft fleet was grounded for various reasons. But this had less effect on operations in our sister branches due to overlapping capabilities from other aircraft in their fleets. The Army does not have an answer if our Shadow fleet were to be grounded again.

Currently, the newest military technologies being sought around the world concern electronic warfare (EW) for UAS. American defense contractors are actively pursuing technologies specifically designed for offensive UAS operations. It should go without saying that our enemies are also developing technologies to counteract the capabilities we are seeking for our UAS. However, there has been less discussion about the possibility of an electronic attack against our UAS. Simply put, if the Army's Shadow fleet is somehow grounded due to an EW attack, or even a mechanical flaw discovered from a new upgrade, then the only other capable UAS in the Army's fleet is the Gray Eagle and the soon-to-be retired Hunter. We do not have as effective overlapping capabilities with our UAS fleet as we should.

The U.S. Army Communications-Electronic Research, Development and Engineering Center, Intelligence and Information Warfare Directorate and Program Manager Electronic Warfare are actively seeking contractors to provide EW packages for our UAS. They recently requested contractors to “determine what systems, capabilities and techniques currently exist, or could be modified, to provide UAS-based EW capabilities to include potential surgical/targeted EW techniques (with emphasis on successful completion of an Airborne Electronic Attack mission)”<sup>14</sup> According to this statement, the Army doesn’t want to develop new EW technologies for the future, we want modify them for Army UAS now. This also means that our enemies are doing the same.

The collection void that exists due to the Hunter’s retirement and Shadow’s expeditionary shortfalls puts the Army’s tactical level intelligence collection at risk. The Aerosonde is one of potentially many UAS that are proven and capable enough to fill the gap left by Shadow’s growth and will provide the Army a contingent UAS in case the Shadow fleet is grounded again.

## Conclusion

The era of strategic UAS such as the Global Hawk is over, at least for our generation. I mean this literally as the Air Force has stopped purchasing Global Hawks and will retire the fleet prematurely in FY 2014 due to purchase and maintenance costs.<sup>15</sup> And as the Army’s budget continues to shrink, our choice of new military technologies will soon be limited. However, there may be opportunity in this difficult situation for the Army to request smaller, more efficient UAS technologies from defense contractors that will be scrambling for fewer military contracts. As our fleet of Shadows grows, across the board upgrades and repairs will soon become too costly. The RQ-7C upgrade was already put on hold once in 2010 due to budgetary constraints and there has been unconfirmed discussion that it will be on hold once again for the same reason.<sup>16</sup> For some time Congress has been debating the price justification of military UAS. A 2012 Congressional Research Service report asks the question: “How should (the) DOD, Congress and the UAS manufacturers balance cost with capability?”<sup>17</sup>

TUAS diversification answers this question. We are potentially spending too much on a system that may one day prove inadequate for all our operational needs and we should act to correct these problems before they become too expensive to justify to Congress. The Army needs a TUAS that our MOS 15Ws can operate in the field, from any field. Considering the innovative defense contractor spirit that brought America’s intelligence sectors the Predator UAS 20 years ago, we should expect no less effort be invested in our demand for a more capable, tactical, affordable, and rapidly deployable TUAS for present and future operations.

## Endnotes

1. Congressional Budget Office, “*Policy Options for Unmanned Aircraft Systems*,” (CBO Publication No. 4083), June 2011, 4. At <http://www.cbo.gov/sites/default/files/cbofiles/ftpdocs/121xx/doc12163/06-08-uas.pdf>.
2. Scott R. Gourley, “Soldier Armed: Shadow UAS,” *Army*, 20 January 2012, 61-62. At [http://www.usa.org/publications/armymagazine/archive/2012/01/Documents/SA\\_0112.pdf](http://www.usa.org/publications/armymagazine/archive/2012/01/Documents/SA_0112.pdf).
3. Ibid., 62.
4. CBO, Publication No. 4083,4.
5. *AAI Unmanned Aircraft Systems Awarded \$358 Million for Upgraded U.S. Army and Marine Corps RQ-7B Shadow® TUAS*, 09 July 2012. At <http://investor.textron.com/phoenix.zhtml?c=110047&p=irol-newsArticle&ID=1712963&highlight=>.
6. Paul McLeary, “UAV to Change from Watcher to Hunter,” *Defense News*, 26 July 2012. At <http://www.defensenews.com/article/20120726/DEFREG02/307260002/UAV-Change->.
7. *AAI Unmanned Aircraft Systems Wins USSOCOM MEUAS II Award Valued at Nearly \$600 Million*, 11 Apr. 2012. At <http://phx.corporate-ir.net/phoenix.zhtml?c=110047&p=irol-newsArticle&ID=1682104&highlight=>.

8. *Aerosonde® Mark 4.7: Redefining Expeditionary*, 2010. At <http://www.aerosonde.com/pdfs/aerosonde-mark-47.pdf>.
9. *AAI Flies AeroSonde(R) Mark 4.7 Aircraft with Heavy Fuel Engine*, 07 Oct. 2010. At. <http://investor.textron.com/phoenix.zhtml?c=110047&p=irol-newsArticle&ID=1480238&highlight=1>.
10. *Goodrich Launches TASE 400 Stabilized Microgimbal*, 11 October 2011. At <http://ir.goodrich.com/phoenix.zhtml?c=60759&p=irol-newsArticle&highlight=1&ID=1615654>.
11. Ed McKenna, "Product Focus: Sensor Payloads," *Avionics Today*, 01 August 2012. At [http://www.aviationtoday.com/av/issue/cover/Product-Focus-Sensor-Payloads\\_76841.html#.UfGrztg98yY](http://www.aviationtoday.com/av/issue/cover/Product-Focus-Sensor-Payloads_76841.html#.UfGrztg98yY).
12. *AAI Receives \$70.7 Million Award for Shadow® Tactical Unmanned Aircraft System Laser Designator Kits*, 26 October 2010. At. <http://investor.textron.com/phoenix.zhtml?c=110047&p=irol-newsArticle&ID=1487182&highlight=1>.
13. Amy Butler and Graham Warwick, "Integrator Draws on ScanEagle Lessons," 23 August 2010, *The Fifth Column*. At <http://www.w54.biz/showthread.php?16-UAV-s-UCAV-s-and-other-such-matters/page44>.
14. Request for Information (RFI), Unmanned Aerial System (UAS) Electronic Warfare (EW) Capabilities, *Federal Business Opportunities*, 05 February 2013 at <https://www.fbo.gov/index?s=opportunity&mode=form&id=bed2728b806d600001f07e5983c7029e&tab=core&tabmode=list>.
15. Amy Butler, "Global Hawk Block 40 in Budget Crosshairs," *Aviation Week and Space Technology*, 19 February 2013. At [http://www.aviationweek.com/Article.aspx?id=/article-xml/awx\\_02\\_19\\_2013\\_p0-550454.xml](http://www.aviationweek.com/Article.aspx?id=/article-xml/awx_02_19_2013_p0-550454.xml).
16. Kate Brannen, "Army: Tremendous Demand for UAVs in Afghanistan," *sUAS News*, 17 December 2010. At <http://www.suasnews.com/2010/12/31/49/army-tremendous-demand-for-uavs-in-afghanistan/>.
17. Jeremiah Gertler, "U.S. Unmanned Aerial Systems," Congressional Research Service, 03 January 2012, 13. At <http://fpc.state.gov/documents/organization/180677.pdf>.

**2LT Matthew Polek is a former Hunter and Shadow UAV operator and a 2012 graduate of the MI Officer Basic Course. He received his BA from Washington State University, Pullman, Washington and is currently pursuing an MS in Emergency Management from Jacksonville State University, Jacksonville, Alabama. He is currently the Multi-Sensor Ground (MSG) Platoon Leader in B. Co, 4<sup>th</sup> BSTB, 4-10 MTN, Fort Polk, Louisiana.**

**I would like to personally thank CPT Gabe Justus. Without his mentorship and support I may not have been able to accomplish so many of my professional goals.**



## Fort Huachuca Museum

Check out the Fort Huachuca Museum website at  
<http://huachucamuseum.com>

# S2 Leadership: 10 Lessons Learned from a Combat BCT S2



by Major Thomas W. Spahr

The brigade combat team (BCT) S2 position is the most important and challenging job for Military Intelligence (MI) majors in the Army. My experience during three deployments in BCT level S2 shops, the final as the BCT S2 in the most active district in Afghanistan, led to this list of tenets that I found necessary for success as a BCT S2. The purpose of this article is to capture and share some of these guiding principles. While this article focuses on my experience specifically, it also includes my interactions with other BCT S2s while acting as the 82<sup>nd</sup> Airborne Division Deputy G2. While the Army's mission is always changing, many of these lessons translate to any type of fight. An underlying theme with all is that as the BCT S2 you have an enormous leadership responsibility. Being a good analyst will not ensure success; you must lead the intel effort in your BCT!

## 1. Build your team.

As a BCT S2 you will lead a group of talented junior officers, warrant officers (WOs), mid-level noncommissioned officers (NCOs), and civilians with a collective wealth of experience. The battalions (BN) S2s in your unit, while they don't directly work for the BCT S2, are also a part of your team and need your mentorship. Your challenge is to organize the members of this talent pool and motivate them to work as a team. This means defining a clear mission for your team, mentoring them in their positions, getting them to work collaboratively toward a common goal, and occasionally moving them into different jobs. During my time as a BCT S2, I had an officer team of ten captains, eleven lieutenants (LTs), and

six WOs (including the MI Company (MICO) and BN S2 shops), augmented by a strong team of NCOs.

Building your team may be the most important thing you do as a BCT S2. In order to succeed you must first get to know your team and help them to get to know each other. Your training cycle facilitates this effort by placing the intel leaders together for multiple exercises and professional development sessions. To further build these relationships I created battle rhythm events that forced the team to come together. In garrison we met weekly, but once deployed, the BCT S2 and BN S2s had scheduled touch points four days a week. The company intelligence support teams (CoISTs) were brought into the brigade intel sync meeting every other week (in addition to their almost daily syncs with their BN S2s). The meetings with the BN S2s occurred primarily over SVOIP and included a formal sync, an attack the network (ATN) working group, an Intel deep-dive with the BCT Commander, and a counter IED (C-IED) working group. During each of these working groups the BN S2s had a briefing role, or were asked to comment on the BCT S2's analysis.

Every other week in the formal BCT S2/BN S2 sync one BN's CoISTs would brief their situation template (SITEMP) and an update on the population in their sector (popular sentiment, key leaders, problem areas). Through these interactions along with regular phone conversations and occasional battlefield circulation, the BCT and BN S2s were able to get to know and understand each others' challenges and remain synchronized in their assessments.

In addition to these events I employed several deliberate team building techniques. In garrison, the entire BCT S2 shop did PT together every day. We did several out-of-office team builders as well, including going to the Rod and Gun Club on post to shoot personally owned weapons and having the BCT, MICO, and BN intelligence leadership to the BCT S2's house for a social. Prior to the deployment I presented all of my captains with a copy of John C. Maxwell's *The 17 Essential Qualities of a Team Player*, and talked to them directly about the challenges I anticipated we would face and the importance of open, frank communications and teamwork.

Team building doesn't stop once you are deployed and should, in fact, become easier. Clearly defining your mission is a critical step. After we arrived in theater and completed the relief-in-place I brought the entire BCT intel team together, as we had many additions once deployed, and outlined my understanding of our mission, our Commander's vision, and my vision for the intelligence team. I emphasized the importance of teamwork and constant, disciplined communications throughout the intel enterprise.

Finally, the BCT S2 leaders designed and purchased an intelligence enterprise chip that we gave to every S2 and CoIST Soldier across the BCT. When I was able to battlefield circulate with the BCT Commander I always made sure that those in the CoISTS had received their chip and if they had not, I presented them with one.

Positioning your leaders is another important part of building the intelligence team. During the ARFORGEN cycle we made at least four moves to reposition talent, including replacing BN S2s, and moving a very capable 2LT to the lead Intelligence Battle Captain's position on the Joint Operations Center floor. When I first became the BCT S2 I visited each of the subordinate BN Commanders to discuss how their S2s were performing. I let them know that I was the senior intelligence officer and if they had concerns that they should contact me. Building these relationships helped me anticipate problems and react. This process may be painful in the short term, but it proved absolutely necessary to getting the right people where they needed to be.

As the BCT S2, you can't do it all, and I learned early on that I had to instill a feeling of ownership for different focus areas. For example my S2X owned

the CoIST training program, and my electronic warfare officer led language training for the battalions and companies. You cannot be the sole presenter as the BCT S2, it is important to build briefing confidence in several analysts. A technique that I used was to brief a few large presentations early on to earn credibility and demonstrate to my team how I liked information presented, then I forced others to take the lead. Once we identified a few strong briefers, they took turns at the daily Commander's updates. As the S2, I always guided and reviewed the material, but they owned it.

## **2. Build the base of the pyramid—the CoIST.**

I regularly described the intelligence enterprise in a BCT as a pyramid, with the CoISTS at the wide bottom and the BCT S2 at the top. Intelligence in counterinsurgency (COIN) is largely bottom driven—derived from patrols, key leader engagements, tip lines, and company level assets to include raid cameras, biometrics, hand-held scanners, and Raven UAVs. As such we needed strong intelligence specialists at the lowest levels.

Training the CoISTS was the responsibility of the BCT S2 shop. The Brigade S2X worked with the BN S2s to track the CoISTS across the BCT and to manage the training. We primarily utilized the Mission Support Element's CoIST training course at Fort Bragg and the BCT MICO ran collections and targeting training. In addition we reached to outside organizations for some additional systems training and contracted a course specifically focused on helping our Soldiers learn to talk to Afghans, spot sources, and gather basic priority intelligence requirements (PIR). They were also taught when to pass off a developing source to a trained Human Intelligence (HUMINT) Soldier. The training was aimed at making every Soldier a sensor. While we initially used a contracted trainer, we quickly determined that our senior HUMINT NCOs and WOs could lead this course just as well.

We learned several important lessons in managing CoISTS. First and foremost, it is as important to train the company commander (CO) as it is his intel team. The CO in today's Army has more assets to leverage than a BN commander did 15 years ago. These include HUMINT Teams (HCTs), Signals Intelligence (SIGINT) (Wolfhounds, PRD-13s, hand held scanners), Geospatial Intelligence (GEOINT)

(raid cameras, aerostats, Raven or Puma UAVs), biometrics (BATS/HIIDES, SEEK systems), and the Tactical Ground Reporting System and/or DCGS-A analytical systems.

He needs a strong Intel support team, but he also needs to know what to ask for and how to support them. We trained our COs during the pre-deployment phase by running an intelligence, surveillance, and reconnaissance (ISR) orientation leader professional development (LPD) and getting the COs read on to some of the National-level SIGINT capabilities. During the rotation we shared tactics, techniques, and procedures (TTPs) and circulated Intelligence NCOs to the companies.

In retrospect, however, I wish we had focused more training on specifically leveraging a CoIST. We learned that while a five person CoIST was optimal, it was not always possible. Our companies were spread across the battlefield, and we sustained casualties during the deployment, forcing cuts in some places. We eventually modified the brigade standard to a two person CoIST with three more personnel trained. One technique was to train one CoIST member from each platoon and have them patrol with that platoon, but pull part-time duty in the company tactical operations center (TOC). This technique kept them in sync with the patrols, and also helped the platoon leaders who were often isolated from the company and had to do their own intelligence analysis.

Finally, retraining of CoIST members and sharing TTPs proved important during the rotation and is discussed later in this article.

### **3. Your commander is the best intel officer in the BCT.**

Learn how he thinks, advise him on capabilities, and let his instincts be your guide. He will typically have at least ten years more experience than you and has access to information that you do not because of his position. Recognize this, learn how to think like him, leverage his instincts, then present information to him in a way he understands. This is critical to your success.

Capturing what he learns through battlefield circulation is an art that is unique to each commander/S2 relationship. Some S2s achieve success by embedding recorders with the commander or having an intelligence analyst travel with him. However, I

found this was not always possible because of limited seats. Another technique is to have a battle rhythm intel deep-dive with the commander. In this forum, you can guide the conversation by what you present, and then glean what he learned and his vision is from his comments.

Unfortunately, personalities matter and there is no formula that ensures that the BCT Commander and his S2 will mesh. I have witnessed good intelligence officers fail because they could not get inside their commander's inner circle or did not get along well with their boss. Make this relationship a top priority.

### **4. Build the relationship with your MICO commander and STB chain of command.**

The BCT S2/MICO relationship and the BCT S2/Special Troops Battalion (STB) Commander relationship are vital to your success. The MICO commander owns much of your intelligence team, yet he is not in your rating chain. I have found that the key to success is to force communications and build personal relationships with the MICO and the STB commanders, and to make sure the MICO commander has a fighting role. Making the BCT S2 the intermediate rater for the MICO is a technique that likely helps, but the relationship is more important.

Breaking down the separation between the MICO and S2 early on is important. You can accomplish this by integrating your training meetings and getting out of the office and visiting the MICO's training. Draw clear lines on what intel training the MICO owns and the leaders in the BCT S2 shop own. We generally empowered the MICO to focus on training the collectors (LLVIs, HCTs, UAV teams), while the BCT S2 shop focused on synchronizing intelligence training for the all source analysts, the BN S2 shops, the CoISTS, and the non-intel MOSSs. Team build with the MICO. A simple technique is to have the specific intel function analysts (All Source, SIGINT, etc.) do PT together once or twice a week.

Additionally, I strongly encourage the BCT S2 to draft training guidance for the MICO, though this has to be vetted through the STB Commander. When drafting this guidance the BCT S2 should leverage the expertise that resides in his shop, specifically his single source WOs. If presented properly, most STB commanders will appreciate this input from the S2.

A challenge I experienced and regularly heard from other BCT S2s was incorporating the MICO into training and production with the S2 shop in garrison. A technique is to issue a BCT order to the STB to have a number of analysts dedicated to production in the S2 shop. Despite trying this, my BCT struggled with this challenge until approximately the last ten weeks of the ARFORGEN. Our combat training center (CTC) rotation was a terrific team builder for the BCT intel team, and we were able to maintain that momentum by immediately transitioning to a four week overwatch exercise facilitated by the Fort Bragg Foundry program. The MICO Commander and I worked closely to synchronize our calendars and publish an order over two months out in order to isolate our analysts for this event.

The overwatch included a weekly video teleconference with the S2 shop we were replacing in Afghanistan and culminated each Friday in a briefing delivered to the BCT and BN Commanders. These briefs stimulated so much conversation amongst the leadership that the BCT Commander ordered them to continue after the exercise ended, thus keeping us in a near-permanent state of overwatch until we deployed. This impetus forced what I had been working to solidify for months—the constant presence of the MICO analysts working side by side with the S2 analysts.

The MICO commander must find a fighting role once he is deployed. I have witnessed several MICO commanders train their troops for war, then take a back seat to the BCT S2 and do little more than worry about maintenance and administrative tasks once deployed. These are important, but the executive officer and first sergeant should be able to handle them with minimal command oversight. Before we deployed I asked my MICO Commander to compare himself to an Infantry CO who he was competing with for a top block OER. The Infantry commander fights his company and has regular face time with his BCT leadership. The MICO commander needs to do the same. In our case the MICO Commander led the ATN cell, but a more common role may be as the head of the collection management team. Where he or she fits is something the BCT S2, the MICO and STB Commanders can work out given the mission as long as the expertise of this senior intelligence captain is contributing to the fight.

Finally, the BCT S2's relationship with the STB commander is absolutely critical as he is the BN commander for so much of the intelligence enterprise. I carbon copied the STB commander on messages I sent to the entire Intel team and visited him regularly to seek his advice. I was fortunate to have an STB Commander who was an MI officer and he too found a fighting role that greatly benefitted the intel enterprise. He chaired the BCT ATN and C-IED Cells. He leveraged the MICO Commander to lead the ATN effort, and the BSB S2 to lead the C-IED working group. His presence and leadership ensured these working groups functioned efficiently. I kept an active role in both of these efforts, but having his leadership behind them enabled me to focus on the day-to-day fight, intel plans, and the COIN effort. The team effort we were able to develop proved essential to the success of the intelligence enterprise.

## ***5. Leverage the staff around you to produce the information you need.***

During our leader training program (LTP) for the National Training Center, our BCT Commander directed the staff to organize around lines of effort (LOEs) and assigned ownership of each of them to a staff lead. The S9 led the political LOE; the engineer led infrastructure; the advisory team led the Afghan National Security Forces, and the S2 led the ATN LOE. The S3 issued orders requiring subordinate units to report information in a standardized format that made it easier for each staff lead to gather the information they needed. Once the LOEs were clearly defined, we oriented our PIR around them, focusing on the major questions that each needed answered. Since we were fighting a COIN effort, our number one PIR was political, oriented on identifying the key leaders in each subdistrict who could influence the people to stand up to the Taliban. Not all LOEs were equal, and not all had a PIR assigned, but PIR were focused on the Commander's priority for decision points within each LOE.

For the S2, the greatest advantage of organizing the staff this way was that it forced ownership for different parts of the operational environment, and enabled the intelligence team to benefit from the other staff elements' analysis, but focus its efforts on the enemy. This did not exclude the S2 from having a part of each of the other LOEs. For example, the GEOINT team worked closely with the engineers

and leveraged GMTI to identify the most important routes and to graphically represent the infrastructure challenges. SIGINT, HUMINT, and Fusion all supported the political effort by collecting and sharing information on who we perceived were the key leaders and who they were loyal to. Fusion helped the LOE leads produce a SITEMP that graphically displayed their analysis.

This worked well in a COIN environment and is largely transferable to a conventional fight. Prior to the COIN-dominated missions of the last twelve years, the Army commonly paid lip service to the concept of reverse battlefield operating system analysis (the Air Defense Artillery (ADA) officer supports the analysis of the enemy ADA, the Signal officer helps understand the enemy communications architecture, the Engineers the enemy engineer effort), but rarely have I seen this concept well executed. Convincing your command team of the importance of having the entire staff understand the operational environment, and splitting responsibility for becoming experts on its separate parts is a concept that will benefit a unit involved in any type of warfare.

## ***6. Master and monitor multiple methods of disseminating information.***

The BCT S2 must understand the capabilities of not only your intelligence systems, but of the communications systems that you can leverage to disseminate information. Don't be afraid to use the FM net, or the TACSAT to put out an oral intsum, especially when the environment is fluid. Oftentimes the Blue Force Tracker (BFT) is the best way to disseminate information to the lowest echelons of the BCT. This might be a challenge on often overused nets, but it is important and will likely stimulate feedback from lower echelons if you are missing a piece of the puzzle. The BCT S2 needs to spot check that his collection manager (CM) understands the PACE plan (Primary, Alternate, Contingent, and Emergency) for all of his assets and that the back-up communications are reliable and have been rehearsed.

Be creative with how you disseminate and build redundant methods of dissemination. I found one of the most effective ways to publish emerging TTPs was in a weekly or bi-monthly CoIST/C-IED bulletin that we sent to all intelligence personnel and leaders down to the company First Sergeants. This four

to five page graphic-intensive product stimulated significant feedback and comments.

Finally, intel leaders in the S2 shop need to spot check that relevant information is getting to the people that need it. I made a habit of spot checking the BFT when we discovered an IED with an overhead asset. You would be surprised that sometimes it would not be posted in this most obvious of places. Whenever I was able to circulate the battlefield I always came armed with a list of recent products the BCT or BN shop had produced that were relevant to that company's region. At the same time, I always had many questions for the CoISTS who always knew their area better than my analysts at the BCT, then backbriefed my team when I returned to the headquarters.

Dissemination methods are absolutely critical to keeping a BCT intelligence enterprise functioning collaboratively and efficiently. Make the S6 your best friend, and treat his team with the utmost respect because they are your lifeline.

## ***7. Leverage the National level intel enterprise.***

The U.S. has developed a robust National intelligence architecture and the U.S. Army Intelligence and Security Command (INSCOM) has invested significant personnel and resources to provide access to these agencies. The National agencies and INSCOM want to support you, but you must understand what they do, how they deliver their support, and how to ask for help.

The first step is educating yourself on what the National agencies can bring to your fight and how to reach out to them. In my case, serving a year at INSCOM taught me its capabilities and how to leverage them. It introduced me to critical organizations like the DA Intelligence Information Services, the 704<sup>th</sup> MI Brigade, the Army GEOINT Battalion, and all of the National Ground Intelligence Center's (NGIC) resources.

The ARFORGEN helped the BCT S2 shop learn about these capabilities through the CTC and the Senior Leader ISR (SLISR) trip to the Washington D.C. region. Throughout my preparation and deployment I kept a collection of business cards and built a point of contact list that I regularly referenced. Many of the National agencies produce relevant products and disseminate them by posting

to a web portal, or pushing them through systems organic to the BCT. Make your intelligence analysts build a list of key websites and disseminate it by email, posting it to your portal, and printing it and posting it in the S2 area. Update this regularly.

Second, as the BCT S2, you must master the vast array of capabilities your shop is supposed to have through its organic equipment and then force your team to keep these systems functioning. For example, understanding all of the capabilities that the DE-CGS (now the Tactical Ground Station) and the Global Broadcast System were important to pulling more than just National imagery and the news.

One of your most important leadership tasks as the BCT S2 is to ensure your subordinates, including your BN S2s and CoISTs, understand what resources are available to them. To educate the CoIST, the MICO led classes on the BCT's organic intel collection systems. Training on National level intelligence capabilities was more challenging. We accomplished this through several methods. First, we began several of our weekly synch meetings with a capabilities brief from one of the different agency LNOs. We closely managed the SLISR trip to best leverage what was relevant to us and what we were already familiar with. Finally, we organized regular intelligence LPDs for S2s and occasionally expanded to all leaders across the BCT. We also rotated our intelligence leaders for week-long visits to several critical national agencies. For our mission these included the C-IED Operations/Intelligence Integration Center (COIC) and NGIC COIN targeting program (CITP). The S2 must reach out to the different national agencies, bring the LNOs in to educate your team (especially in the current fiscally-constrained environment), and then hold these LNOs accountable if they are not meeting your standard.

Another program the BCT S2 can leverage is your Commander's LPD program. This knowledge enables the battalion and company level leaders to ask for the capabilities they need, and at the same time helps them understand the limitations of the intelligence enterprise and manages their expectations. The BCT Collection Manager led one LPD on the capabilities of relevant collection platforms, and our SIGINT lead led another in the Sensitive Compartmented Information Facility (SCIF) on SIGINT-specific capabilities. Because our company commanders were controlling large regions and employing a wide array of intelligence assets, we felt

justified requesting TS clearances for all of them.

The final and most important pre-deployment LPD 4/82 held was a two-day "shura" during which we attempted to bring together representatives from all the entities that would be supporting the brigade in theater or through reach back. This included U.S. Agency for International Development representatives, a National Security Agency (NSA) representative, and multiple Special Operations Forces representatives. This forum helped educate the BCT leadership on different capabilities, and gave our BCT Commander an opportunity to orient our support infrastructure on his priorities.

## **8. Conduct training and TTP sharing constantly.**

No matter how perfect you feel your training was, your team will continue to learn and refine their techniques once deployed or in a certifying training exercise. Additional enablers will also become available or evident to you. Prioritizing training while deployed is difficult, but necessary to continuing to develop your team. Sharing TTPs is not as difficult, but must be scheduled on the battle rhythm to ensure that it happens.

I have observed several techniques for sharing lessons learned during a deployment. During my unit's intelligence synchs, we had one BN's CoISTs (approximately five teams) brief their situation and then conclude with one lesson or TTP they had learned. About half way through our deployment we began publishing a weekly or bi-monthly CoIST/C-IED bulletin. This four to five page, graphic-intensive document commonly included pictures of emerging threat TTPs, friendly techniques in the C-IED fight, vignettes highlighting a positive action or a negative incident, an example of an effective product that a CoIST or BN S2 shop produced, and an emphasis message from the Commander. For example, we struggled to get the CoISTs to regularly complete collection plans to synchronize all of the assets that the companies had to leverage. When we found one team that was performing this task well, we published a copy of their daily collection sync matrix for others to mimic.

Finally, retraining CoIST members and augmenting them was critical. Several of the BN S2s pushed 35F intelligence analysts or MI lieutenants to the companies or platoons in the hottest regions. From the BCT, we constantly rotated four intelligence an-

alysts to companies for two weeks to a month at a time. We also leveraged the talent at our higher headquarters, in this case a division acting as a joint task force (JTF). We had two E-6s from the Division, who had experience as BN level analysts, rotate to the companies and spend a week mentoring the CoISTs and advising the COs. Rotating analysts this way also increased the communications flow because it built personal relationships up and down the echelons. My S2X debriefed the analysts who returned from a CoIST and kept a contact list of all of the CoIST members. This feedback combined with the varying threat in the different regions helped us target where we needed to surge intel analysts to CoISTs.

Throughout the deployment we continued to leverage our National level augmentation to train the Intel team on emerging capabilities, or to remind them of what they can ask for. To accomplish this, I had a different LNO (NGA, COIC, NGIC CITP, NSA CST, ORSA) brief their specific capability during our intel synchs. I also tried to rotate our BCT augmentation and JTF specialty assets to the BNs for short periods of time to demonstrate their capability first hand.

## **9. Build redundant methods to force fusion.**

Intel professionals give consistent lip service to the fusion of information, but what I have found is that 35 series Soldiers are oftentimes introverts and that sharing and collaboration does not happen naturally. Building an environment that facilitates fusion and creating battle rhythm events to force fusion proved important to ensuring the correct information became intelligence and was delivered to the Commanders. The first thing we did to ensure sharing was to position analysts near each other. Proximity encourages cooperation. Second, each of the specific intelligence functions and subordinate BNs published daily intelligence summaries (INTSUM). This process forced them to review all of their reporting and gave the leadership an easy and redundant method to read the recent information. As a leader, I found it was important to read and comment on as many of these reports as possible, and to encourage my intel function leads to do the same. As the BCT S2 I did not have time to read every INTSUM, but I did skim through many of them and always tried to comment when something rele-

vant caught my eye, when one was particularly well done, or when I noticed the quality lacking. Letting all of your team members know that you value their work ensures quality over a long deployment.

Finally, and in my case most importantly, we held a daily BCT intel sync meeting. This meeting helped me get through all of the information efficiently and focus the analysts on what was most important for the commander's daily update. My S2X also ran a daily intelligence sync with the Afghan army, police, and investigative service and brought back what he learned to this forum. I recommend keeping this type of engagement simple and verbal around a map with each intel function briefing what they have seen that day. I held the team members accountable by making spot corrections if they came unprepared, but at the same time tried to limit the time it took them to prepare by not using slides. The fusion analysts would then take the most relevant intelligence and turn it into slides to present in the daily battle update brief which occurred a few hours later. While all of the same information was published in the SIGSUM, HUMSUM, and GRINTSUM, sitting around a table and verbally going through the highlights ensured the separate intel functions were communicating and facilitated discussion and analysis. On multiple occasions we would make links and I could walk out of this meeting with intelligence that required action. Almost daily, this meeting laid the foundation for a relevant intel update to the BCT Commander.

## **10. Be a good staff team player.**

I always counsel my subordinates that 50 percent of being successful in the Army is being a likable person able to work well with others. This is not to say that I did not have disagreements with my peers, but we did not allow these disagreements to prevent long-term cooperation. The S2/S3 relationship is key, and the S2 has to work to develop it. I always attempted to sit next to the S3 or one of his key subordinates. During NTC I sat next to the chief of operations (a major), and during the deployment I shared an office with the BCT S3. We both quickly learned the value of overhearing the information that was flowing across the other's desk. Any time I deemed it necessary to walk into the Commander's office with hot information I always told the S3 first and he usually accompanied me. This helped ensure that we were both prepared to follow up with

how we were addressing a situation or present a recommended action.

The tie-in with the S3 is important at all levels. During our training and deployment, my AS2s became masters of drafting orders and moving them through the S3 and into the daily BCT order. I initially reviewed all of these, but once the process became fluid, I trusted my AS2 to release them to the S3. This process formalized the intelligence training priorities and put them on the Operations calendar. It also helped protect the intelligence training because it had the Commander's name on it. Once deployed we published orders mandating that the subordinate units report priority information in a standard format that we could easily ingest into the LOE SITEMPs. The subordinate units disliked having to produce through a BCT-driven format, and we compromised in places to make the process efficient, but in the end they appreciated the value of having their analysis reflected in the higher echelon's products.

Synchronizing the Collection Manager between the S2 and S3 was another success story that we had to work through. I counseled my CM early on that she needed to flow between the S2 and S3 since she was tasking assets that belonged to the BCT Commander. We fought for a place in the daily Ops synch meeting for the Collection plan and we published the collection plan as a part of the daily order. This process ensured the collections assets remained synchronized with daily operations.

## **And Finally...**

This final point I encourage BCT S2s to take to heart is the importance of getting out of the TOC and seeing the actors in the intelligence enterprise. You'll be amazed at what you will learn and be able to fix as a result. Force your team members to get out and see the fight as well so they appreciate the challenges of their subordinate units. Commanders do battlefield circulation because of what they learn and to exert their influence across the unit; the BCT S2 is the leader of an expansive intel enterprise and needs to do the same. A strong AS2 should be able to run the brigade shop temporarily, so the BCT S2 can lead the brigade intelligence enterprise. 

## **Endnotes**

1. In addition to what the NTC cadre taught us, our BCT leadership learned about this method from the Z. Tenay Guvendiren and Scott Downey "Putting the Priority Back into PIR: PIR Development in a COIN Environment," This article describes how the 2<sup>nd</sup> BCT, 1<sup>st</sup> Cavalry Regiment organized itself during Operation Iraqi Freedom, 06-08.

## **References**

- Flynn, Michael T., MG, U.S. Army, CPT Matt Pottinger, USMC, and Paul D. Batchelor, "Fixing Intel, A Blueprint for Making Intelligence Relevant in Afghanistan," Voices from the Field, Center for New American Security, January 2010.
- Flynn, Michael, LTG, US Army, and BG Charles A. Flynn, "Integrating Intelligence and information: Ten Points for the Commander," Military Review, January-February, 2012. 4-8.
- Guvendiran, Z. Tenay and Scott Downey, "Putting the PRIORITY Back into PIR: PIR Development in a COIN Environment," Small Wars Journal, 12 April 2009. At [www.smallwarsjournal.com](http://www.smallwarsjournal.com).
- Moore, Gregory, CPT, U.S. Army, "Ten Principles of Intelligence on the Battlefield," The Military Intelligence Professional Bulletin, Vol 33, Number 1, (January-March, 2007). 22-29.
- Violand, David E., MAJ, U.S. Army, "Recommendations for the BCT Staff-The Intelligence Warfighting Function," NTC Ops Group-Bronco Team, 18 Feb, 2013.

*I would like to thank my fellow MI field grade officers in the 82<sup>nd</sup> Airborne Division for their help with this article. Second, I thank the Task Force Fury team, especially the intel leaders, our Deputy Commander, LTC Scott Halstead, and my fellow Majors for the team work and camaraderie during this very difficult deployment. Finally, I thank COL Brian Mennes, Fury 6, for his mentorship and for making Intelligence a priority in Task Force Fury.*

*MAJ Thomas W. Spahr is currently serving as speechwriter for the Vice Chief of Staff of the Army. He served as a BCT S2 4<sup>th</sup> BCT, 82<sup>nd</sup> Airborne Division, in the Zharay and Maiwand Districts, Kandahar Province, Afghanistan during 2012. He also served as an MI Detachment Commander, 7<sup>th</sup> Special Forces Group; Battalion S2, 1st Battalion, 7<sup>th</sup> Special Forces Group, and Collection Manager in the 75<sup>th</sup> Ranger Regiment. He has a PhD in History from The Ohio State University and taught Military History at West Point.*

# *OSINT: Truths and Misconceptions*

by Lieutenant Colonel Craig D. Morrow

## **Introduction**

It has been seven years since the publication of the Military Intelligence Professional Bulletin's issue dedicated to Open Source Intelligence (OSINT). Since 2005 most contemporary intelligence professionals have come to acknowledge the value of OSINT and its virtues are now widely understood. OSINT facilitates information sharing with partner nations, and with governmental and tribal entities below the federal level as well as nongovernmental organizations. It is also timelier than other intelligence disciplines. Like it or not, global news organizations (e.g., CNN) can get to a person "on the ground" at any distant trouble spot more quickly than the Intelligence Community (IC). OSINT is also much less costly (in terms of risk as well as dollars) than almost any other intelligence discipline.

Unfortunately, many misconceptions about the application of OSINT continue to endure throughout the community. These misconceptions, such as the notion that a "Google™ search" equals OSINT, serve to impede a wider implementation of a comprehensive OSINT program across all elements of the IC. I will discuss six common "myths" about OSINT in an effort to provide a more complete picture of what it is, and what it is not.

♦ **Myth One: OSINT is less credible than other intelligence disciplines.** Across the IC, the broad acceptance of OSINT as a primary source has been hampered by the idea that it is inferior to, or lacks the veracity of, classified information. This belief appears to be rooted in the idea that intelligence gathered by other means is derived from

more candid sources. If our adversary is hiding the information from us then it must be genuine; anything we can obtain freely must be less valid.

This logic, while valid on its face, fails when we consider that our adversary is not communicating (or obscuring communication) with a single audience. A simple analogy may help to clarify: If you wanted to know the size of the garage I built (out of sight) in my backyard, I may be reluctant to tell you and I may even take steps to prevent you from determining this information. I may boast to another neighbor about my nice new 500 square foot garage, and you may believe you have obtained the information I attempted to hide from you. However, when I place an advertisement in the newspaper asking for a painter to paint a 400 square foot structure, I have a vested interest in ensuring this information is accurate.

In this story the information obtained surreptitiously is flawed and the information openly available in the newspaper is significantly more accurate. When information is communicated in various unclassified fora, in many cases all parties involved have a clear interest in ensuring that the information communicated is complete and correct—even if this is information that they may not want an outside party to know.

Is OSINT always better than information from other intelligence disciplines? Of course not, but it may be. Any information can be flawed or even false, regardless of how it is obtained. It is worth emphasizing, however, that OSINT can not only be

as good as other information; in many cases **OSINT can provide better information than that from other intelligence disciplines.**

♦ **Myth Two: Intelligence requests require classified information.** Related to the idea that OSINT is inherently inferior to other intelligence disciplines is the belief that any intelligence requirement can (or should) be answered exclusively with classified information. Simple mathematics quickly refutes this notion. What is perhaps the largest database in the world belongs to AT&T. This database contains more than 323 terabytes (323,000 Gigabytes [GB]) of information—including more than 1.9 trillion phone call records.<sup>1</sup> Although the total amount of classified data in existence is hard to estimate, if we assume that each of the 17 members of the IC—from the Drug Enforcement Agency to the National Security Agency—each possessed a data base as large as the largest known database (AT&T), we would have a combined repository of less than 5.5 petabytes (5.5 million GB).<sup>2</sup> This would be an immense amount of data, and the answers to many intelligence requirements would undoubtedly be contained within.

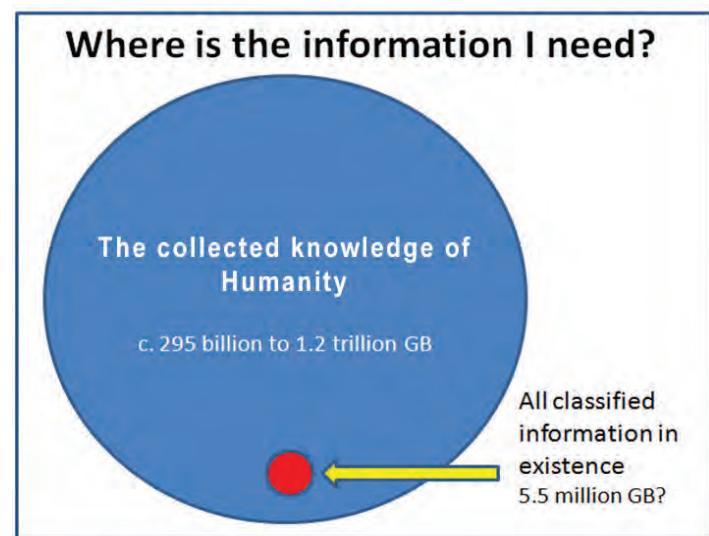
Although the exact quantity of classified information in existence cannot be known, it is very certainly quite large, but at the same time it is equally certain that this classified information represents but a minuscule fraction of the total information available to answer intelligence requirements. It has been estimated that humanity—all 6 billion of us—has a total collective store of information that amounts to 1,200 petabytes (1.2 billion GB) of information.<sup>3</sup> Beyond the information that we carry in our heads, a modest estimate of the collective wisdom of humankind stored for posterity is 295 exabytes (295 billion GB).<sup>4</sup> Another estimate puts the total amount of information in existence in 2010 at 1.2 zettabytes (1.2 trillion GB).<sup>5</sup>

By any measure, the total sum of human knowledge is enormous, and the vast majority of this is unclassified information. These numbers continue to grow increasingly larger every year; however, it is folly to believe that the quality of classified information—no matter how large or in what form—will ever be but a trivial portion of all information.

**An over-reliance on classified information is poor practice and results in poor analysis.**

Relying exclusively on classified information ignores the vast majority of information available to the an-

alyst. It requires a blend of intelligence hubris and mathematical ignorance to believe that “the answer” always (perhaps even usually) lies in the classified realm.



♦ **Myth Three: Every analyst can “do” OSINT.** Every analyst across the IC is very likely capable of performing a search of the Internet; in many cases they are capable of performing rather sophisticated searches. Nonetheless, this does not qualify them as OSINT analysts. While it is true that any analyst can perform many of the functions of skilled OSINT analysts, it is also true that both a fireman and a cardiac surgeon can perform cardio-pulmonary resuscitation. Although both are skilled experts, I would recommend discretion in selecting one or the other to perform a heart transplant.

It does not take a great deal of time or other resources to create an effective OSINT specialist, but it does require some investment by the organization to grow these skilled specialists. There are a number of schools available that will provide the novice OSINT specialist with critical tools to increase the efficiency and effectiveness of their work. However, beyond the formal training, much of the actual trade-craft is derived from on-the-job experience. The neophyte doing an Internet search may or may not find an answer to the requirement; an OSINT expert is more likely to find an answer, and that answer is likely to be more comprehensive.

While the neophyte will do an Internet search, the expert will do multiple searches. The skilled OSINT professional understands that the “answer” is unlikely to be found, even using a sophisticated search. The truth is that the initial search will most

often provide a clue that leads to a subsequent clue. Each clue refines the search and informs the researcher. The “answer” typically does not exist on a single, readily-accessible webpage; it is the compilation of multiple pieces of information that build upon each other to lead the OSINT expert to a fuller understanding of the reality being sought.

Finally, OSINT specialists should be analysts who are already familiar with the area in which they will be focused. Implicit in this is the idea that most organizations would be better served by OSINT “specialists” than OSINT “generalists.” For example, regional OSINT specialists should have linguistic fluency and cultural familiarity related to the region on which they are focused. One obvious advantage is that they will be able to make use of native-language materials. A perhaps less apparent, but potentially more important, aspect of regional expertise is the ability of these analysts to identify potential sources of information deriving from the culture and perhaps unique to the region. Most intelligence professionals can perform basic OSINT tasks but ***an experienced OSINT specialist can provide substantially greater benefit to the organization.***

◆ **Myth Four: OSINT = Google™.** The Internet is a vast repository of information from around the globe, and it is indeed a critical part of any comprehensive OSINT program. A search for the letter “e” returns more than 25 billion pages, suggesting that even that portion of the Internet using the Roman alphabet contains a massive amount of information. This incredible resource will provide analysts with a lifetime of content through which they could sift. However, the content of the worldwide web is substantially larger than most web surfers will ever know—perhaps orders of magnitude larger.<sup>6</sup>

All Internet search engines have algorithms that help present their customer with what they believe is the most relevant information. Unfortunately, this results in the failure to index many pages in a way that will facilitate access through any search engine. Although there are limitations on exploring the totality of the web, understanding the capabilities and limitations of multiple search engines allows the OSINT expert to more fully exploit the content of the worldwide web than the average analyst.

The Internet is indeed an incredible resource; however, OSINT encompasses much more than this. Nonetheless, many of us continue to associ-

ate OSINT with the worldwide web. ***Broadcast and print media, public (governmental) data, academia, and numerous other areas offer a wide spectrum of sources for OSINT.***

◆ **Myth Five: OSINT is free.** The term “Open Source” is used in the computer programming community to refer to code that is not subject to licensing fees or royalties—it is free. A similar belief has permeated the IC. Unfortunately “Open Source” in our community does not always mean free, or even low cost. While an enormous amount of useful information can indeed be obtained at little additional cost to the organization, there are extraordinary opportunities to acquire information from a variety of sources for what are indeed relatively modest fees.

Unfortunately the idea that OSINT is (or should be) “free,” especially when combined with the idea that “classified is best,” can create situations in which decision makers in the IC may choose not to spend several thousand dollars to purchase information in favor of spending multiple times this amount to fund the collection of the information through more “traditional” intelligence means.

We continue to develop intelligence leaders who are trained to use the more traditional intelligence disciplines, with OSINT being marginalized or entirely excluded from the discussion. Unsurprisingly, for these leaders who have been trained to use a “hammer” over the course of their careers, every intelligence requirement will begin to look like a nail.

In addition to overcoming a “conventional” mindset among decision makers, funding OSINT can also present challenges. Our organizations have long-established mechanisms for funding a wide variety of collection methods, but lack an established means of providing adequate funding for *ad hoc* OSINT requirements/opportunities. This can create a system that makes it less bureaucratically complex to commit many tens of thousands of dollars to move Americans around the globe—and expose them to significant risk—to satisfy intelligence requirements than to spend a few thousand dollars for an extant publication that would satisfy the same requirement. ***OSINT is not always free, but it is typically the least costly option.***

◆ **Myth Six: OSINT is “easy.”** As already stated most people can perform rudimentary OSINT functions, although the results will typically be less

valuable than those derived from a trained OSINT specialist. In this respect OSINT may be easy, but you will get out of it what you put into it. More importantly, there are certain hazards associated with the OSINT field, and an uninformed neophyte could potentially jeopardize friendly operations as a result of poorly performed OSINT research. As Michael Taylor has previously pointed out, OSINT can provide indicators of U.S. plans and operations. A savvy adversary may be able to conclude U.S. intentions from the purchasing of certain documents, performing specific web searches, or asking questions at public events.<sup>7</sup> Given the increased potential to betray U.S. intention through OSINT operations, it is essential to ensure that OSINT specialists are cognizant of the hazards of this discipline.

Within the category of Internet searches, there are numerous means of betraying U.S. intentions and even revealing classified U.S. information as a result of poor practices within the discipline. Even some of the tools and technologies that appear to offer some degree of identity obfuscation to the Internet user have shortcomings that need to be thoroughly understood by the OSINT practitioner.

Can anyone perform as an OSINT analyst? Yes, but anything that can be done, can be done poorly. To perform most effectively in an OSINT capacity the analyst requires specialized training and immersion in the discipline. Likewise, to safeguard friendly information and intentions **the OSINT function should be executed by properly trained specialists.**

## Conclusion

The irony of OSINT is apparent in the fact that it was only recently recognized as a distinct “intelligence discipline,” despite being perhaps the oldest of all intelligence disciplines. This apparent inconsistency is linked to the belief that something rare (e.g., information not publically available) is inherently valuable (or “better”). This belief perpetuates this myth of an inherent supremacy of classified information. The effect of this mindset has been to keep OSINT from taking a more central place in the IC. Historically being marginalized, it has remained under resourced and under respected. Because everyone engages in “OSINT” on the personal level—whether it be reading a newspaper or a web log—we develop the notion that everyone can do OSINT at the professional level. The truth is that OSINT can not only be as valuable as the other disciplines, it

can be more valuable. However, to fully leverage the capabilities of this intelligence discipline it must be more fully resourced and we must focus on developing our first generation of true OSINT specialists. 

## Endnotes

1. Compare Business Products, “*Top 10 Largest Databases in the World*,” at <http://www.comparebusinessproducts.com/fyi/10-largest-databases-in-the-world>. Accessed 18 August 2012.
2. “Our Strength Lies in Who We Are” at <http://www.intelligence.gov/about-the-intelligence-community/member-agencies/>. Accessed 18 August 2012. This site lists the following as members of the IC as: the Central Intelligence Agency; Department of Energy; Office of Intelligence and Counterintelligence; Department of Homeland Security, Intelligence and Analysis; Department of State, Intelligence and Research; Department of Treasury, Office of Intelligence and Analysis; Defense Intelligence Agency; Drug Enforcement Administration; Federal Bureau of Investigation; National Geospatial Intelligence Agency; National Reconnaissance Office; National Security Agency; Office of the Director of National Intelligence; U.S. Air Force, Intelligence, Surveillance and Reconnaissance; U.S. Army, Military Intelligence; U.S. Coast Guard, Coast Guard Intelligence; U.S. Marine Corps, Marine Corps Intelligence Activity; U.S. Navy, Office of Naval Intelligence.
3. T. K. Landauer, “How much do People Remember? Some Estimates of the Quantity of Learned Information in Long-term Memory,” *Cognitive Science*, 10 (4): 477-493.
4. Jon Stewart, “*Global Data Storage Calculated at 295 Exabytes*,” at <http://www.bbc.co.uk/news/technology-12419672>. Accessed 18 August 2012.
5. “All Too Much: Monstrous Amounts of Data,” *The Economist*, 25 February 2010 at <http://www.economist.com/node/15557421> accessed 18 Aug 2012.
6. Michael K. Bergman, “The Deep Web: Surfacing Hidden Value,” *The Journal of Electronic Publishing* 7(1), August 2001, 1-17.
7. Michael C. Taylor, “Open Source Intelligence Doctrine,” *Military Intelligence Professional Bulletin*, October 2005, 12-14.

***The views expressed by the author do not reflect the official policy or position of the departments of the Army and Defense, or the U.S. Government.***

Lieutenant Colonel Craig Morrow is currently assigned as the Program Director for the General Psychology for Leaders program at the U.S. Military Academy (USMA). His previous assignment was as the Deputy J2 for the Combined Forces Special Operations Component Command-Afghanistan. Before his assignment to the U.S. Special Operations Command he was the Chief of the Open Source Intelligence Division at the U.S. European Command Joint Analysis Center. He holds a PhD in Psychology from Penn State, a Master's degree in Strategic Intelligence from the National Intelligence University and a BS in Military History from USMA.



# The Targeting-ISR Relationship

by Major Jeffrey Fair

## Competing for ISR

The requirements for collection come from multiple sources, but all are related to the Joint Commander's priorities. Two of the primary functions that generate collection requirements are intelligence and targeting. The J2 prepares a list of priority intelligence requirements (PIRs) for the commander. A PIR is defined "as an intelligence requirement, stated as a priority for intelligence support that the commander and staff need to understand the adversary or other aspects of the operational environment."<sup>2</sup> PIRs drive the allocation of ISR assets because these key questions are the intelligence needs identified by the commander. There are other intelligence requirements (IR) that the J2 uses to task collection, but PIRs provide focus to collection activities because of their origin and importance.

PIR will have significant overlap with the needs of the theater targeting effort because of the similarities in information needs. While PIR drives collectors to obtain answers to questions that the commander needs, targeting efforts drive collectors to locate targets for commander-directed operations and assess post-strike disposition. If, for example, the commander wants to know what route a second-echelon enemy unit will take because it drives an identified decision point and becomes a PIR, targeting personnel will require that information in order to successfully target that unit. Much of this overlap is not coordinated; it occurs because the targeting sections are following the same commander's guidance that the PIR do.

During peacetime, however, ISR is used to provide indications and warnings (I&W). JP 1-02 defines I&W as "those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the U.S. or allied and/or coalition military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of hostile actions or intentions against the U.S., its activities, overseas forces, or allied and/or coalition nations."<sup>3</sup>

## Introduction

Successful targeting efforts are enabled by quality intelligence derived from a robust and well-managed collection plan. The ability for a headquarters to target enemy elements or individuals can only be done if that same headquarters has the intelligence, surveillance, and reconnaissance (ISR) support it needs in order to identify, locate, and track desired targets. Synchronization of the ISR plan and the targeting plan is essential if a unit is to be successful in accomplishing the Commander's desired effects on the battlefield. On a joint staff, synchronization of both efforts takes place through the execution of the cross-functional organizations built into the staff's organization and battle rhythm. The challenge for planners is to satisfy all of the competing needs for ISR from the joint staff and from subordinate commanders.

JP 1-02, DoD Dictionary of Military and Associated Terms, defines ISR as "an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function."<sup>1</sup> ISR crosses the boundaries between operations and intelligence not only because of the dual nature of intelligence collection, but also because of the source of the requirements levied against it. Collection operations are missions conducted with the aim of gaining information that can be used to generate intelligence on a certain topic. The missions conducted have an operational component because they are actions on the battlefield, planned and executed by operators. The operators, to a large extent, are intelligence professionals who have direct ties to the larger joint or interagency intelligence enterprise.

Again, there is some overlap between I&W and targeting needs, but these activities are normally not formally coordinated as well. I&W drive ISR to focus on certain locations or weapons systems, the key enemy systems that would signal a heightened state of war readiness. Targeting requires updates on all of the locations, units, and equipment that are programmed to be attacked, especially in the first days of a conflict.

At the joint unified command or sub-unified command level, targeting may not be the sole domain of intelligence professionals. In fact, it is common to have targeting personnel in both the operations and intelligence branches of a staff at the joint command and component command levels. It is imperative for theater targeting organizations to remain connected and integrated with intelligence organizations because not all targeting ISR needs will be met by other intelligence functions. There are multiple ways to synchronize ISR with targeting, but the two main areas for integration are deliberate targeting and dynamic targeting.

## **Deliberate Targeting**

A joint staff must constantly work to coordinate and synchronize efforts of the staff and the assigned components. JP 3-33, Joint Task Force Headquarters, states: "The most common technique for promoting this cross-functional collaboration is the formation of an appropriate organizational structure to manage specific processes and accomplish tasks in support of mission accomplishment."<sup>4</sup> This organizational effort includes the formation of boards, cells, and working groups to integrate and synchronize across the staff. This includes the effort to coordinate the targeting and ISR activities.

ISR has two key meetings in the cross-functional architecture, the Joint Collection Working Group (JCWG) and the Joint Collection Management Board (JCMB). The JCWG is where action officer level discussions about the use and employment of ISR assets take place in preparation for a decision, many times by the J2, as the chairman of the JCMB. The results of the JCMB are displayed at the Joint Targeting Coordination Board (JTCB) to demonstrate that the ISR plan supports the targeting effort. The chair of the JTCB is generally the J3 or his representative, who ensures that targeting is synchronized with not only ISR, but also accounts for the projected enemy situation and the component maneuver plans.

In order to communicate targeting needs in the planning process, targeting representatives must attend the JCWG to get requirements to collection managers early in the process. A constant dialogue outside of the formal meetings is even more helpful, allowing both parties to eventually anticipate the needs of the other. Targeting requirements are first outlined in the Targeting Working Group (TWG) where components and joint staff receive guidance for the air tasking order (ATO) day being planned. Air operations and joint fires are planned in 24-hour cycles that are detailed in the ATO. After receiving commanders' guidance, targeteers determine what they must strike during that ATO in order to meet the desired effects sought by their component commander and the joint force commander.

The needs developed in the TWG are then brought to the ISR planners. This can be done formally, at the JCWG, or informally through regular cross-staff coordination or request for support from components. The planners at the JCWG work to ensure the targeting needs are met during the ATO being planned. This includes pre-strike collection and post-strike battle damage assessment collection. Once the JCWG has the requirements, the planners prepare to brief the J2 at the JCMB for approval of the collection plan for that ATO.

There can also be several additional meetings in a joint staff's battle rhythm that assist in targeting-ISR coordination to include synchronization meetings that bring analysts into the discussion. In a bilateral or coalition environment, it is common to hold a combined JCMB in addition to a U.S.-only event. Targeting officers from the coalition nations should attend the combined JCMB with their U.S. counterparts to ensure synchronization between all parties and efficient use of all coalition assets.

During the deliberate targeting planning process, the cross-functional collaboration meetings on the staff serve the purpose of getting all of the right people together in one location to ensure mission accomplishment. The key to making the meetings successful is cooperation outside of the working group and board process to ensure the detailed planning is accomplished in both the ISR and targeting arenas. Building relationships will facilitate close cooperation between ISR and targeting, and will also enable other key intelligence organizations such as analysts and national intelligence agency liaison officers to contribute to both efforts.

## **Dynamic Targeting**

Once the chair of the JTBC approves the targeting plan, it is handed over to operators for execution at the component level. On the joint staff, operations officers monitor the components' execution of the plan and attempt to anticipate when and where changes may occur. Dynamic targets can emerge from changes to the approved plan or from targets that are identified after the JTBC meets. The dynamic targeting process is described in JP 3-60, Joint Targeting, as "targeting that prosecutes targets identified too late, or not selected for action in time to be included in deliberate targeting."<sup>5</sup> Targets routinely fall into this category because the enemy is determined to achieve their desired results and will not always work on the same timeline as the joint staff.

The Joint Operations Center (JOC) is another cross-functional organization that is key to success in ISR-targeting cooperation. Many times, this is the area in which operations organizations and their targeteers dominate the interaction with ISR. For example, the Joint Fires Element will have a group of people manning the fires and targeting portion of the JOC. The J2 also has personnel in the JOC and will typically have their intelligence operations personnel manning the floor with close links to the ISR personnel.

The personal relationships described earlier can definitely help to make last minute, out-of-cycle changes to the ISR plan, but the key venue to handle emerging targeting opportunities is thorough the JOC. Many are familiar with time sensitive targets (TSTs) that must be acted upon quickly when found because they provide fleeting opportunities to achieve the effects desired by the joint force commander. TSTs, however, are only one type of out-of-cycle requirement that must be coordinated with J2. Targeting and J2/ISR personnel at the JOC should handle any target that emerges following the JTBC because it becomes out of cycle if it cannot be approved at the board.

When operations targeting personnel identify a TST or other out-of-cycle target, they will immediately notify the J2 representatives at the JOC. This allows the J2 representative to coordinate for increased or additional ISR support to that area. If a targets requires verification, that can be provided by traditional ISR assets or through operational assets that are in the area.

TSTs are especially challenging because they require quick work by all at the JOC to ensure the emerging target can be serviced successfully. The targeting personnel must lead the effort to clear fires and task a component to strike the target. The J2 representative must, at the same time, attempt to maintain surveillance of the target and ensure that the destruction of the target does not eliminate any greater future collection value. It is a time-compressed process run as a battle drill in the JOC and must be practiced regularly by both ISR and targeting officers.

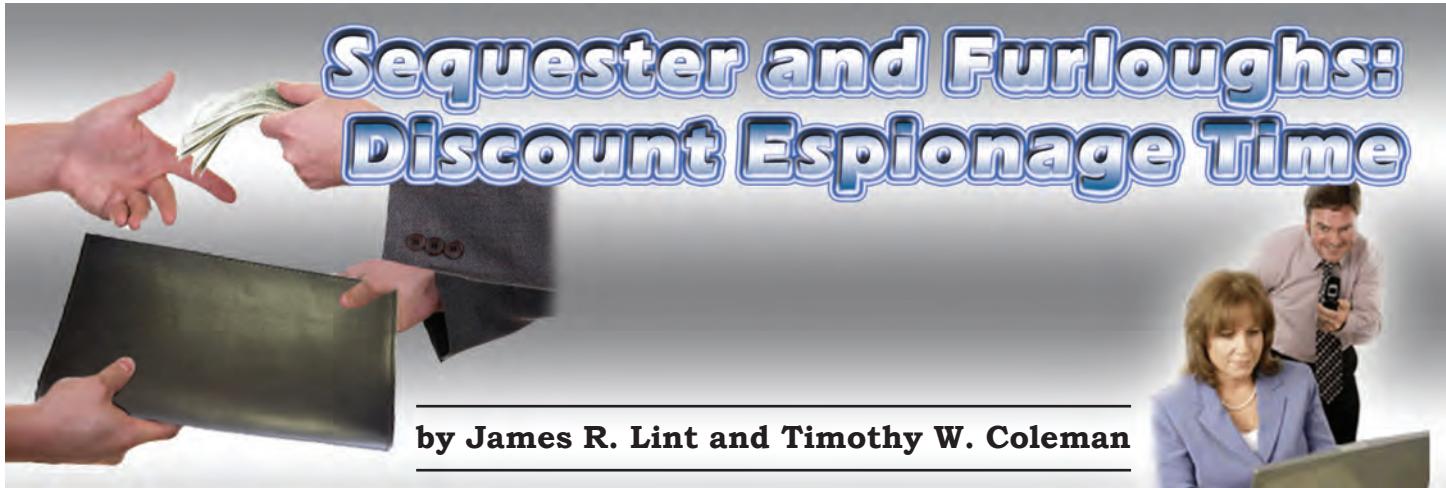
## **Conclusion**

The ISR personnel on a joint staff will likely be undermanned and fully engaged responding to requirements from the J2. In order for targeting professionals from both the intelligence and operations organizations on the joint staff to integrate and synchronize with ISR, targeteers must work hard to establish relationships and remain engaged in the ISR and J2 battle rhythm. The invaluable support ISR provides to targeting will be substandard if it is not well planned and rehearsed routinely. It is imperative that both sides of the relationship learn as much as they can about the other, so both are fully prepared to develop a synchronized plan that supports the joint force commander. These planning and rehearsal efforts are key to ensuring the ISR and targeting teams are ready to achieve mission success. 

## **Endnotes**

1. JP 1-02, DoD Dictionary of Military and Associated Terms, 8 November 2012, amended through 15 April 2013, 141.
2. Ibid., 224.
3. Ibid., 134.
4. JP 3-33, Joint Task Force Headquarters, 30 July 2012, II-10.
5. JP 3-60, Joint Targeting, 31 January 2013, GL-5.

*Major Fair is currently a Senior Joint Targeting Officer, U.S. Forces Korea. He has served as the Operations Officer and Executive Officer in the 109<sup>th</sup> MI Battalion and 3-38<sup>th</sup> Cavalry Squadron; Current Intelligence Officer and SGS, I Corps; JSTARS Company Commander and Deputy Mission Crew commander, and as a Company Commander, 25<sup>th</sup> Infantry Division. He holds a BA in International Affairs; an MBA with concentration in International Business; a Master's in Public Administration, and a Master's in Strategic Intelligence.*



# Sequester and Furloughs: Discount Espionage Time

by James R. Lint and Timothy W. Coleman

## Introduction

The threat of penetration by Foreign Intelligence Security Services (FISS) is ever present and the Army trains its soldiers, as well as civilian employees, to remain always vigilant. Training and awareness efforts are clearly articulated in Army Regulation 381-12, Threat Awareness and Reporting Program (TARP).

Formerly known as Subversion and Espionage Directed against the U.S. Army (SAEDA), TARP outlines the policy and responsibilities for threat awareness and reporting within the U.S. Army. Specifically, it requires Department of the Army personnel to report any information to Counterintelligence (CI) regarding known or suspected espionage, international terrorism, sabotage, subversion, theft or illegal diversion of military technology, information systems intrusions, and unauthorized disclosure of classified information, among other required security and espionage concerns.

This requirement is not without justification. Cleared personnel can become targets for recruitment by foreign spies and hostile intelligence services through no fault of their own. It is simply the reality and consequence of having access to classified information and sensitive U.S. government secrets.

## Not Access Alone

It is not only access to classified information that makes one an inviting target, there are other factors that increase the desirability. In fact, any Army team member/employee and or soldier can be targeted because of where they are stationed, where they travel, or even because of an ethnic or cultural background of particular interest.

It should be noted and emphasized that being a target for recruitment does not necessarily reflect poorly on an individual. The opposite also applies, especially if the reason one is targeted is because of their susceptibility to recruitment or exposure to compromise. Even so, just being a target does carry with it embedded risk factors, as it clearly increases the potential that a weakness or pressure point can be discovered and exploited by foreign intelligence collectors.

## Three Targeting Elements

The historical record clearly demonstrates that U.S. personnel with security clearances are regularly targeted. Foreign agents have repeatedly been able to entice Americans to turn and commit treason. The question quickly becomes, what is it that makes certain Americans so inviting and targets of opportunity?

Prominent and well-publicized instances of Americans turned traitor show that monetary reward and financial gain are often major driving factors in the equation. In turn, it should come as no surprise that foreign intelligence agents seeking new, well-placed assets often examine the financial circumstances and standing of potential targets. Financial difficulties provide an initial area of potential temptation as an element to facilitate the evolution of an individual's compromise, but it is generally not the only factor at play in the targeting and recruitment effort.

Another, and sometimes more nefarious, element to recruitment can include exploiting personal feelings of disillusionment, anger, frustration, and disappointment. These sentiments can arise for a multitude of reasons and may run the gamut to

include being passed over for a promotion, feeling under appreciated at work, or disgruntled with the Army or even America itself. These beliefs, often manifested in feelings of anger as well as resentment, are then used by foreign intelligence case officers to manipulate a potential target into justifying his or her espionage.

An individual who possesses a security clearance, financial trouble, and is disgruntled is a dangerous combination and a complex problem, especially for CI interdiction efforts.

### **Catch More Flies with Honey**

Given the current budgetary environment with furloughs the talk of the town and the term sequestration becoming a water cooler buzzword, targets may seem to abound. A quick superficial read of Letters to the Editor in various magazines and publications that are widely read by federal employees and members of the military makes the case for a target rich environment for foreign agents. There are countless letters and blog comments that clearly depict a growing segment of government personnel, many likely holding security clearances, venting their frustration and anger.

Disgruntled individuals who publicly voice their concerns make easy work for foreign intelligence operatives who seek potential turncoats of opportunity. In many respects, it would appear as though potential opportunities for penetration are being served up at an all you can eat buffet and the chow line stretches around the proverbial corner!

Currently, sequester and looming furloughs are expected to greatly impact soldiers. Stress, greater work scrutiny, coupled with an increase in regulations and even some mandated early outs will impact all ranks of the Army. Inevitably, this will extend into the civilian workforce, particularly with an estimated 20 percent pay cut reportedly on the horizon.

While 99.9 percent of the individuals likely to be hardest hit are loyal and dedicated American patriots, there is no question that many will feel disgruntled and could even encounter financial hardship as a consequence. This only makes the job of foreign intelligence operatives all the more easy.

### **The Certainty of Maybe Not Today**

As accurate and apropos as the adage, "If you play with fire you will get burned" is, it is vital to

plainly state that if you commit espionage you will be caught. The Army's military intelligence and CI organizations are designed to protect soldiers and employees from espionage threats and FISS espionage overtures. They remain key to protecting the technology advances that give American soldiers the edge on the battlefield. Army CI units have partnered with the Federal Bureau of Investigation (FBI) for some great wins in the past. Today, it may be a target rich environment for FISS recruitment, but one should assume that Newton's Third Law of Motion applies here to CI activities—for every action there is an equal and opposite reaction.

The disgraced former U.S. Army Signals Intelligence analyst working for the National Security Agency, David Sheldon Boone, whose 24 years and four months sentence for espionage on behalf of the former Soviet Union is proof positive. Boone was arrested following a successful sting operation by the FBI in 1999 that was supported in large part by Army CI efforts. According to press reports at the time, Boone decided to become a Soviet spy in order to alleviate "severe financial and personal difficulties."

### **Remaining True to the Core Values**

It is not by accident that loyalty is the first word cited as part of the Seven Core Army Values. It is also not accidental that the U.S. Army is composed of both soldiers and civilians who know the importance of the mission at hand and, therefore, go well above and beyond what is expected. They all bear truth to the core value of loyalty.

Nevertheless, with the current operating environment, the realities faced by all and the resulting pressures, there should be no doubt that an array of well-trained, highly proficient foreign intelligence professionals are operating in overdrive. We must remain as vigilant as ever. This is why support to your battle buddies, and knowing your left and right flanks will get us through this time of trials with our core values remaining intact.

A 'discount espionage' opportunity exists in the eyes of American adversaries, as it may now be cheaper to buy a turncoat. The return on investment for a foreign intelligence service is made easy with disgruntled, financially overextended, and cleared individuals who more than ever may be perceived as ripe targets for espionage recruitment operations.

For this reason that we must enhance our awareness, redouble our vigilance, and steadfastly support our fellow co-workers. The Army has a series of vitally important programs that are there to take care of our people, and yet often go underutilized. These are not new programs, as many were launched over 50 years ago. They are, however, overlooked and underappreciated. The Army Community Services, Employee Assistance Programs, and organizational Chaplains are there to serve those who serve. Financial counseling and assistance is also available.

Your Army, as well as those that lead it, are ready, willing, and able to do their part. Your responsibility remains to be vigilant and help your fellow soldiers and office workers. It is one Army and one team, and we are dependent on that more today than ever before.

## Espionage Indicators

- Disgruntlement with the U.S. Government.
- Any statement that suggests conflicting loyalties may affect the proper handling and protection of sensitive information.
- Active attempts to encourage others to violate laws or disobey security policies and procedures.
- Membership in, or attempt to conceal membership in, any group which: advocates the use of force or violence to cause political change within the U.S.; has been identified as a front group for foreign interests; or advocates loyalties to a foreign interest.
- Requests to obtain or facilitate access to classified material without authorization.
- Extensive, unexplained use of copier, facsimile, computer equipment, unauthorized cameras, or recording devices to reproduce or transmit sensitive or classified material.

On his deathbed in 1801, the infamous traitor Benedict Arnold reportedly said, "Let me die in this old uniform in which I fought my battles. May God forgive me for ever having put on another." Remember, inaction begets targeting. Targeting invites compromise. Compromise precipitates contrition. And forgiveness for treason is not an option. 

*James Lint has 37 years of experience in Military Intelligence within the U.S. Marine Corps, U.S. Army, contractor, and civil service. He is retired from the U.S. Army and is a MICA MI Corps Mentor. He has served in the DHS Office of Intelligence and Analysis and at the Department of Energy S&S Security Office. He is currently the G2 for the Communications-Electronic LCMC. His military assignments include Korea, Germany and Cuba in addition to numerous CONUS locations.*

*Timothy W. Coleman is a writer and a security analyst who has co-founded two technology startup firms. He has a Masters of Public and International Affairs in Security and Intelligence Studies and a Masters of Business Administration in Finance.*

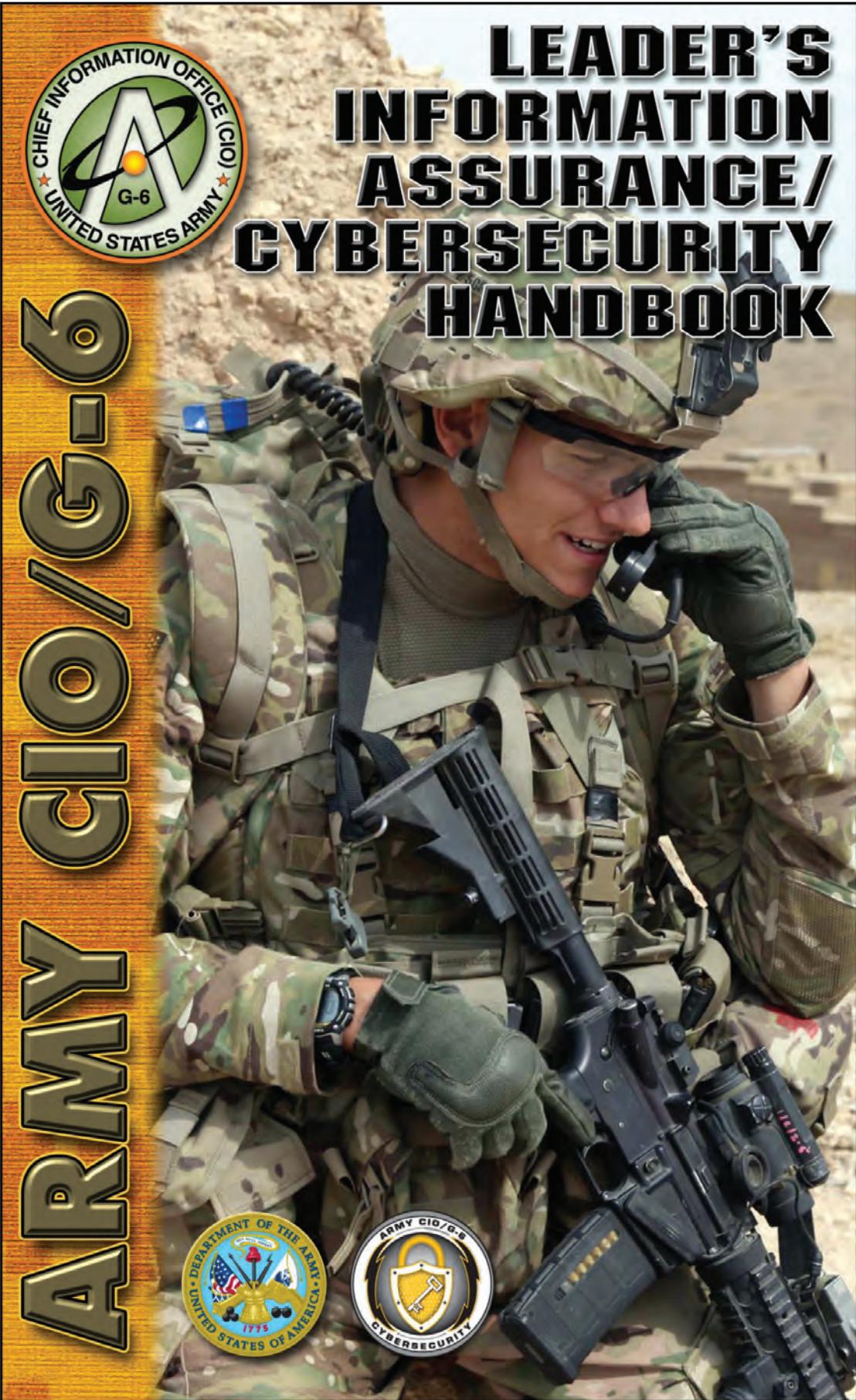
- Unauthorized removal or attempts to remove unclassified, classified, export-controlled, proprietary, or other protect material from the work place.
- Working odd hours without approval or with no logical reason.
- Unexplained affluence or life style inconsistent with known income.
- Joking or bragging about working for a foreign intelligence service.
- Behavior indicating concern that one is being investigated or watched, such as actions to detect physical surveillance, searching for listening devices or cameras, and leaving "traps" to detect search of the individual's work area.
- Any part-time employment or other outside activities that may create a conflict of interest with one's obligation to protect classified or sensitive but unclassified information.

- Courtesy APG News, 25 April 2013

*This article originally appeared in Homeland Security Today Magazine on 15 July 2013. <http://www.hstoday.us/blogs/guest-commentaries/blog/sequester-and-furloughs-its-discount-espionage-time/ce7c3324c8fc03c57cac-45bacd507b1a.html>. It is reprinted with permission.*

# Check Out MIPB Online @





## **IA/CYBERSECURITY IS CRITICAL TO OPERATE IN CYBERSPACE**

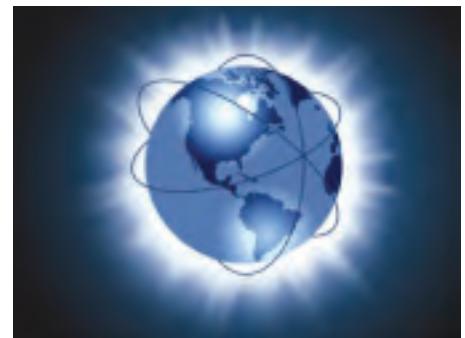
**Commanders, leaders, and managers are responsible for ensuring that Information Assurance/Cybersecurity is part of all Army operations, missions and functions. You must make certain that your organization adopts and institutes the practices necessary to ensure the protection of information and personnel.**

This Handbook is designed to provide leaders the information and tools to address today's complex security challenges. It is also a quick reference for managing Cybersecurity issues that will help ensure that Soldiers, Civilians and contractors know their responsibilities for daily practices that will protect information and our IT capabilities.

### **WE MUST PROTECT THE NETWORK!**

Information Assurance (IA)/Cybersecurity is the Army unified approach to protect the confidentiality, integrity and availability of our information and operations. IA/Cybersecurity is critical to your mission success and therefore must be part of your risk management processes.

It is essential in assisting you with identifying vulnerabilities and taking the necessary steps to conduct your daily operations. Army regulations, policies and guidance provide the Army imperatives authority, responsibility and accountability necessary to promote a culture that is risk aware and complies with practices that minimize vulnerabilities to Army networks, systems and information. As leaders, you must ensure that your organization remains committed to practices that protect Army networks, systems and information as well as personnel identity.



## **INSTITUTING THE IA/CYBERSECURITY IMPERATIVES**

- Incorporate IA/Cybersecurity into your Risk Management Process
- Treat IA/Cybersecurity like Safety
- Link IA/Cybersecurity to Readiness

As a leader, it is your responsibility to ensure that your business and information systems are protected.

You must make certain your personnel are responsible for daily practices that protect information and IT capabilities for mission success.

It is your responsibility to assess your mission capability and practice good Cyber Hygiene - personal practices that comply with policies, process, and standards that safeguard computer use.



**Remember: It is your responsibility to ensure the protection of our networks, information, and people, through increased IA training, improved Cybersecurity practices, and appropriate risk management.**

## EMPOWER YOUR IA/CYBERSECURITY TEAM

### Know Your IA Team!

Your IA team manages your IA/Cybersecurity program. Get to know these professionals as they are key in helping you set your priorities for protecting the network and safeguarding information. Your organization must know that you make Cybersecurity a priority and understand that Cybersecurity is everyone's business.



#### Your IA/Cybersecurity team may include:

- **G-6/S-6** - The principle staff officer with the responsibility for the management of the commander's IA program.
- **IA Program Manager (IAPM)** - Senior IA advisor to the commander.
- **IA Manager (IAM)** - Implements the IA/Cybersecurity program with assistance from the IASOs.
- **IA Support Officer (IASO)** - Provides Information Assurance oversight, guidance and support to the general user.

## TRAIN YOUR PERSONNEL

Everyone must complete the appropriate training required for their position.

The Army Training and Certification Tracking System (ATCTS) provides reports and manage personnel IA training records for your IA/Cybersecurity training management.

IA training is provided through the Army IA virtual training, and successful completion of training courses is automatically reported to the ATCTS site.

The Army IA Virtual Training site also offers training for

- ◆ Portable Electronic Devices
- ◆ Personally Identifiable Information (PII)
- ◆ Safe Home Computing



**Army Training and Certification Tracking System (ATCTS):** <https://atc.us.army.mil/>

**Army IA Virtual Training:** <https://iatraining.us.army.mil/>

**DoD Cyber Awareness Challenge** <https://ia.signal.army.mil/DoDIAA/default.asp>

Your local IA/Cybersecurity team can answer your questions about IA training requirements. Questions concerning ATCTS or the Army IA virtual training site can be directed to [cio-g-6netcomiawip.inbox@mail.mil](mailto:cio-g-6netcomiawip.inbox@mail.mil).

## IA/CYBERSECURITY IS EVERYONE'S RESPONSIBILITY

**Cyber Hygiene is adherence to laws and regulations, DoD and Army policies, procedures, and standards. Enforcing IA compliance is critical to strengthening the Army Cybersecurity posture.**

Beyond required security training, leaders must ensure that Soldiers, Civilians and contractors understand the threat they pose to operational security with non-compliance to IA/Cybersecurity policies and practices. People are the Army's first line of defense in sustaining good cyber hygiene and reduction in the insider threats. Most vulnerabilities and malicious acts against Army systems and information can be addressed through comprehensive and effective cyber hygiene.

Everyone is responsible for Cybersecurity!



**As leaders, you must remain vigilant and constantly assess your IA/Cybersecurity posture and program with regard to readiness, risk, resources, and reporting. Have your IA/Cybersecurity team use the IA Self Assessment Tool located at <https://iatraining.us.army.mil> to evaluate your security posture, and report back to you with the results, and their plans to address any weaknesses identified.**

## PHISHING: UNDERSTANDING THE THREAT

Everyone has seen them; an email that claims to be from a trusted source and requests your personal information, or directs you to a seemingly innocent website. These phishing attempts are usually obvious. However, phishing is a major issue that plagues the DoD and Army. Phishing is often successful because the improved quality of these attacks make it more difficult to identify them as a hoax. Phishing attacks have also become more sophisticated, targeting specific individuals with content customized specifically to them.



**Everyone must be constantly aware of the phishing threat. Always be sure an email is legitimate before clicking any links or attachments, and never click any links or attachments that were received in an email that was not digitally signed.**

Ensure your personnel annually complete the anti-phishing course located at:  
<https://iatraining.us.army.mil/>

## SECURING THE SYSTEM

The Internet poses serious potential threats. We must constantly ensure all computers and devices meet the appropriate security requirements before connecting them to the network.

All office and home computers must be up to date with required system security patches, Anti-Virus software application, and should only be connected to the internet from behind a firewall.

The Army Home Use program makes it easy for Army Soldiers and Government Civilians, to secure their home computers by giving them free access to both Symantec and McAfee anti-virus and firewalls.

<https://www.acert.1stiocmd.army.mil/Antivirus/>



Protecting your home computer with current antivirus applications and connecting to the internet from behind a firewall, are vital to preventing malware from infecting your computer.

You should discuss with personnel the importance of IA/Cybersecurity on their home computers. Ensure they are aware of the free resources available to soldiers and government civilians, and are practicing good Cyber Hygiene both at work and at home.

## PERSONAL MOBILE DEVICES

Department of Defense and Army policies prohibit connecting unauthorized information systems to the network, and prohibit conducting official business on personally owned devices that do not meet Army standards and certification requirements.

Although the Army is currently considering a strategy to allow personal mobile devices access to the Army Network, personal cell phones, tablets or other mobile devices are currently not authorized for access and government use. Using unapproved devices for official business is not only a security violation, but could also cause major security incidents jeopardizing sensitive information and putting our operations and personnel at risk. Compromising classified information in these cases is a serious security violation that may result in punitive actions.



More information on personal mobile devices can be found at:  
<https://informationassurance.us.army.mil/>

## THE COMMON ACCESS CARD (CAC)

Your CAC is your physical and digital identification; treat it as a sensitive item!

- ◆ Your CAC allows you to digitally sign emails so recipients can verify that you are the sender and the information was not altered in transit.
- ◆ Your CAC protects sensitive information in emails and computer files by allowing you to encrypt them.
- ◆ Your CAC is a physical piece of IA/Cybersecurity and is tightly bound to your online identify. Therefore, it must be protected at all times, even when not in use.
- ◆ Report a lost CAC card as soon as it's confirmed to be missing.



SIPR Tokens for SIPRNet access, have many CAC-like security capabilities and will be required to access SIPR systems. Treat it as a sensitive item and protect them as you would your CAC.

## RISK MANAGEMENT

Leaders must always assess potential threats and the impact on operations. Contingency plans are critical for sustaining operations through attacks or interruptions to network service.

Organizations must develop Continuity of Operations Plan (COOP) in order to maintain and sustain operations.

For your COOP to be effective, it must include:

- ◆ A Business Recovery Plan
- ◆ An Information Technology Contingency Plan
- ◆ A Facility Disaster Recovery Plan

Ensure that your plan works in conjunction with any existing COOPs adjacent to your area of control.

In addition to a fully developed COOP you must review the plans annually and practice its execution as required for the sensitivity level of the information being handled.

More information on COOPs is found in DA PAM 25-1-1.



## INCIDENT RESPONSE

Every organization should have processes in place and the people to contact in case of an incident whether it is a security breach, information spillage, or disclosure of Personally Identifiable Information (PII). Guidelines on reporting processes are defined in AR 25-2. [http://www.apd.army.mil/pdffiles/r25\\_2.pdf](http://www.apd.army.mil/pdffiles/r25_2.pdf)

### Common Examples of Reportable Incidents Include:

- ♦ Unauthorized Disclosure of Classified Information (spillage) - Higher-level classified information is placed on a lower level classified information system (i.e., sending an email that contains Secret content on the NIPRNET).

US CERT has a one-hour reporting requirement for PII related incidents. Ensure your IA team's response plan meets this requirement.



- ♦ Loss or Compromise of Personally Identifiable Information (PII) - PII information that can uniquely identify, contact, or locate a single person (i.e., posting a personnel roster which includes names, SSNs, addresses and medical information on a public website). Specific instructions on PII incidents and the reporting processes are on the Records Management and Declassification Agency's website located at: <https://www.rmda.belvoir.army.mil>
- ♦ Receipt of suspicious emails and phishing scams. Examples include requests to provide passwords or other sensitive information to an unknown source.

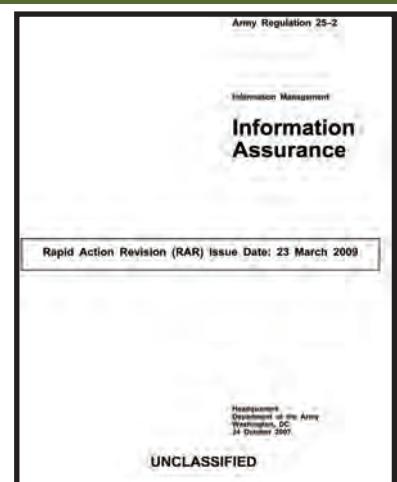
**Always contact your IA team or NEC if there is any question concerning a security matter.**

## INFORMATION ASSURANCE ENFORCEMENT

AR 25-2 outlines sanctions that may be imposed for civilian, military and contractor personnel found in violation of Army security practices.

AR 25-2, paragraph 1-5.j states that military and civilian personnel may be subjected to administrative and/or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place Army information systems at risk by not ensuring the implementation of DoD and Army policies and procedures.

AR 25-2 further stipulates that military personnel may face administrative as well as non-judicial or judicial punishments authorized by the Uniform Code of Military Justice. Similarly, sanctions for civilian personnel may include administrative actions as well as judicial punishment. And defense contractors employees must perform under the terms of the contract and applicable directives, laws, and regulations.



## QUESTIONS AND TOPICS FOR YOUR IA/CYBERSECURITY TEAM

1. Ask personnel if they know who to contact with IA questions or concerns.
2. Do your people understand the importance of protecting their CAC card?
3. Question personnel about the last time they completed their DoD Cyber Awareness training. Do they require any additional certifications? If so, what's the status of those additional certifications?
4. Do your people understand Phishing, and the risk it poses to their personal and professional life?
5. Are your people using a firewall and anti-virus software on their home computers. Are they aware of the free security software that is available for their home computers? <https://www.acert.1stiocmd.army.mil/Antivirus/>
6. Do you include IA/Cybersecurity topics in your all-hands or town hall meetings?
7. What processes are in place to ensure personally identifiable information and sensitive/classified information is not posted on your public facing pages?
8. Conduct periodic brown bag sessions on topics such as safe home computing practices, incident reporting procedures, and using unapproved personnel devices such as smart phones and tablets to conduct official business, etc.
9. Leverage articles and cartoons from “OnCyberPatrol” website as part of your overall awareness strategy. Content can be accessed at: <http://ciog6.army.mil/OnCyberPatrol.aspx>
10. Lead by example and counsel people who break the rules.



## REFERENCES AND CONTACTS

Army IA One Stop Shop: <https://InformationAssurance.us.army.mil/>

IA/Cybersecurity Leader’s Handbook Discussion Forum: <https://www.milsuite.mil/book/docs/DOC-73030>

Army Training and Certification Tracking System (ATCTS): <https://atc.us.army.mil/>

Questions regarding the ATCTS or the Army IA virtual training site can be directed to:  
[ciog-6netcomiawip.inbox@mail.mil](mailto:ciog-6netcomiawip.inbox@mail.mil)

Army IA Virtual Training: <https://iatraining.us.army.mil/>

Army IA Self Assessment Tool: <https://iatraining.us.army.mil/>

DoD Cyber Awareness Challenge <https://ia.signal.army.mil/DoDIAA/default.asp>

US Army Computer Emergency Response Team (ARCERT) <https://www.acert.1stiocmd.army.mil/>

Army Home Use program <https://www.acert.1stiocmd.army.mil/Antivirus/>

Army Publishing Directorate <http://www.apd.army.mil/>

Army e-Learning (Skillport) <https://usarmy.skillport.com/>

**IA/Cybersecurity Leader's Handbook Discussion Forum:**  
<https://www.milsuite.mil/book/docs/DOC-73030>



**AMERICA'S ARMY:  
THE STRENGTH OF THE NATION™**

**Army Chief Information Officer/G-6  
107 Army, Pentagon  
Washington, DC 20310  
CIOG6.Army.mil**

v13.5.9b

# **Words and Action**

## **How Text Analysis is Transforming the War on Terror**

### **Introduction**

Deep within the Department of Defense (DOD) and Intelligence Community (IC), there are hundreds of linguists and analysts at work with a mandate to translate, process, and extract intelligence from an ever-expanding mountain of documents in many languages. These highly-trained specialists are a first line of intelligence in the war on terror and other areas of interest. Typically, linguists will translate each document from its native language into English, or at the very least, manually locate and translate the names within a document so that an analyst can match those names and connect them to any other relevant information or databases.

This incredibly important source of intelligence is time-intensive and costly, and until recently, it was a fully manual process. It could take hours—or days—to manually review and input accurate standardized translations. However, these linguists and analysts now use a simple Microsoft Office plug-in called *Highlight*, which automatically finds, translates, and matches names to IC standards. Users select persons and places highlighted in the document, and are instantly provided with correct spelling options for translations. *Highlight* utilizes advanced text analytics to empower its users to process documents at a faster pace with higher accuracy.

The Defense Intelligence Agency (DIA), through funding provided by the Office of the Director of National Intelligence (ODNI), has sponsored the development and licensing of *Highlight*, so that the software can be implemented easily and at no cost to any agency within the IC and DOD. Program managers can simply make a request to DIA for the software by providing the number of user copies needed. The upcoming version of *Highlight* will add Mandarin to the currently supported languages of Arabic, Dari, Farsi, Pashto.

“With the capability to have names and places instantly highlighted and referenced for proper standardization, we save so much time,” says Nick Bemish, Senior Human Language Technology Expert at the DIA’s Center for Language, Regional Expertise, and Culture. “It allows multiple government departments and agencies to cooperate and collaborate. This means we work smarter and faster. We save on costs, and we get critical information to our intelligence operations more quickly.”

### **A Sense of Urgency**

U.S. intelligence operations have always relied on correct interpretations of Arabic documents and references in English-language reports. But the events of 9/11 prompted, over time, a complete overhaul of how agencies prepare these reports. Due to a vast degree of language inconsistencies in these reports, DOD/IC operatives were placed at a disadvantage, unsure of key information which could play a central role in the investigation of a possible hostile party.

Much of the problem was related to various, often subtle discrepancies found in the spellings/presentations of the names of people (such as persons of interest in a terrorism plot) and geographic locations. A suspect could be identified as both “Farid” and “Fared” interchangeably throughout a number of documents, for example, or even within the same document.

The lack of uniformity resulted in significant, recurring flaws in the ability to consume the intelligence reports, which contribute highly valuable information for ongoing investigations, field operations and communications with policy makers/lawmakers. A sense of urgency emerged to implement spelling standardizations of names and places, one involving the often intricate process of linguistic analytics—automatically isolating, extracting and iden-

tifying words for transliteration so they align with IC standards and match with confidence against watchlists and other databases.

## Policy in Play

Top IC decision makers took action to address the growing concerns. In 2002, the Intelligence Authorization Act specified that the Director, Central Intelligence must institute a standardized method for transliterating any names referencing a person and/or place originally rendered in a foreign language-based alphabet into the Roman alphabet.<sup>1</sup>

In May 2003, an IC standard for the transliteration of Arabic names was issued, to be applied to all final written reports and products for IC users.<sup>2</sup> It was not, an official-use memo stated, intended to eliminate any variations of a name which can contribute forensic information. Instead, it was intended to establish a uniform English-language transliteration from modern Arabic to link to forensic information in a way that would identify names being referenced.

"Ambiguities can result...because the Arabic source generally omits short vowel markings, double consonant marks, and other diacritics that would clearly distinguish the name," the May 2003 memo states. "Linguists use their experience with the language and aids such as online tools and name dictionaries to determine the exact Arabic and the appropriate transliteration into the Roman alphabet."

On June 4, 2003, CIA Deputy Director of Central Intelligence for Community Management Joan A. Dempsey issued an official-use memo which set a July 1, 2003 deadline for agencies to take steps to implement a uniform Arabic-transliteration scheme for personal names, and ensure that their staffers have access to the CIA World Factbook leadership profiles for consistent spellings of well-known Arabic names.<sup>3</sup> The IC Foreign Language Executive Committee and the Assistant Director of Central Intelligence for Analysis and Production (ADCI/AP) collaborated upon the project, which was reviewed and approved by the National Intelligence Analysis and Production Board (NIAPB).

In addition, the memo reported that the ADCI/AP was working with language/technical experts to bring in automated tools to assist personnel with the deployment of the system.<sup>4</sup>

The latter initiative remained key. At the time, analysts and linguists generating these reports were resigned to inputting changes based upon standardized language guidelines, and then reviewing documents for inconsistencies and correcting them, in a time consuming, manual manner.

## An Automated Alternative to Manual Processes

At the time of the June 2003 directive from the CIA, a Cambridge, Massachusetts based company named Basis Technology was already developing an automated technology solution, now called Highlight, which is enhancing manual, text-authentication practices.

Basis Technology started out in 1995 as a commercial services firm, focusing on helping enterprises do business globally. Since that time, the company has developed a suite of products that provides morphological analysis, entity extraction, name matching and name translation for enterprise software applications.

An early customer was Google, which brought Basis on board when it expanded to China and required support to perform text segmentation in search functions. By May 2002, Basis made its products available to the federal market, where its enterprise text analytics software is now utilized throughout the DOD and IC.

In 2006, the company introduced the first version of Highlight to the IC. With this new solution, IC analysts and linguists could automate the entire process or use it to improve and speed up their existing workflow. The incremental cost of adding a capability such as Highlight as a productivity tool to the linguist or analyst's workflow is approximately 0.7 percent of the cost of a person working without the technology.

The original contract for what is now Highlight began as a joint project sponsored by four different IC agencies in 2006. The program then funded by ODNI and administered by DIA. The goal of this ongoing project is to provide a Microsoft Office plug-in that supports linguists and analysts when they need to correctly render names of people and places that are being transliterated from non-Latin scripts, such as Arabic.

In one example from 2008, Highlight was used by Coalition Forces to standardize a list for the Iraqi

government, one involving the names of 93,000 “friendly” Iraqi militia military members who were contributing to the U.S. effort. The members were set to serve solely for Iraq, and all 93,000 names had to be translated in a standardized manner to Arabic before the hand-off could take place. Because Basis brought automation to what previously was a manual undertaking, the entire project was completed in days, as opposed to months.

With Highlight, there is no integration, as the solution functions as a plug-in which can be immediately downloaded and added to existing Word/Excel/Office tool sets. It is compatible with Windows 8. If there is a non-Windows environment for which Highlight is desired, managers can contact Basis to see if a custom configuration may be arranged. Highlight complies with a broad range of network security clearances and certifications.

English (IC)	Gloss	POS	Arabic
Khalaf	substitute/scion	Name/Noun	خلف
Khalf	behind	Adverb	خلف
Khalf	rear/back/behind	Noun	خلف
Khilf	teat/nipple	Noun	خلف
Khulf	dissimilarity/variance	Noun	خلف

English	Country	Title
KHALID bin Ahmad bin Muhammad Al Khalifa	Bahrain	Minister o
KHALID bin Ahmad bin Salman Al Khalifa	Bahrain	Minister o
HAMAD bin Isa Al Khalifa	Bahrain	King
AHMAD bin Muhammad bin Hamad bin Abdallah Al Khalifa	Bahrain	Minister o
RASHID bin Abdallah bin Ahmad Al Khalifa	Bahrain	Minister o
Mohamed CHARFI	Algeria	Minister o

The latest version of Highlight (6.0), due to launch in October, has a very user-friendly interface, and is designed to empower—but not replace—the analyst. Analysts/translators call up a document and then select a particular name or place with their cursors. With this, Highlight immediately presents the best translation options. The user decides if the software will work interactively or automatically, depending on their workflow. This is because, as with spell-checking tools, humans should have the option to make the final decision, rather than relying on machines to do so. (Spell-check programs typically will offer incorrect “best recommendations” based upon misinterpretations on the part of the software program. Highlight operates with this potential technology-based error potential in mind.)

“Allowing users to control their workflow and utilize the level of automation they need will be a huge boost for our teams,” Bemish says. “Highlight serves as a force-multiplier for our linguists and analysts, giving them increased speed, accuracy and control over all the names within their documents. This simple software plug-in is a great example of inter-departmental cooperation in the effort to accomplish a mission.”

In the future, Basis Technology will continue to merge its enterprise text analytics abilities into Highlight, providing more robust processing and intelligence capabilities into the Office plug-in. One future feature of interest is Basis’s capability to provide “entity resolution” which can cross-reference names of entities (people, places, and things) within multiple documents and link them to each other and automatically

ويقول أنصار مرسى إنهم تعرضوا لنيران قناصة كانوا يعتلون أسطح المباني القريبة خلال الاشتباكات عند موقع مراسل بي بي الاعتصام، حسبما أفاد كونتني سومرفيلد ويضيف مراسلتنا أن أنصار القاهرة Cairo سي في مرسى يزعمون أن ثمة مسلحين كانوا في حماية قوات في غضون هذا، أورد التلفزيون الرسمي أن الأمان الشرطة اعتقلت سبعة من أنصار محمد مرسي بالقاهرة.

منذ ذلك، مرسى، قاتلوا لحياتهم أسلحة غير مرخصة على خلفية إزاحته عن الإنفاذ الوطني. السلطة التي يتبعها مرسى - بن في مدن عدة من بينها القاهرة والاسكندرية.

English (IC)	Gloss	POS	Arabic
Muhammad	Muhammad//Mohamed	Name	محمد
Mhammed	Mhammad	Name	محمد
???	(original input)		محمد

English Country Title

Muhammad MURSI	Egypt	President
Mohammad KHAZAI-Torschizi	Iran--NDE	Permanent Representative to the UN, New York
Mohammad MOMANI	Jordan	Minister of Parliamentary Affairs

connect every entity reference to a matching entry within a database such as *Intellipedia*. Basis will also continue to add additional language support such as Korean or Russian, as requested by its users. \*

To find out more about acquiring Highlight for your organization, contact Jennifer Flather, Highlight Program Manager, DIA, (202) 685-6783 or [jennifer.flather@dodiis.mil](mailto:jennifer.flather@dodiis.mil).

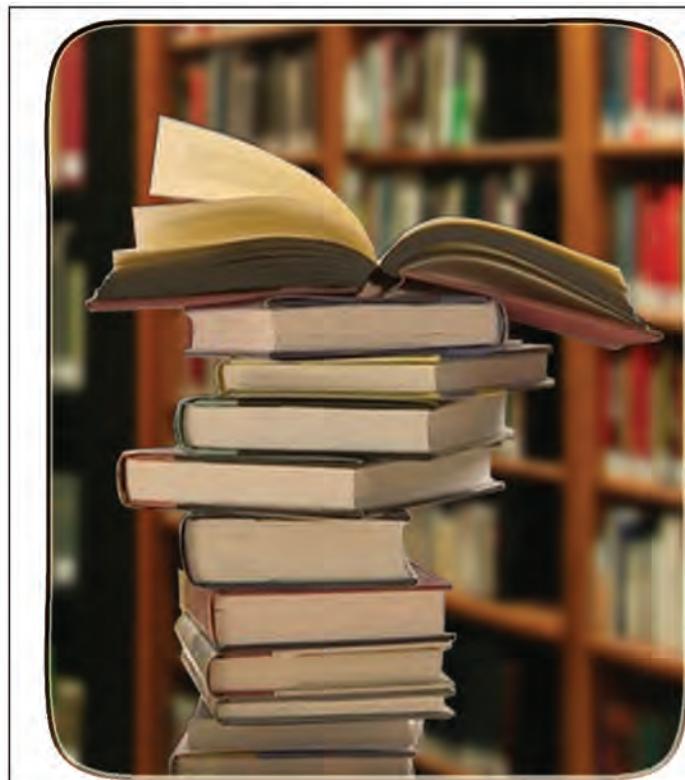
## Endnotes

1 Intelligence Authorization Act for Fiscal Year 2003, “Standardized Transliteration of Names into the Roman Alphabet,” 27 November 2002, Section 352.

2. IC Standard for Transliteration of Arabic, May 2003, 1.

3. Intelligence Community Standard for the Transliteration of Arabic Names in Final Written Reports and Products, 4 June 2003, 1.

4. Ibid., 1.



# Read any good books lately?

We welcome reviews of books related to Intelligence or Military History. Please review our list of available books and book review submission standards under the Professional Reader Program at [https://ikn.army.mil/apps/mipb\\_mag](https://ikn.army.mil/apps/mipb_mag).

Email your book reviews along with your contact information to [sterilla.smith@us.army.mil](mailto:sterilla.smith@us.army.mil).



**Mission Command Center of Excellence  
US Army Combined Arms Center  
Fort Leavenworth, Kansas  
28 June 2013**

## Doctrine Update 3-13

The United States Combined Arms Center publishes the Doctrine Update periodically to highlight recent and upcoming changes to doctrine and provide information related to doctrine use.

This Doctrine Update provides information on the overall Doctrine 2015 strategy. To maximize the understanding of the Doctrine 2015 strategy and the timelines of significant publications, disseminate this update to the lowest level.

The proponent of Doctrine Update is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations by e-mail to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil or by mail to Commander, U.S. Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCK-D (Doctrine Update 3-13), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337. POCs for this update are Mr. Clinton J. Ancker III at clinton.j.ancker2.civ@mail.mil and LTC Augustus Dawson at augustus.r.dawson@mail.mil.

### Army Publishing Directorate Notifications

To stay current on what the Army publishing directorate (APD) has published, subscribe to APD's weekly update at: [http://www.apd.army.mil/AdminPubs/new\\_subscribe.asp](http://www.apd.army.mil/AdminPubs/new_subscribe.asp). This update lists all authenticated Army publications published in the last week and those publications that have been rescinded.

### Development Status of Army Doctrine Reference Publications

Listed below are selected Army doctrine reference publications (ADRs) and their development status as of 1 July 2013:

ADRP 1	<i>The Army Profession</i>	Published
ADRP 1-02	<i>Operational Terms and Military Symbols</i>	Revision Development
ADRP 3-28	<i>Defense Support of Civil Authorities</i>	Published

### Development Status of Field Manuals

Listed below are the Doctrine 2015 FMs and their development status as of 1 July 2013:

FM 1-0	<i>Human Resources Support</i>	Final draft staffing
FM 1-04	<i>Legal Support to the Operational Army</i>	Published
FM 1-05	<i>Religious Support</i>	Published
FM 1-06	<i>Financial Management Operations</i>	Initial draft development
FM 2-0	<i>Intelligence Operations</i>	Signature draft development
FM 2-22.3*	<i>Human Intelligence Collector Operations</i>	Exempt from Doctrine 2015
FM 3-01	<i>Air and Missile Defense Operations</i>	Signature draft development
FM 3-04	<i>Aviation Operations</i>	Final draft development
FM 3-05	<i>Army Special Operations</i>	Final draft development
FM 3-07	<i>Stability Operations</i>	Initial draft staffing
FM 3-09	<i>Field Artillery Operations</i>	Signature draft development

FM 3-11*	<i>Multi-Service Doctrine for Chemical, Biological, Radiological, and Nuclear Operations</i>	Exempt from Doctrine 2015
FM 3-13	<i>Inform and Influence Activities</i>	Published
FM 3-14	<i>Army Space Operations</i>	Initial draft development
FM 3-16	<i>The Army in Multinational Operations</i>	Final draft development
FM 3-18	<i>Special Forces Operations</i>	Program directive staffing
FM 3-22	<i>Army Support to Security Cooperation</i>	Published
FM 3-24	<i>Insurgencies and Countering Insurgencies</i>	Initial draft development
FM 3-27	<i>Army Global Ballistic Missile Defense Operations</i>	Final draft development
FM 3-34	<i>Engineer Operations</i>	Signature draft development
FM 3-38	<i>Cyber Electromagnetic Activities</i>	Signature draft development
FM 3-39	<i>Military Police Operations</i>	Final electronic file development
FM 3-50	<i>Personnel Recovery</i>	Final draft development
FM 3-52	<i>Airspace Control</i>	Published
FM 3-53	<i>Military Information Support Operations</i>	Published
FM 3-55	<i>Information Collection</i>	Published
FM 3-57	<i>Civil Affairs</i>	Signature draft development
FM 3-61	<i>Public Affairs Operations</i>	Signature draft development
FM 3-63	<i>Detainee Operations</i>	Signature draft development
FM 3-81	<i>Maneuver Enhancement Brigade</i>	Signature draft development
FM 3-90-1	<i>Offense and Defense Volume 1</i>	Change 1 published
FM 3-90-2	<i>Recon, Security and Tactical Enabling Tasks Volume 2</i>	Published
FM 3-94	<i>Division, Corps, and Theater Army Operations</i>	Initial draft development
FM 3-95	<i>Infantry Brigade Operations</i>	Final draft development
FM 3-96	<i>Armored Brigade Combat Team Operations</i>	Final draft development
FM 3-97	<i>Stryker Brigade Combat Team Operations</i>	Final draft development
FM 3-98	<i>Reconnaissance and Security Organizations</i>	Final draft development
FM 3-99	<i>Airborne and Air Assault Operations</i>	Signature draft development
FM 4-01	<i>Transportation</i>	Initial draft staffing
FM 4-02	<i>Army Health System</i>	At Army Publishing Directorate
FM 4-30	<i>Ordnance Operations</i>	Signature draft development
FM 4-40	<i>Quartermaster Operations</i>	Signature draft development
FM 4-95	<i>Logistics Operations</i>	Final draft staffing
FM 5-02	<i>Operational Environment</i>	Initial draft development
FM 6-0	<i>Commander and Staff Organization and Operations</i>	Signature draft development
FM 6-02	<i>Signal Operations</i>	Signature draft development
FM 6-27	<i>The Law of Land Warfare</i>	Initial draft development
FM 6-99	<i>Report and Message Formats</i>	Final electronic file development
FM 7-15	<i>Army Universal Task List</i>	Revision staffing
FM 7-22	<i>Army Physical Readiness Training</i>	Published

\* FM 2-22.3 and FM 3-11 are exempt from Doctrine 2015 timelines due to policy decisions.

## **Other Recently Published Publications**

Recently published Army Techniques Publications (ATPs) (listed by date of publication) include:

ATP 3-01.50	<i>Air Defense and Airspace Management (ADAM) Cell Operation</i>	5 April 2013
ATP 3-20.98	<i>Reconnaissance Platoon</i>	5 April 2013
ATP 4-0.6	<i>Techniques for Sustainment Information Systems Support</i>	5 April 2013
ATP 4-16	<i>Movement Control</i>	5 April 2013
ATP 3-55.12	<i>Multi-Service Tactics, Techniques, and Procedures for Combat Camera (COMCAM) Operations</i>	12 April 2013
ATP 4-02.46	<i>Army Health System Support to Detainee Operations</i>	12 April 2013
ATP 3-06.1	<i>Multi-Service Tactics, Techniques, and Procedures for Aviation Urban Operations</i>	19 April 2013
ATP 3-07.20	<i>Multi-Service Tactics, Techniques, and Procedures for Integrated Monetary Shaping Operations</i>	26 April 2013
ATP 3-11.42	<i>Multi-Service Tactics, Techniques, and Procedures for Installation Emergency Management</i>	26 April 2013
ATP 3-11.47	<i>Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Enhanced Response Force Package (CERFP) / Homeland Response Force (HRF) Operations</i>	26 April 2013
ATP 3-37.10	<i>Base Camps</i>	26 April 2013
ATP 1-05.03	<i>Religious Support and External Advisement</i>	3 May 2013
ATP 3-05.20	<i>Special Operations Intelligence</i>	3 May 2013
ATP 3-05.40	<i>Special Operations Sustainment</i>	3 May 2013
ATP 1-06.1	<i>Field Ordering Officer (FOO) and Pay Agent (PA) Operations</i>	10 May 2013
ATP 3-01.60	<i>Counter-Rocket, Artillery, and Mortar Operations</i>	10 May 2013
ATP 3-06.20	<i>Multi-Service Tactics, Techniques, and Procedures for Cordon and Search Operations</i>	10 May 2013
ATP 3-07.40	<i>Multi-Service Tactics, Techniques, and Procedures for Conducting Engagements and Employing Engagement Teams</i>	10 May 2013
ATP 4-02.5	<i>Casualty Care</i>	10 May 2013
ATP 4-12	<i>Army Container Operations</i>	10 May 2013
ATP 3-39.35	<i>Protective Services</i>	31 May 2013
ATP 4-35.1	<i>Techniques for Munitions Handlers</i>	31 May 2013
ATP 2-19.5	<i>Multifunctional Team</i>	14 June 2013
ATP 2-22.35	<i>Human Intelligence Debriefing Techniques (S//NF)</i>	14 June 2013

All published Army doctrinal publications are available online at <https://armypubs.us.army.mil/>.

Recently published doctrinal joint publications (JPs) (listed by date of publication) include:

JP 3-14	<i>Space Operations</i>	29 May 2013
JP 1-02	<i>Department of Defense Dictionary of Military and Associated Terms</i>	15 April 2013

All published joint doctrinal publications are available online: <http://www.dtic.mil/doctrine/doctrine/doctrine.htm>.

## Terminology Update

Table 1 lists significant new terms since Doctrine Update 2-13. A complete list of new, revised, and rescinded terms can be found at <https://www.milsuite.mil/book/docs/DOC-25269>

Doctrinal Term	Discussion/Rationale/New Definition	Terminologist Comments
Army Civilian Corps	The non-uniformed Department of the Army civilian members of the Army Profession	ADRP 1 establishes official definition (issue date 14 June 2013)
Army Ethic	The evolving set of laws, values, and beliefs, deeply embedded within the core of the Army culture and practiced by all members of the Army Profession to motivate and guide the appropriate conduct of individual members bound together in common moral purpose.	ADRP 1 establishes official definition (issue date 14 June 2013)
Army Profession	A unique vocation of experts certified in the design, generation, support, and ethical application of landpower, serving under civilian authority and entrusted to defend the Constitution and the rights and interests of the American people.	ADRP 1 establishes official definition (issue date 14 June 2013)
Army Professional	A member of the Army Profession who meets the Army's certification criteria of competence, character, and commitment.	ADRP 1 establishes official definition (issue date 14 June 2013)
certification	Verification and validation of an Army professional's competence, character, and commitment to fulfill responsibilities and perform assigned duties with discipline and to standard.	ADRP 1 establishes official definition (issue date 14 June 2013)
character	An Army professional's dedication and adherence to the Army Values and the profession's ethic as consistently and faithfully demonstrated in decisions and actions.	ADRP 1 establishes official definition (issue date 14 June 2013)
commitment	The resolve of Army professionals to contribute honorable service to the Nation, to perform their duties successfully with discipline and to standard, and to strive to successfully and ethically accomplish the mission despite adversity, obstacles, and challenges.	ADRP 1 establishes official definition (issue date 14 June 2013)
competence	An Army professional's demonstrated ability to perform his/her duties successfully and to accomplish the mission with discipline and to standard	ADRP 1 establishes official definition (issue date 14 June 2013)
definitive identification	The employment of multiple state-of-the-art, independent, established protocols and technologies by scientific experts in a nationally recognized laboratory to determine the unambiguous identity of a chemical, biological, radiological, and/or nuclear hazard with the highest level of confidence and degree of certainty necessary to support strategic-level decisions.	ATP 3-11.37 (issue date 25 March 2013)
field confirmatory identification	The employment of technologies with increased specificity and sensitivity by technical forces in a field environment to identify chemical, biological, radiological, and/or nuclear hazard with a moderate level of confidence and degree of certainty necessary to support follow-on tactical decisions	ATP 3-11.37 (issue date 25 March 2013)
flank attack	A form of offensive maneuver directed at the flank of an enemy.	FM 3-90-1 modifies term. (issue date 22 March 2013)
global engagement manager	Provides automated tools and decision aids that enable commanders to exercise mission command of ballistic missile defense forces deployed within the combatant command area of responsibility.	ATP 3-27.5 (issue date 22 March 2013)
military expertise	The design, generation, support, and ethical application of landpower, primarily in unified land operations, and all supporting capabilities essential to accomplish the mission in defense of the American people.	ADRP 1 establishes official definition (issue date 14 June 2013)
presumptive identification	The employment of technologies with limited specificity and sensitivity by general-purpose forces in a field environment to determine the presence of a chemical, biological, radiological, and/or nuclear hazard with a low level of confidence and degree of certainty necessary to support immediate tactical decisions.	ATP 3-11.37 (issue date 25 March 2013)
quick response force	(Army) A dedicated force on a base with adequate tactical mobility and fire support designated to defeat Level I and Level II threats and shape Level III threats until they can be defeated by a tactical combat force or other available response forces.	ATP 3-37.10 (issue date 26 April 2013)

Doctrinal Term	Discussion/Rationale/New Definition	Terminologist Comments
stewardship	(Army) A dedicated force on a base with adequate tactical mobility and fire support designated to defeat Level I and Level II threats and shape Level III threats until they can be defeated by a tactical combat force or other available response forces.	ADRP 1 establishes an Army unique official definition (issue date 14 June 2013)
theater validation identification	The employment of multiple independent, established protocols and technologies by scientific experts in the controlled environment of a fixed or mobile/transportable laboratory to characterize a chemical, biological, radiological, and/or nuclear hazard with a high level of confidence and degree of certainty necessary to support operational-level decisions	ATP 3-11.37 (issue date 25 March 2013)
token	An electronic identification method used within a multi-node configured command and control, battle management, and communications suite to identify the lead server for transmission of track data. The token may be transferred between suites to maintain positive integrity of track data. The suite where the token resides is the only suite that may make changes to the AN/TPY-2 (FBM) system configuration. The token methodology also applies within a single node command and control, battle management a, and communications suite, but the token remains within the single node.	ATP 3-27.5 (issue date 22 March 2013)

 TRADOC CULTURE CENTER  
**ONE STOP SHOP**  
FOR ALL THINGS CULTURE 

The TRADOC Culture Center (TCC) is your culture center and the Army's One-Stop-Shop for all things culture related. Service Members are the customer, and the TCC tailors products and training to meet the needs of the customer.

Smart Books : Smart Cards : Pocket Guides : Interactive Training : Videos

### Why is Culture Important?

Cross-cultural competency (3C) is a critical combat multiplier for commanders at all levels that enables successful mission accomplishment. Possessing cultural understanding is one of the critical components for Soldiers who interface with the local population. At a minimum, soldiers must possess cultural awareness. Leaders must demonstrate cultural understanding and be proficient in applying cultural knowledge effectively to achieve mission objectives. The TCC can help Soldiers gain this mission essential proficiency. Lessons learned from 10 years of operational deployments clearly indicate that 3C is a huge and indispensable combat multiplier.

### OVER 160,000 SERVICE MEMBERS TRAINED

The TCC supports Soldiers and leaders throughout the Army and other services in numerous ways. It conducts ARFORGEN/predeployment training for any contingency; trains culture trainers; and produces professional military education (over 160,000 military personnel trained since 2004). The TCC will create or tailor any products deploying units require.

The TCC has developed several distance learning products available for facilitated instruction or individual student use. As an example, two seasons of "Army 360" that the TCC produced contain 19 episodes of missions run in six countries. "Army 360" is an interactive media instruction (IMI) training product which meets the Army Learning Concept 2015 learner-centric requirements. The TCC is in the process of turning the "Army 360" IMI into digital apps which will be easily accessible for all Soldiers. The TCC produced an Initial Military Trainee (IMT) training product for the initial entry level Soldier called "IMT-BCT What is Culture?" We are also producing a BOLC IMI product. Both products are or will be available via the TCC website. The TCC is expanding other products into the apps arena as well as developing additional distance learning products to provide new 3C training and sustainment.

**REQUEST TRAINING NOW!**

at <https://ikn.army.mil/apps/G3MTT/>

Specify what the unit needs are and we will deliver training that fits your objectives.



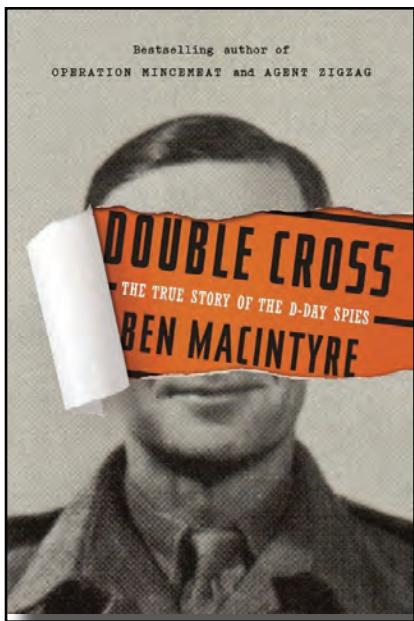
**DOWNLOAD TRAINING TO YOUR SMART PHONE:**  
<https://ikn.army.mil/apps/tccv2/>



The TCC produces cargo pocket-sized training products to include smart books and smart cards, as well as digital downloads for smart devices. Areas covered include Iraq, Afghanistan, North Korea, Democratic Republic of Congo, and more. Let us know what we can produce for you. For a complete list of materials, see:

<https://ikn.army.mil/apps/tccv2/>.

# Professional Reader



## Double Cross: The True Story of the D-Day Spies by Ben Macintyre

Crown Publishers, New York, 2012, 399 pages  
ISBN: 9780307888754

This book is about the use of double cross spies recruited by the British to spy against the Germans during World War II. A double cross spy is one who is recruited to spy on a particular country, but who is then persuaded by representatives of that country to spy on the country that first requested their services. In some cases such spies could be quite useful. During World War II a number of individuals were recruited by the Germans to spy on Britain, who then in turn, spied against Germany. This book is about some of these spies. The author notes that this particular group of double cross spies was "without question, one of the oddest military units assembled. They included a bisexual Peruvian playgirl, a tiny Polish fighter pilot, a mercurial Frenchwoman, a Serbian seducer,

and a deeply eccentric Spaniard with a diploma in chicken farming." (5) These double cross spies were motivated to help the British for a variety of reasons such as adventure, gain, patriotism, greed, and personal conviction. (358)

Although many attempts were made by the allies to fool the Germans about the invasion, this work focuses on one attempt—the providing of false information from these five double cross spies about the place of the invasion. The most obvious target of the allies for an invasion was Pas de Calais, the region nearest the British coast, and it was here that the Germans believed the invasion would take place which was understandable. Yet, it was at Pas de Calais that the allies wanted the Germans to believe that the invasion would take place. Hence, they plotted in a number of ways to confuse and deceive the Germans as to where the actual invasion would take place. The overall deception plan to fool the Germans was called "Bodyguard," but within this plan was a part called "Fortitude" which focused primarily on where the army of allies would be landing in Europe. (5)

In making "Fortitude" a success, the British officer in charge used the five double cross spies who are described in the book variously as courageous, treacherous, capricious, and inspiring. (258) Their goal was to convince the Germans that the invasion would not take place where it actually did occur. The author believes that this group of double cross spies was successful in achieving the goal. Implied in the book is that their use would have obvious advantages. It would shorten the war and save the lives of allied combatants because the Germans would not be as prepared for the invasion as they might have been. Had the Germans been correct in knowing when and where the invasion would take place, they could have deployed more of their military resources in a concerted effort to repel the invasion. This would undoubtedly cost more allied lives and seriously jeopardize the success of the allied invasion. If we learn anything from this book, it is that confusing the enemy even by the use of double cross spies can bring benefits to a country.

In writing this book the author used a number of sources such as documents, photographs, interviews and memories. Both German and British individuals were of help to him in this endeavor which made it one of the more interesting works about intelligence activities. \*

**William E. Kelly, PhD  
Auburn University**



# CONTACT AND ARTICLE Submission Information



*This is your magazine. 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 and exercises; 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. Propose changes, describe a new theory, or dispute an existing one. 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. Maximum length is 5,000 words.
- ◆ Be concise and maintain the active voice as much as possible.
- ◆ 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 re-publication upon request.

## **What we need from you:**

- ◆ **A release signed by your unit or organization's information and operations security officer/SSO stating that your article and any accompanying graphics and photos are unclassified, nonsensitive, and releasable in the public domain OR that the article and any accompanying graphics and photos are unclassified/FOUO (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.
- ◆ A Public Affairs or any other release your installation or unit/agency may require. Please include that release(s) with your submission.
- ◆ 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. Please indicate whether we can print your contact information, email address, and phone numbers with the biography.

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 [sterilla.smith@us.army.mil](mailto:sterilla.smith@us.army.mil). Our fax number is 520.538.1005. Submit articles by mail on disk to:

MIPB  
ATTN ATZS-CDI-DM (Smith)  
U.S. Army Intelligence Center of Excellence  
Box 2001, Bldg. 51005  
Fort Huachuca, AZ 85613-7002

Contact phone numbers: Commercial 520.538.0956  
DSN 879.0956.

# The Military Intelligence Corps 2013 Hall of Fame



**CSM (R) Franklin Saunders**



**Brevet BG George Sharpe  
(Deceased)**



**COL (R) William (Jerry) Tait**



**Mr. Robert Winchester**

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

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

**PIN: 103557**