

# MILITARY INTELLIGENCE

PB 34-04-2

Volume 30 Number 2

April-June 2004



## STAFF:

### Commanding General

Major General James A. Marks

### Deputy Commandant for Training

Jerry V. Proctor

### Deputy Commandant for Futures

Colonel Jack W. Russell

### Director/Dean of Training Development and Support

Russell W. Watson, Ph.D.

### Chief, Doctrine Division

Stephen B. Leeder

### Managing Editor

Sterilla A. Smith

### Editor

Elizabeth A. McGovern

### Design Director and Administration

Specialist Misty L. Bolaños

### Cover Design:

Specialist Misty L. Bolaños

**Purpose:** The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) publishes the *Military Intelligence Professional Bulletin* quarterly under provisions of AR 25-30. *MIPB* disseminates material designed to enhance individuals' knowledge of past, current, and emerging concepts, doctrine, material, training, and professional developments in the MI Corps.

**Subscription:** Subscription rates are \$21.00 (Domestic, APO, and FPO) and \$29.40 (Foreign). For information on subscriptions, see page 71.

**Disclaimer:** This publication presents professional information, but the views expressed herein are those of the authors, not the Department of Defense or its elements. The content does not necessarily reflect the official U.S. Army position and does not change or supersede any information in other U.S. Army publications. We reserve the right to edit any submitted material.

**Contact Information** for *MIPB* is on page 72.

## FEATURES

- 4 **Farewell Thoughts from Major General James A. Marks**  
by Major General James A. Marks
- 9 **Office of the Chief of Military Intelligence**  
by Lieutenant Colonel Harvey L. Crockett
- 10 **Upcoming Changes in MI Occupational Specialties**  
by Walter J. Crossman
- 12 **Overview of MI Initial Entry Training Courses Taught By the 309th MI Battalion**  
by George Stemler
- 16 **Geographic Information Systems (GIS) As Assured Mobility Enablers**  
by Major John H. Haefner
- 21 **An Open-Source Overview of the Technical Intelligence Collection Threat in Asia**  
by Sergeant First Class Wade C. Wilson
- 25 **Operation Shadow Guam**  
by First Lieutenant Catharine T. Wentz, First Lieutenant Dan Ma, and Second Lieutenant Kelley Calene Woods
- 29 **The Reserve Component Military Intelligence Linguist: A Historical Perspective on a Multicapable Asset**  
by Lieutenant Colonel Jeffrey F. Mitchell, UT ARNG
- 33 **Excess Reporting—CI and HUMINT Collectors Hand off Issues**  
by Master Sergeant Lisa A. Connors
- 35 **Lessons Learned From OIF: An SF Battalion S2's Perspective**  
by Captain Brian Gellman
- 43 **The Intelligence and Electronic Warfare Tactical Proficiency Trainer—A Capability That Is Long Overdue**  
by Paul Menoher (Lieutenant General, U.S. Army, Retired) and Roger McNicholas
- 48 **The Postgraduate Intelligence Program for Reserves: A Ten-Year Milestone**  
by Colonel Mark A. Jensen, USAR

2	Always Out Front	58	TSM Notes
3	CSM Forum	60	Professional Reader
50	CSA's Focus Area 16: Actionable Intelligence	64	MI Corps Hall of Fame
52	Doctrine Corner	70	Sly Fox Notes
55	Letter to the Editor	72	Contact Information
56	Proponent Notes		Inside Back Cover 300th MI Brigade (Linguist)

By order of the Secretary of the Army:  
Official:

JOEL B. HUDSON  
Administrative Assistant to the  
Secretary of the Army  
0413101

PETER J. SCHOOOMAKER  
General, United States Army  
Chief of Staff

# Always Out Front

by Major General James A. Marks

Commander, U.S. Army Military Intelligence Center and Fort Huachuca

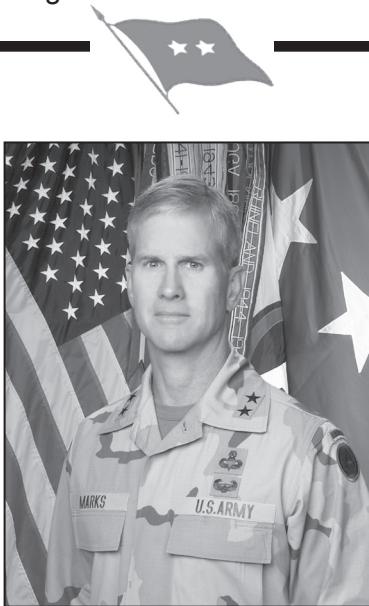


This is my last opportunity to speak to the field as your Commanding General and Chief of the MI Corps. What an incredible three years in command! I assumed command on 9/11, went to war as the CFLCC/CJTF-7 C2, and then resumed my duties as the Commanding General, USAIC & FH. No one could design a better, more fulfilling way to complete service to the nation.

As I quickly approach my retirement date from active duty, I am filled with both pride in our Army and gratitude to the fantastic soldiers, leaders, and teammates I have had the privilege to "soldier with" throughout my career. My career was continually enriched thanks to the hard work and outstanding character of countless true American heroes. Today, I owe thanks to the entire MI Corps that is soldiering tirelessly to support the Nation and Army at War.

Ours is an Army at War. The Global War on Terrorism (GWOT) will redefine our culture and the way we organize, equip, train, and fight. Much as the Cold War shaped our Army over the past 50 years, the GWOT will do the same in the coming decades. This will be your calling, to resolve that our Army will be as it has been for over 200 years: unmatched physically, intellectually, and morally.

The intelligence team that contributes to and leads our Army must continue the tradition of excellence and sacri-



fice. You will. There is no question; you will.

Remember, our team is a team of soldiers, other service members on the Joint team, civilians, and contractors. They must be enabled, certainly, by the best technology our nation can provide. But never forget the soldier on the ground. It is he and she who provide the leadership, drive, and focus that push our enablers to do what we demand of them. It is the soldier who shows the way, understands the commander's intent, translates that intent into action, and answers the call. It is the soldier. It's all about the soldier. Soldiers are not in the Army; they are the Army.

Over the 30 years I have been in uniform, soldiers taught me lessons, all sorts of lessons. These were not lessons just simply applicable to life as a soldier; these were life's lessons, lessons that guide me today as a husband, father, brother, friend. As I fold my BDUs and store them away, let me share for a final time the thoughts of soldiers who shaped me as a soldier. The legacy of service lives in them and their lessons continue to guide all of us into the future. Pass these lessons along. You are a link in the chain of selfless service.

Using these essential lessons, I urge everyone to drive on in your mission to defend our nation and its interests and to take the fight to our enemies. In the October-December 2001 issue of **MIPB**, not long after those dark hours on 11 September, I issued a call to recommit ourselves to our profession. I issue that challenge again today. We are all members of a critical team. Keep your head up. Take pride and responsibility for what you do and when the commander needs intelligence support, tell him—

## I GOT IT!

**Soldier's Lessons . . . Pass them along**

*Take the job, not yourself, seriously.*

*Disagreement is not disrespect or disloyalty.*

*Always consider the little guy first.*

*Be visible, sensitive, compassionate . . . and hard as nails.*

*Be a good listener, . . . squint with your ears.*

*Talk up your soldiers to their buddies and their boss.*

*Challenge every assumption. Be innovative.*

*Inspect something daily.*

*Own the mission . . . give orders in your name.*

*Never look the other way—take immediate corrective action.*

*Smoke those of low integrity.*

*Explain to soldiers what they are about to do and why.*

*Underwrite mistakes and risk taking. Risk management—always.*

*Live a disciplined life.*

*Experience the soldier's hardships.*

*Have a love affair with the Army—be enthusiastic!*

*"In the wake of the recent tragedy, I call on all intelligence personnel—military, civilian, and contractor—to recommit themselves to our profession. We witnessed a reminder of the importance of what we do and why we do it. An awesome responsibility to shoulder, this is a burden we can bear together. Although we must look inside and consider our roles in this endeavor, we can rest assured that we have a vast store of corporate strength within our great Army institution."*

# CSM Forum

by Command Sergeant Major Lawrence J. Haubrich  
U.S. Army Military Intelligence Corps



As you all know, this past March we held our 2004 Worldwide Command Sergeants Major/Sergeants Major (CSM/SGM) Military Intelligence (MI) Conference here at Fort Huachuca, Arizona. Once again, the conference was a great success and provided much to our Military Intelligence community.

In conjunction with our conference, the MI Corps presents the CSM(R) Doug Russell Award annually to recognize a soldier for significant contributions to Military Intelligence. This year's selection board considered eleven very professional and competitive soldiers who, without exception, have all been decisively engaged in the Global War on Terrorism (GWOT). Many of these soldiers have deployed to forward areas and several remain forward with their respective units at the present time. This year's selection board had the very difficult task of reviewing the packets of soldiers who stand in the very forefront of their respective formations and represent the very best of our Military Intelligence Corps.

The 2004 Doug Russell Award winner is Specialist Daniel R. Sheldon, an Intelligence Analyst at the MI Detachment, 75th Ranger Regiment, Fort Benning, Georgia. SPC Sheldon's deployments in support of current real world operations include a deployment to Iraq in support of Operation IRAQI FREEDOM as well as two past deployments to Afghanistan supporting Operation ENDURING FREEDOM (OEF). He has deployed for a third time to OEF. Our congratulations go to SPC Sheldon as the fourth Annual Doug Russell Award recipient.

SPC Sheldon is an excellent example of the type of soldier for whom the award committee was looking....To win, it takes a soldier who distinguishes himself within the Military Intelligence community as well as one who has demonstrated professionalism in his or her military occupational specialty.

In January, I attended the Sergeants Major Academy (SMA) Nominative CSMs Conference at Fort



Bliss, Texas; more than 225 CSMs representing the top major commands throughout the Army attended. This year's guest speaker was the Chief of Staff of the Army, General Peter J. Schoomaker, who provided a briefing on his vision for the Army over the next ten years and talked about the emphasis all non-commissioned officers should place on the Warrior Ethos. Much of what he said is in **The Way Ahead: Our Army at War...Relevant and Ready** document that is available online at <http://www.army.mil/thewayahead>.

Other presentations at the SMA Conference were by Headquarters, Department of the Army and other agencies ranging from the Army G1, G3, and G4, to the Chief of Army Reserve and Director of Army National Guard. Breakout groups discussed significant Army issues and briefed their conclusions back to all in attendance. I encourage all to log on the Army Web Page and check out this year's SMA Nominative CSM Conference briefs and topics of discussion.

During the past few months, as always, I had the opportunity to travel and visit our great MI soldiers in your formations and attended some additional conferences. I traveled to Utah and attended the 300th MI Brigade (Linguist) Language Conference and again met with the great soldiers assigned to the Brigade. I also visited Guantanamo Bay, Cuba, or GITMO, the Military Intelligence Readiness Command (MIRC), the Southeast Army Reserve Intelligence Support Center (ARISC), and the 221st MI Battalion (Technical Exploitation Battalion) at Fort Gillem, Georgia. As always, our Military Intelligence warriors are doing great things in support of the GWOT. I personally thank each and every one of you for what you all do as MI professionals and warriors. Let's take care of each other, our soldiers, and our families. You train hard, you die hard; you train easy, you die easy. Peace needs protection.

**ALWAYS OUT FRONT!**

# *Farewell Thoughts from Major General*

## *James A. Marks*

Photographs Courtesy of SPC Natalie Butler.



MG Marks, as C2, CFLCC, during Operation IRAQI FREEDOM, with Commander, CFLCC, Lieutenant General McKiernan and Command Sergeant Major (CSM), CFLCC, CSM Sparks, outside Najaf, Iraq on 23 March 2003.

Major General James A. Marks was commissioned 4 June 1975 into Military Intelligence upon graduation from the United States Military Academy. During his 29 years of commissioned service, MG Marks has held command and staff intelligence assignments including: Company Commander, 1st Battalion, 503d Infantry Regiment, 101st Airborne Division (Air Assault), Fort Campbell, Kentucky; Aide de Camp, Commander in Chief, US Pacific Command, Camp Smith, Hawaii; S3, 319th Military Intelligence Battalion (Airborne), 525th Military Intelligence Brigade, XVIII (Airborne) Corps, Fort Bragg, North Carolina; Executive Officer, 313th Military Intelligence Battalion (Airborne), 82d Airborne Division, Fort Bragg, North Carolina; Commander, 107th Military Intelligence Battalion, 7th Infantry Division (Light), Fort Ord, California; G2, 6th Infantry Division (Light), Fort Wainwright, Alaska; Special Assistant to the Chief of Staff of the Army; Commander, 504th Military Intelligence Brigade III Corps, Fort Hood, Texas; Deputy Chief of Staff, Intelligence, Headquarters, US Army, Europe and Seventh Army, Heidelberg, Germany; Executive Officer to the Commanding General, Stabilization Force, Sarajevo, Bosnia; Assistant Chief of Staff, J2 (Intelligence), United States Forces, Korea, and Deputy Chief of Staff, C2, Combined Forces Command; Commander, United States Army Intelligence Center and Fort Huachuca (USAIC&FH); deployed as C2, Coalition Forces Land Component Command during Operation IRAQI FREEDOM; and resumed Command of USAIC&FH. He is an Honor Graduate of the US Army Ranger School, a Master Parachutist, Air Assault qualified, and authorized to wear the Canadian and Republic of Korea Airborne wings.

MG Marks holds a Master of Arts degree in International Relations from the University of Virginia and a Master of Science degree in Theater Operations from the School of Advanced Military Studies. He is a graduate of the Military Intelligence Officers' Advance Course, the United States Army Command and General Staff College, the School of Advanced Military Studies, and the Army War College.

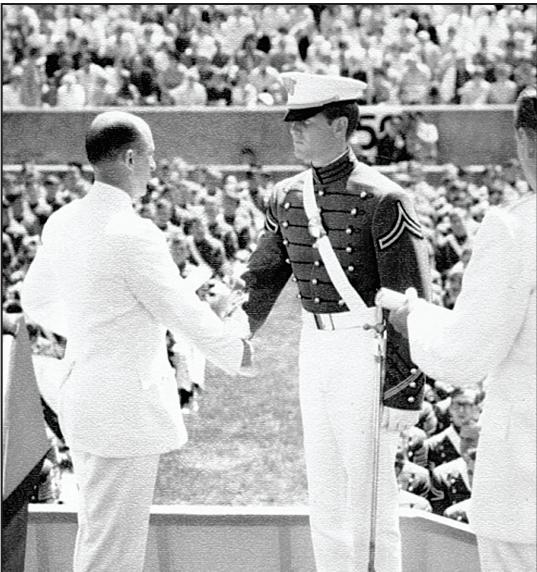
His awards and decorations include: the Distinguished Service Medal, Defense Superior Service Medal, Legion of Merit with one Oak Leaf Cluster, Bronze Star, Defense Meritorious Service Medal, Meritorious Service Medal with four Oak Leaf Clusters, Army Commendation Medal, Army Achievement Medal with one Oak Leaf Cluster, Armed Forces Expeditionary Medal, Global War on Terrorism Expeditionary and Service Medals, Korean Defense Service Medal, and the North Atlantic Treaty Organization (NATO) Medal.

MG Marks graciously provided his comments on highlights of his three-year command here at Fort Huachuca, as well as his thoughts and advice on a number of issues of importance to him and the school during his official exit interview for the USAIC History Program on 5 May 2004. He was interviewed by Ms. Katharine W. Schmidli.

---

### **Q: To begin this interview, would you please describe your personal philosophy of leadership and command?**

*Focusing most directly on the leadership aspects: I'd like to think that I am a leader with a personal touch. I am very interested in the soldier as an individual. I am extremely interested in his and her personal as well as professional growth. You can't have one without the other. There must be a balance of both. Balance is open-ended; there is no template. It is a personal and professional definition that each individual leader needs to make sure he or she can achieve, can live, can demonstrate, and then can demand from his or her subordinates and those around him or her.*



Cadet Marks graduating from West Point on 4 June 1975.

**Q: Sir, you hit the ground running on September 11th 2001 when you took command. What modifications did your initial vision for the Intelligence Center and School undergo after this event?**

*My assignments were primarily as a tactical soldier in multiple divisions, both as an infantryman and an intelligence professional. In addition to the tactical assignments, I had the opportunity to serve at the joint level and on the Department of the Army's staff. My experiences were broad enough, but more deep in terms of my tactical experiences and perspectives in the application of intelligence. So I crafted my vision for the Intelligence Center and School to make sure that we could reinforce those soldier intelligence skills at the very lowest levels of engagement; but making sure we educated all of our soldiers as to what was available throughout the "Mud-to-Space" construct of leveraging all intelligence capabilities at the tactical through strategic levels.*

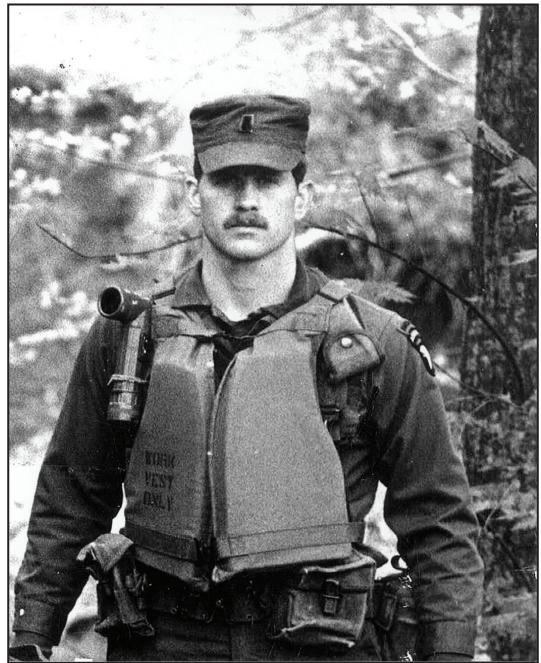
*But when you take command on 9/11, you tear that vision up when you suddenly realize that we are now a nation at war. Soldiers are going to be deployed. My vision shifted as we realized there would be an inevitable increase in the number of intelligence soldiers coming through the school. We have seen that. We have gone from 11,000 students trained during the course of a year to around 15,000. We are on a steady incline in terms of the demands our nation has put and will continue to put upon us as intelligence professionals.*

*Maintaining relevance with the field became even more critical. The only way we could do that was to send soldiers to the field, send mobile training teams to the field and stay connected to the field in multiple and redundant ways so I would know what the field commanders and intelligence professionals needed from us.*

**Q: You deployed to Camp Doha, Kuwait, in September 2002 where you joined the CFLCC and remained with the team during the race to Baghdad, returning to the School in June 2003. Could you tell us about your role in Operation IRAQI FREEDOM and any observations based upon your experiences during your deployment?**

*I was the C2, the senior intelligence officer for the CFLCC which was formed out of the Third US Army. The intelligence professionals that I was blessed to work with demonstrated professionalism and the moral and physical courage that you would expect from the young Americans we are raising.*

*We made some modifications when I came back here to USAIC in terms of how we train these professionals. Primarily we stressed the concept of "fighting Intelligence Surveillance and Reconnaissance." "Fighting ISR" goes beyond collection management and those traditional collection manage-*



1LT Marks, 101st Air Assault Division in 1976.



Jumpmaster MAJ Marks, 82d Airborne Division in 1987.

ment terms and tactics, techniques, and procedures (TTPs). It is an approach toward taking those intelligence capabilities that are a part of our formations and those that are external to our organic formations, demanding the most of those capabilities and leveraging every aspect of them at all times. It's a mind set; it's TTPs that must be imbued in our intelligence professionals from noncommissioned officers all the way through our very senior intelligence officers.

*At the end of the day, warfighting is all about execution superiority. That is based upon decision superiority, and decision superiority is based upon information and knowledge superiority. The commander must be comfortable, within the bounds of comfort and assumption of risk, that he has the best intelligence available so that he can make good solid decisions.*

*Once those decisions are made, we move into execution superiority. You have got to execute a program across the entire spectrum. That goes from building a church or a school to providing security to dropping kinetic weapons systems and trying to kill as many bad guys as you can very precisely and aggressively. Information superiority leads to knowledge superiority which leads to decision superiority which leads to execution Superiority. We*

*always knew that. But it has been revalidated and reconfirms how we train here; we have made some tweaks. When you look at each of the Military Occupational Specialties (MOS), you can see some TTPs that have been modified based on our common experiences. I won't go into detail, but suffice it to say we are taking that experience from the field and bringing it back to the school.*

*Let me tell you that interagency cooperation has never been finer. Those are all the agencies that contribute to the fight when we talk about the high end of "Mud to Space"—the Central Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, and the Defense Intelligence Agency. All of those agencies contribute immediately to what is going on, on the ground. They help create that environment where a commander can make good solid decisions. But none of this happens in a vacuum. It happens because intelligence professionals fuse information in a very timely manner.*

**Q: There are changes coming to Military Intelligence (MI) as a result of the Chief of Staff of the Army's decision to move quickly towards a future force structure. What do you see as some of the challenges facing the MI Corps as the Task Force Modularity decisions begin to be implemented?**

*Let me re-phrase your question. I don't see them as "MI challenges," I see "MI opportunities." There are increasing demands on our intelligence pro-*



COL Marks, Commander, 504th MI Brigade.

fessionals at all levels. They aren't challenges but opportunities to do what is demanded of us. We are so blessed to be alive today, during this time, so that we can make these contributions. To be in uniform, to be United States Army intelligence professionals, is a magnificent opportunity.



Running with the 501st MI Brigade, 2 April 2004, Camp Humphreys, Korea.

going to be, so we can be predictive, so we can get ahead of him. We don't want to react, we want the enemy to react, we want to shape.

The opportunities are immense. We are going to have intelligence professionals in brigade-like Units of Action which will have some division capabilities. We are going to have intelligence professionals at the division level with corps-like capabilities embedded in them. We are taking some of the greatest capabilities we have in our Army and we are shoving them down, for lack of a better verb, to the lowest levels of engagement on the ground where we can really make a difference. The leveraging capabilities of what is out there in terms of intelligence have got to be present all the way down to brigade level. We are doing that today.

With the advent of these units, the number of intelligence professionals will increase. Those command opportunities are essential because our Army has a culture of command. But the toughest job an intelligence professional has ever had is that of staff "2", being the senior intelligence officer at any of these levels. That's a staff job. But if you take the point I made about "fighting ISR" and you pull that into a staff position, what you will see are staff officers who are going to have command-like responsibilities—not authorities, but responsibilities to leverage across the intelligence community throughout the entire spectrum, "Mud-to-Space," and enabling that tactical formation, or any formation with those capabilities. It is much more important to focus on what is core to our business, and that is being an intelligence professional at all levels. We have to know what is available at the agency levels. But we also have to understand that the essence of our business is at the tactical level of engagement. We have never for-

Having said that, there are some very specific things that the Army is going to ask us to do in the joint construct. We don't fight as an army; we fight as a joint team. We have got to leverage the Air Force, the Marines, the Navy, the Coast Guard, and the National agencies. Everyone contributes. Our job is to fuse it and make sure it gets to the right commander at the right time, in a very timely manner. If there is a latency in anything we do, we are asleep at the switch.

We have to be aggressive in leveraging all of these contributors. How we fight demands it. This includes the soldier on the ground. That young soldier has intelligence that we have got to go

get if we are painting a picture of the enemy, his intentions, his actions, and where we think he is

going to be, so we can be predictive, so we can get ahead of him. We don't want to react, we want the enemy to react, we want to shape.



MG Marks as J2, US Forces, Korea, in a parade.

*gotten that and we have never abandoned that. We have got to continue to hammer that into our young intelligence professionals. So it is more than just increased command opportunities, it is about being the senior intelligence officer at all levels.*

**Q: Of the opportunities that remain, which do you see as systemic to how the Army operates as a whole and what are your ideas to address these challenges?**

*First and foremost, I will tell you that the intelligence team will be embedded at the very lowest levels of engagement. That's point one. And that intelligence professional is a part of the team just like the infantryman or the artilleryman. The senior intelligence officer, at any level, must be part of the team. The tactical commander on the ground needs to make sure he uses the intelligence professional team to train the aggregate that makes up his formation. For instance, the intelligence team can be of particular value during stability operations. Soldiers must be the sensors on the ground; they must have some tactical questioning skills. They must have a sense of their environment; using the information acquired in one location to gain a sense of what type of application of force may be required in another part of the environment.*

*The intelligence training plan that takes place at the lowest levels of engagement must include the fingerprint of the commander. Gone are the days when the commander looks at the intelligence officer and says, "You know, you are as screwed up as anything I have ever seen. Get your act together!" It's not being an apologist anymore. It's not looking at the commander and saying, "Sir, I'm sorry, I screwed that up. I'll get my act together. I'm just the intel guy and I'll work as hard as I can."*

*It's saying, "Time out, Sir. I am a member of YOUR team. Let me help shape a training plan that has YOUR endorsement. You are the coach. How do you want me to work as part of the aggregate, to make you more enabled, more aggressive, more knowledgeable, more precise, more deadly? Whatever the demands are that you have operationally, I will enable as the intelligence guy. But I need your fingerprints on the training, because if I try to do it myself, there are a thousand reasons why guys won't participate, the primary reason being I can't task them. I lead an absolutely critical element of your team. Sir, put your fingerprints on this. I will shape it. We will get it done and there will not be any alibis."*

**Q: What advice would you give your successor?**

*This is a nation at war. We are not going to move away from being a nation at war anytime soon. In fact, what defined my generation of soldiers—we were defined culturally and doctrinally as an Army based on the Cold War. How we fought, how we equipped, how we trained, was based on that inevitable conflict we thought would occur on the plains of central Europe and potentially on the peninsula of Korea. We have gone through a redefinition of that over the course of the last 10 to 12 years since the wall came down in November of 1989 and Operation DESERT STORM. Over the last decade of the nineties, a lot of "brush fires" have occurred around the world.*

*This is a defining war that we are part of now; it is a cultural shift. It is not a brush fire, but a full-fledged engagement that is going to take every aspect of our leadership and our development and our intellectual might to make sure we stay ahead of.*

*My successor is coming in from Iraq. That is a defining experience in her life. Major General Fast will walk in here and will bring those great experiences, the currency with the field, an understanding of what are the true demands, and she will impart that knowledge across the training we conduct here. She will sustain and increase the connection with the field. I would just tell her very briefly, "Strap yourself in and be prepared for a very wild ride, because it's going to be more of what we've experienced during the course of the last three years."*



# OFFICE OF THE CHIEF OF MILITARY INTELLIGENCE

by Lieutenant Colonel Harvey L. Crockett

The purpose of this article is to clarify the duties and responsibilities of a very important but often misunderstood organization—the Office of the Chief of Military Intelligence, or OCMI. OCMI is located at the “Home of the Military Intelligence Corps,” Fort Huachuca, Arizona. While the name leads one to believe that this organization is responsible for all matters involving Military Intelligence (MI), the truth is that OCMI is responsible for the personnel area of the MI Proponent. The actual Chief of the MI Corps is the Commanding General, United States Army Intelligence Center and Fort Huachuca.

Traditionally, the Commanding General wears three hats: Commandant of the Army’s Military Intelligence Center, MI Corps Commander, and Chief of Military Intelligence, or more appropriately for this article, “the” MI Proponent. As the MI Proponent, the Commanding General enlists the help of the Personnel Propriety Office or OCMI to monitor promotions, recruitments or accessions, and retention within the MI force.

Each branch within the Army has a Personnel Proponent office. The mission and responsibilities of this office are explained in AR 600-3. There are eight major areas of personnel propriety responsibility: structure, acquisition, individual training and education, distribution, deployment, sustainment, professional development, and separation, all of which collectively manage the lifecycle of a soldier.

Within these areas of responsibility, OCMI—

- Manages the Officer and Warrant Officer lifecycles.
  - Partners with other parts of the MI Proponent such as Concepts, Doctrine, New Systems, Training, Structure, or Assignments.
- A critical recurring project for OCMI is the submittal of the Military Occupational Classification and Structure (MOCS) packets. At the direction of the CG, USAIC&FH, OCMI prepares yearly MOCS packets for submission to the Department of the Army (DA) Staff and Human Resources Command (HRC).
- The MOCS is the method used to document and submit changes to DA to create, merge, or delete an MOS. Each packet, on average, takes eight months to prepare. Once completed, each packet is staffed through local offices that manage Concept Development, Doctrine, Force Design and, of course, Training. After staffing, the packet is submitted to HRC no later than the fifteenth of May of that year. HRC reviews the packet and then vetts it through each Major Army Command (MACOM) and DA for review and concurrence or nonconcurrence. All must agree or the action is not approved.
- It is important to note that each MOCS action takes three years from submittal to effective date. Toward the end of the three-year process, Tables of Organization and Equipment (TOEs) and Tables of Distribution and Allowances (TDAs) are built or adjusted to reflect the changes. The changes resulting from this process usually take effect at the end of the three years in the month of October.
- The next article in this issue submitted by the Training Development and Integration Division, discusses in detail some of the more important changes that have resulted from the MOCS process.



*LTC Harvey L. Crockett is currently serving as the Director of the Office of the Chief of Military Intelligence.*

# Upcoming Changes in MI Occupational Specialties

by Walter J. Crossman

As a result of the decisions made in 2002 for Career Management Field (CMF) 98 and in 2003 for CMF 96 in the Department of the Army Military Occupational Classification and Structure process, there are some watershed changes in store for these CMFs. According to the schedule, Military Intelligence (MI) will implement these changes in October 2005 (fiscal year 2006 [FY 06]).

## Changes in CMF 98

Discussions regarding military occupational specialties (MOSs) 98C (Signals Intelligence Analyst), 98J (Electronic Intelligence [ELINT] Interceptor/Analyst), 98K (Signals Collection/Identification Analyst), and 98H (Communications Interceptor/Locator) began in the late 1990s when the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) began looking at intelligence MOSs with regard to modifications needed to address changes in the nature of the enemy, resource realities, and the specific needs of the warfighter. Concurrently, the Intelligence Center evaluated the 98 CMF for areas that could potentially merge based on similarities in knowledge and skill sets. As a result, the Army approved deletion of several MOSs, revision of one, and creation of two new MI MOSs. The 2002 CMF 98 Notification of Change (NOFC) outlined the outcome.

MI will delete MOSs 98J and 98K; the skills associated with them merge into other MOSs. The 98J operational ELINT skills and positions will transfer to the revised 98C MOS while the 98J technical ELINT skills and positions transfer to the newly created 98Y (Signals Collector/Analyst) MOS. All 98K skills and positions will be transferred to the new 98Y MOS as well.

MOS 98H converts to a skill qualification identifier (SQI) "A" and the skills and training required for this SQI remain the same as for the old MOS. All 98H positions will convert to either 98G (future title Cryptologic Interceptor/Locator) or 98Y.

MOS 98C will be revised to include the operational ELINT skills of the 98J. The ELINT skills will combine

with the existing 98C communications intelligence (COMINT) skills to create a true signals intelligence (SIGINT) analyst.

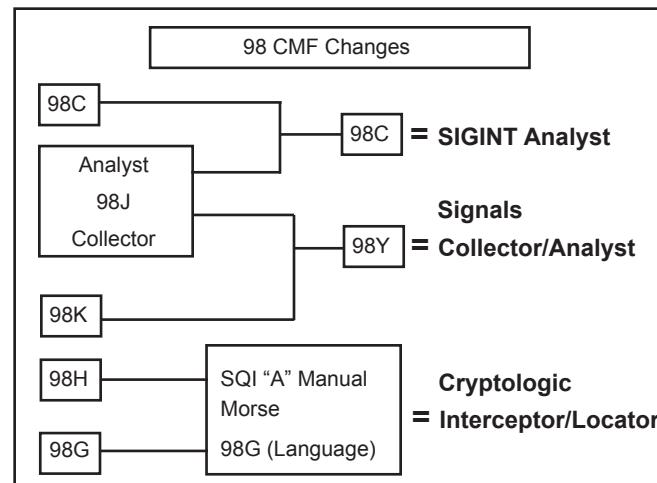


Figure 1. CMF 98 Changes in October 2005.

A new MOS, 98Y (Signals Collector/Analyst), will include 98J technical ELINT skills and 98K skills to create a broader signals collection MOS.

The other new MOS, 98P (Multi-Sensor Operator), was originally created to combine Prophet operator and tactical measurement and signatures intelligence (MASINT) sensor operator functions. Based on findings from Afghanistan and Iraq, the Army determined that MOS 98G was better suited as the Prophet Operator so 98P (Multi-Sensor Operator) will now become the future MI MASINT MOS. Specific knowledge and skill sets for this MOS will be developed by Fort Huachuca training developers in coordination with the U.S. Army Intelligence and Security Command (INSCOM).

Both 98C and 98Y Initial Entry Training and Transitional Training Course requirements are under revision in a combined effort by USAIC&FH, Goodfellow Air Force Base in Pensacola, INSCOM, and the National Security Agency (NSA). Figure 1 provides a graphic representation of the CMF 98 changes.

## CMF 96 Changes

The major changes in this CMF will occur in MOS 97E (Human Intelligence [HUMINT] Collector) and

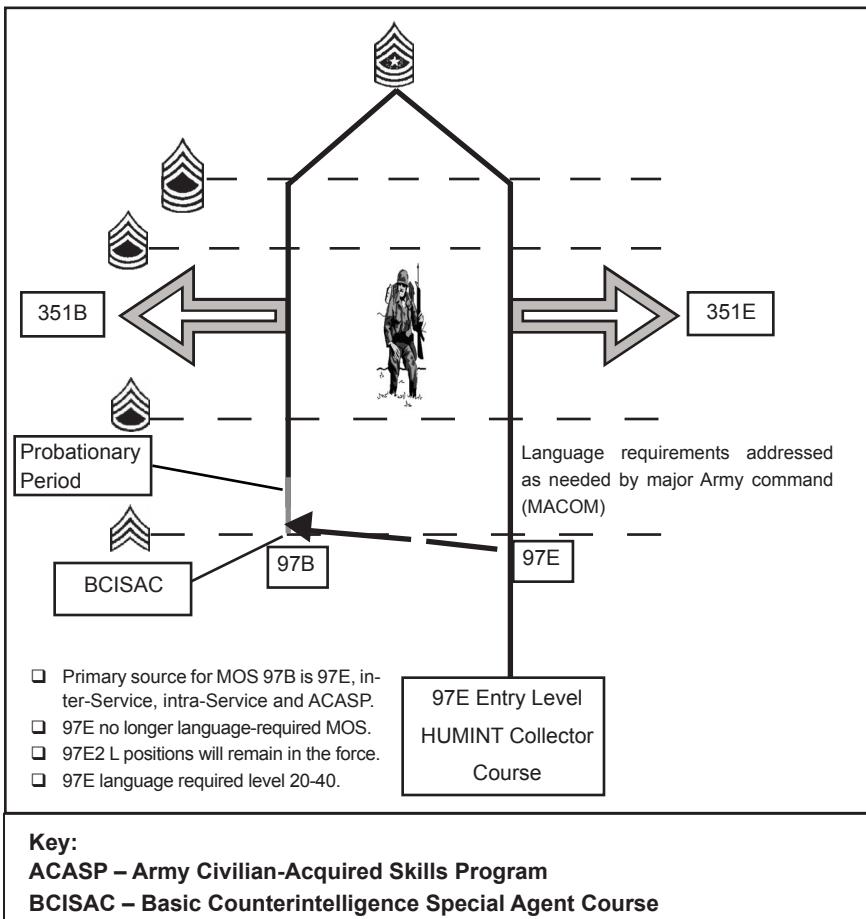


Figure 2. CI and HUMINT MOS Model.

97B (Counterintelligence [CI] Agent). The driving force behind these changes was the findings and recommendations from the CI/HUMINT Integrated Concept Team (ICT) and field observations on how units were employing skill level 1 (SL-1) 97E and 97B soldiers. Additionally, the ICT scrutinized the traditionally low retention rates of SL-1 97E soldiers and the use of a 97E10 soldier's language skills.

Major changes on the horizon for both MOSs include the elimination of the SL-1 language requirement for 97E and the transfer of selected SL-1 skills from MOS

97B to 97E. MI will eliminate the SL-1 entry level for MOS 97B; it will become a SL-2 entry MOS with the primary recruiting path being MOS 97E.

The implementation of these recommendations will facilitate more efficient use of language-training resources, a more focused Counterintelligence course, and the ability to get SL-1 97E soldiers to the field in a timely manner. Figure 2 shows the effect of these changes in CMF 96.

## Additional Thoughts

As the October 2005 implementation date for these MOS changes approaches, all MI leaders, both military and civilian, should become familiar with the implications of these dramatic changes. This will allow them to answer questions from their soldiers and provide guidance. For personnel related issues and questions about enlisted positions, the best point of contact is Sergeant Major Mitchell, Office of the Chief of Military Intelligence (OCMI), at E-mail

maurice.mitchell@hua.army.mil and by telephone at (520) 533-1174 or DSN 821-1174. For training-related issues, please contact the author via E-mail (see below) and telephonically at (520) 533-4644 or DSN 821-4644.



*Walter Crossman (Sergeant Major, U.S. Army, Retired) is the Chief of Enlisted Course Development at Fort Huachuca, Arizona. Readers may contact the author via E-mail at [walter.crossman@us.army.mil](mailto:walter.crossman@us.army.mil).*

## Suggestions or Comments

**MIPB** disseminates material designed to enhance individuals' knowledge of past, current, and emerging concepts, doctrine, material, training, and professional developments in the MI Corps. If you have comments, critiques, questions, and/or suggestions on how we might improve any aspect of this publication, please contact us. You can write to us directly at ATTN ATZS-FDT-M, U.S. Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017, or E-mail us at [mipp@hua.army.mil](mailto:mipp@hua.army.mil).

# Overview of MI Initial Entry Training Courses Taught By the 309th MI Battalion

by George Stemler

*Army Intelligence and the greater intelligence community need to change to fight the Global War on Terror. What we did before 9/11 no longer works. We need to change how we think, and the processes we use, to produce intelligence. It is imperative we do so, not only to prevent another 9/11, but also to take the fight to the terrorists.*

This passage is from the February 2004 Army G2 Notes to the Field , by Lieutenant General Keith B. Alexander, Deputy Chief of Staff (DCS) G2, U.S.



SSGs Crawford Clark and Jaime Garcia, 309th MI Battalion instructors, move unit icons on the map board as they lead 96B students through a tactics review. The map board the instructors are standing on was created by National Geospatial-Intelligence Agency (NGA).

Army. LTG Alexander's comment reflects a philosophy the 309th MI Battalion tries to incorporate into every course we teach at Fort Huachuca, Arizona.

There is no doubt that the Global War on Terrorism (GWOT) has placed increased demands on Military Intelligence (MI) personnel throughout the U.S. Army. The increased operational tempo of an army at war has placed unique demands upon personnel assigned to the 309th Military Intelligence Battalion.

The 309th MI Battalion is responsible for training in excess of 2,000 MI initial entry training (IET) soldiers in five MI military occupational specialties (MOSSs) annually. These MOSSs include: 96B (Intelligence Analyst), 96R (Ground Surveillance Systems Operator), 97B (Counterintelligence (CI) Agent), 97E (Human Intelligence [HUMINT] Collector),

and 98H (Communication Locator/Interceptor.) Not included in the numbers above are more than 600 soldiers we train in our three functional courses: the Intelligence in Combating Terrorism (ICT) Course, the Prophet Operator Course (POC), and the CI and Force Protection Source Operations Course (CFSO).

Additionally, via numerous Mobile Training Teams (MTTs) in the last year, we have trained more than 3,000 soldiers who either have deployed or are preparing to deploy in support of the GWOT. While we know we are making a positive impact through our non-IET training, it is imperative that we constantly remind ourselves that IET is and will remain our number one priority. It is through IET soldiers that we rebuild the Army and the MI Corps every day—one soldier at a time.

The 309th MI Battalion is committed to graduating IET soldiers who can assimilate rapidly into their units of assignment, and immediately make positive contributions to the units' missions. In response to world events, 309th MI Battalion IET courses have made and are making fundamental program of instruction (POI) changes. The 309th training committees continually seek innovative ways to incorporate approved lessons learned from Operations IRAQI FREEDOM and ENDURING FREEDOM (OIF and OEF) into their course curricula. All 309th MI Battalion IET courses are designed to be hands-on performance or performance-based military occupational specialties (MOSSs) training, which includes the contemporary operating environment (COE) and Middle East cultural awareness (see Figure 1).

The following discussion provides a synopsis of each 309th MI Battalion IET course. These include the following courses: Intelligence Analyst, Ground Surveillance Operator, CI Agent, Human Intelligence (HUMINT) Collector, and Communication Locator/Interceptor.

## 243-96B10, Intelligence Analyst Course

**Course Scope.** The 96B10 Intelligence Analyst course is 16 weeks 3 days of hands-on performance

The 309th MI Battalion has inserted Middle East cultural awareness training throughout its IET courses, with emphasis on the countries of Iraq and Afghanistan. Students learn—

- General Middle East geography.
- Strategic Middle East geography.
- Middle East cultural geography.
- Middle Eastern tribalism.
- Islam in general.

**Figure 1. Middle East Cultural Awareness Training Provided to IET Students by the 309th MI Battalion.**

or performance-based training. The course comprises three academic phases: the basic, advanced, and automation phases. The course culminates in a comprehensive field training exercise (FTX) where students exercise all of the skills learned throughout the course.

Phase 1 is 26 days in length and is considered the basic 96B academic phase. Students learn basic skills including: military symbology, military map reading, using intelligence databases, and basic automation skills involving the All-Source Analysis System-Light (ASAS-L).

Phase 2 is the 28-day advanced academic phase in which students learn situational evaluation using intelligence preparation of the battlefield (IPB), enemy courses of action (ECOA) development, and collection management (CM), to support military decisions, and the production of intelligence to support the commander.

Phase 3 primarily focuses on automation training, and culminates in a four-day FTX. During Phase 3, students learn the functionality of the ASAS-L system. ASAS-L is the current intelligence fusion system, which provides automated intelligence analysis, battlefield visualization, management of intelligence and electronic warfare (IEW) resources, and production and dissemination of intelligence. Phase 3 culminates in an intensive four-day FTX.

Throughout the FTX, students work in a tactical operations center (TOC) environment, using all facets of the ASAS-L, their “go to war” automated all-source fusion system. This FTX makes extensive use of a COE-based scenario, while incorporating recently approved lessons learned from OIF and OEF. Students exercise all of the skills they have learned throughout the course, but in a time-sensitive FTX environ-

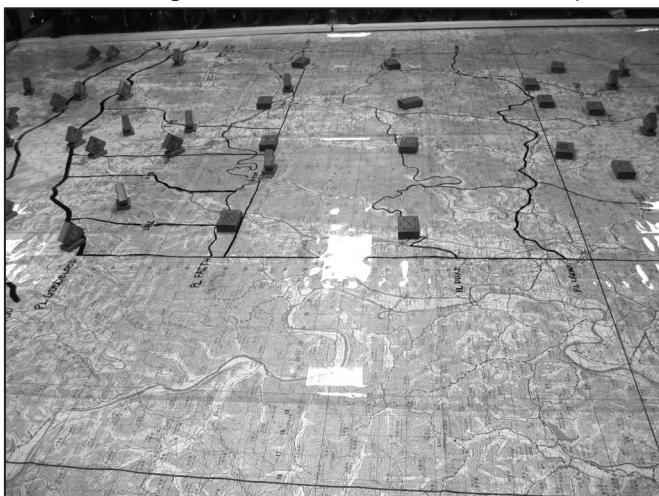
ment. The FTX is an IET requirement that completes the U.S. Army Training and Doctrine Command (TRADOC) mandated soldierization process.

**Future.** We project that student numbers will increase annually for the next few years providing numerous career opportunities for soldiers in MOS 96B. This MOS will continue to be regarded as MI’s “flagship” MOS for the projected future.

## **243-96R10, Ground Surveillance Operator Course**

**Course Scope.** Throughout the hands-on, performance-oriented, 5-week 4-day course, 96R students learn electrical safety procedures to measure direct current (DC) voltage; map reading; basic concepts of IEW; ground surveillance mission planning and reporting procedures; the Army maintenance management system; radio procedures; AN/PPS-5B/D Ground Surveillance Radar (GSR) set operation; combat operations in nuclear, biological, or chemical environments; and the emplacement and recovery of the Remotely Monitored Battlefield Sensor System (REMBASS). The 309th MI Battalion has scheduled REMBASS II system training in October 2004 pending final fielding of the system to the battalion.

Automation training within the 96R10 course primarily revolves around two systems, the AN/PPS-5B/D and the REMBASS systems. Students currently train with both the AN/PPS-5B and its replacement the AN/PPS-5D. The AN/PPS-5D has upgraded electronics while retaining the antenna, tripod, azimuth drive, and telescope assemblies of the AN/PPS-5B. The AN/PPS-5D is easily integrated into multisensor systems and is capable of interfacing with the REMBASS and Improved



**The map board is set up for a scenario.**

REMBASS, and is an easy transition from the old AN/PPS-5B. Once sufficient numbers of AN/PPS-5D systems are delivered to Fort Huachuca, the course will retire the AN/PPS-5B.

Students also learn to emplace and recover the REMBASS and I-REMBASS during the course. The basic purpose of REMBASS is to detect, locate, classify, and report personnel and vehicular (wheeled and tracked) activities in real-time within the area of deployment. REMBASS is a ground-based, all weather, day-and-night, battlefield surveillance, target development, and early warning system capable of remote operation under field conditions. Students use the REMBASS extensively during their three-day FTX.

The course culminates in a comprehensive three-day FTX where students exercise and receive evaluation on all of the skills they have learned throughout the course including the deployment and redeployment of the PPS-5B and REMBASS systems. This FTX is an IET requirement that will complete the TRADOC-mandated soldierization process.

**96R Future.** The future of the 96R MOS is unclear. Currently, the Army has a tactical requirement for the Ground Surveillance System (GSS) and Ground Surveillance Radar (GSR) skills on the battlefield. Therefore, the 96R may evolve into a new MOS 98P, which would emphasize tactical measurement and signatures intelligence (MASINT) collection skills while retaining the 96R's GSS/GSR skills.

## **244-97B10, CI Agent Course**

**Course Scope.** During the 17-week 4-day, hands-on, performance-based, CI Agent Course, 97B students learn a myriad of common CI subjects to include: military justice and intelligence law, threat vulnerability assessments, CI support to security programs, operations security (OPSEC) analysis, CI investigations, CI and HUMINT collection operations, CI special operations, force protection (FP), CI in combating terrorism, and various administrative duties associated with performing the CI mission.

Automation training in the 97B course revolves around the CI/HUMINT Information Management System (CHIMS) which is integrated throughout the course. CHIMS is designed to provide automation support for Army tactical CI and HUMINT collection, investigation, interrogation, document

exploitation, and FP requirements from battalion to echelons above corps (EAC). CHIMS provides CI and HUMINT personnel with the ability to process, analyze, and disseminate collected information of tactical relevance in a timely manner.

The course culminates in a comprehensive FTX conducted at the world-class tactical HUMINT training facility on Fort Huachuca. Throughout the five-day FTX, students participate in a training exercise using CHIMS to integrate and synchronize the collection of CI and HUMINT information in a COE-driven scenario. The FTX allows each 97B student to perform the CI skills learned during the core 97B course. The FTX is an IET requirement completing the TRADOC-mandated soldierization process.

**Future.** In fiscal year 2006 (FY06), the 97B course will expand to an 18-week 4-day all ranks (military and civilian) Basic Counterintelligence Agent Course and will no longer be an IET MOS course. All course training will be at skill level 20(+), and will focus on CI investigations and countering the intelligence threat and activities of our adversaries.

## **241-97E10, HUMINT Collector Course**

**Course Scope.** During the 16-week 3-day hands-on, performance-based 97E course, students are trained in the technical skills necessary to conduct HUMINT operations to include: screening, interrogating, debriefing of friendly forces, elicitation, and the exploitation of multimedia. Students in the 97E course receive approximately 184 hours of hands-on and classroom instruction in the Laws of Land Warfare and the Geneva Convention. Students also learn skills in CFSO, HUMINT section operations, and liaison with CI and military police (MP) assets.

Automation training in the 97E course revolves around the CI/HUMINT Information Management System (CHIMS). CHIMS is designed to provide automation support for Army tactical CI and HUMINT collection, investigation, interrogation, document exploitation, and FP requirements from battalion to echelon above corps (EAC). CHIMS provides CI and HUMINT personnel with the ability to process, analyze, and disseminate collected information of tactical relevance in a timely manner.

The course culminates in a comprehensive FTX conducted at the world-class training facility on Fort Huachuca. Throughout the five-day FTX, 97E and 97B students participate in a combined training exercise, using CHIMS to integrate and synchronize the collection of CI and HUMINT information in a COE-driven scenario. The FTX allows each 97E student to perform the CI skills learned during the core 97E course. This exercise is an IET requirement, which completes the TRADOC-mandated soldierization process.

**Future.** In FY06, the 97E course will expand to an 18-week 3-day course to support an increased Army HUMINT force structure. The 97E course will become the primary IET feeder MOS for the 97 series while continuing to teach the required HUMINT skills outlined above.

## 231-98H10, Communication Locator/Interceptor Course

**Course Scope.** The 22-week 98H course is primarily a self-paced two-phased course. During Phase 1, students learn to copy International Morse Code letters, numbers, and special characters at 20 groups per minute using specified equipment, message recording, and annotation. Students also learn operations involving the intercept processing, recording, and forwarding equipment.

Automation training in Phase 1 is based upon the Basic Morse Mission Trainer (BMMT) that provides independent delivery of self-paced curricula while collecting student performance and administrative data. The BMMT gives the instructors the ability to monitor the students in real time as the students move through the self-paced portion of the course.

Throughout Phase 2 students learn reporting requirements, radio wave propagation, computer network and electronic attack techniques, database maintenance, local-area network (LAN) establishment and maintenance, identifying signal modulation types and parameters, multichannel characteristics and identification techniques, identifying ground surveillance and counterbattery radar signals, signal recording requirements, workstation operation, datalink establishment and maintenance, and how to tune receivers remotely. Phase 2 automation training involves classified material and methods; therefore, this article will not address it.



A 96B student responds to a query by one of his instructors.

The 98H course culminates in a comprehensive FTX where soldiers organize into squad-sized elements. The FTX comprises four phases:

- Phase 1, Tactical movement to the FTX site.
- Phase 2, Set-up field site.
- Phase 3, Situational training exercises (STX) and lane training to include: react to contact (mounted), break contact (mounted), first aid, radio operations, request medical evacuation (MEDEVAC), hand and arm signals, and reporting intelligence information via a situation or spot report.
- Phase 4, Redeployment and recovery.

The FTX is an IET requirement, which completes the TRADOC-mandated soldierization process.

**Future.** The 98H MOS is facing an uncertain future as the Army reduces the annual number of students trained to copy International Morse Code letters, numbers, and special characters. The 98H MOS may be merged into the new 98Y MOS, and Morse Code may become an Additional Skill Identifier (ASI) for 98Y-qualified soldiers.



*George Stemler (First Sergeant, U.S. Army, Retired) is the 309th MI Battalion's Senior Civilian Training Specialist. He has worked as a civilian training specialist since retiring after 20 years of service. Mr. Stemler holds a Master of Science degree in Computer Information Systems from the University of Phoenix and a Bachelor of Science degree in Business Management from Wayland Baptist University. Readers may contact the author via E-mail at stemlerg@hua.army.mil and telephonically at (520) 538-7027 or DSN 878-7027.*

# Geographic Information Systems (GIS) As Assured Mobility Enablers

by Major John H. Haefner

The informational tenet of “assured mobility” (develop the mobility common operating picture [COP])<sup>1</sup> is possible through effectively seeing, visualizing, and conversing about the measurable elements of geographic features such as roads, bridges, and buildings. What are these information requirements for the purveyors of the Mobility battlefield operation system (BOS), chiefly engineers and military police (MPs)?<sup>2</sup> Who has final authority over the measurement and accuracy of these attributes of geographic features in the first place? Moreover, who are the terrain management, measurement, and maintenance stakeholders? Without tackling these issues, we will not see the necessary synergy between several seemingly disparate Army cultures: the sapper, the topographic engineer, and the MP.

The article that follows is the result of a Commanding General, U.S. Army Special Operations Command-(CG-SOC) directed independent study by Major Jack Haefner (Corps of Engineers) and MAJ Ross Guieb (Military Police Corps). Our goals were not only to discover the finer points of our battlefield mobility responsibilities but also to delineate these responsibilities and visualize the terrain in a manner meaningful to our trades. Our purpose from the onset was not to propose a maneuver support generalist; rather, we envisioned a complementary partnership between the maneuver and mobility support manager (MP) and the mobility enabler (engineer). Moreover, we believe that the concepts of data collection, data management, and collaborative geographic symbolization to be useful to all BOS functions, especially Intelligence.

## Problem Statement

There currently is no method or system for allowing users to view and analyze a common feature in a manner specific to their mobility discipline. In other words, how can those responsible for assured mo-

bility (engineers and MPs, for example) collaborate about, examine, and analyze a common geographic feature but retain those attributes specific to their trade?

To approach this problem, we found several issues that we must address:

- What are our language (data) requirements?
- What data elements have current definitions in Military Specification (MILSPEC) or Standardized Agreement (STANAG) documentation?
- Exactly what does the engineer and MP need to know beyond the published standards?
- How do we organize our data?
- How do we exploit this data?
- What do we do with the data—how can others benefit from our data collection efforts?

## Developing a Common Language

Developing a common mobility language (see Figure 1) required a certain degree of restraint. Although our impulse was to break down every wall between the engineer and MP, we maintained our intention to avoid generalizing the skills of each mobility stakeholder. In short, we wanted the solution to multiply the effects of our existing expertise, not replace it. We required that our solution built a COP; if it did not synthesize data into a clearly understandable and meaningful picture specific to the engineer or MP (but not both), we would have missed the boat.

Our next step was to determine our data requirements.<sup>3</sup> Since we would render our data as vector data (a feature database of points, lines, and polygons), we found reverse engineering to be most practical. We used one geographic feature for our study; we could easily apply our findings to others. Our example, a bridge point,<sup>4</sup> suited our needs since it is a simple and prominent feature affecting mobility and has a particular—and differing—meaning to the MP and engineer. Again, we can extend what we learned to other features. A good starting point for all possible alternative features is a common 1:50,000 topographic line map (TLM).

Although not nightstand reading, the National Geospatial-Intelligence Agency (NGA) (formerly

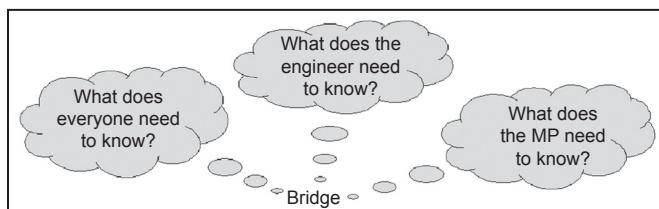


Figure 1. Common Language Requirements.

the National Imagery and Mapping Agency or NIMA) Vector Product Format (VPF) MILSPEC family (vector map [VMap], for instance) reiterated that VPF data will vary in attribute requirements by type: the fewest number of attributes stem from VMap 0 and VMap 1; the densest attributes will flow from DTOP. In addition, we found that the DTOP MILSPEC attributes for a bridge point covered a majority—but not all—of our information requirements (see Figure 2). To further enrich existing bridge attributes and meet our full requirements, we added the items shown in below to a separate database (Figure 2).<sup>5</sup>

#### **Engineer:**

- Controlling authority (unit, command).
- Mean flood stage (could populate data remotely from the Engineer Research and Development Center [ERDC] or other sources).
- Image hyperlink (hyperlink to a file containing a reconnaissance image).
- Abutment material (concrete, aggregate, and so forth).
- Abutment condition (good, cracked, etc.).
- Embankment slope (for adjacent bridging).

#### **Military Police:**

- Force protection (FP) status (standoff from weapons system, overwatch, etc.).
- Last observation (date-time group).

<b>DTOP Attributes</b>	Width of Second Traveled Way Length of Greater Precision
Row Identifier	
FACC Code*	
Bypass Condition Category	
Bridge Opening Type	
Bridge/Bridge Superstructure Type	
Existence Category	
Horizontal Clearance	
Identification Number	
Load Class Type 1	
Load Class Type 2	
Load Class Type 3	
Load Class Type 4	
Length/Diameter	
Material Composition Category	
Number of Spans	
Overhead Clearance Category	
Transportation Use Category	
Underbridge Clearance Category	
Minimum Traveled Way Width	
<b>Engineer Attributes</b>	
Controlling Authority	
Mean Flood Stage	
Abutment Material	
Abutment Condition	
Embankment Slope	
Hyperlink of Photograph	
<b>MP Attributes</b>	
Force Protection Status	
Force Protection Comment/Last Observation	
Note:	
	*Feature and Attribute Coding Catalogue (FACC); coding scheme promulgated by the Digital Geographic Information Working Group (DGIWIG) ( <a href="http://www.digest.org">www.digest.org</a> ).

Figure 2. Sample Attributes.

## Organizing the Data

Having considered several meaningful additional attributes, the data required organizing and normalizing (see Figure 3). Normalization greatly reduces the database size by minimizing redundancy. However, one must note that, although it is often preferable to normalize for space and bandwidth considerations, “joining the data” (i.e., linking between the key in the primary table and the related table) can have processing costs on the client side.

Normalization reduces data space requirements by storing a simple and unique integer in the master (or primary) table and joining that “key” to a separate reference table. When inputting into the database, one designs the “look up” function so it is transparent to the user—one sees only the definition, but the integer (key) is stored. For example, if we had 300 bridges in our area of responsibility, 200 of which were operational and 100 destroyed, we could store the words OPERATIONAL and DESTROYED 200 and 100 times respectively, but this would take space and be prone to errors. Instead, we could normalize as follows: split the original table into two tables. In the first table (tblBridge), we would store only the integer key to the definitions in our second table. In the second table (tblExs), we would have two fields: the unique ID (existence) and the definition of that unique ID. We would then populate the table with current DTOP definitions: 0 (UNKNOWN), 5 (UNDER CONSTRUCTION), 7 (DESTROYED), and 28 (OPERATIONAL). Thus, in our master table, we would only store the integer 1 and 2.

If populated with text, a query by bridge status would reveal every type: OPERATIONAL, DESTROYED, and all misspelled variants.

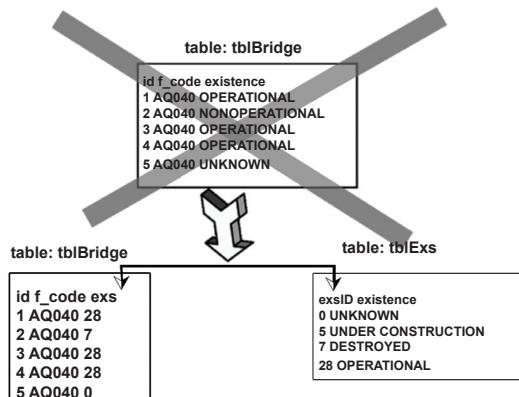
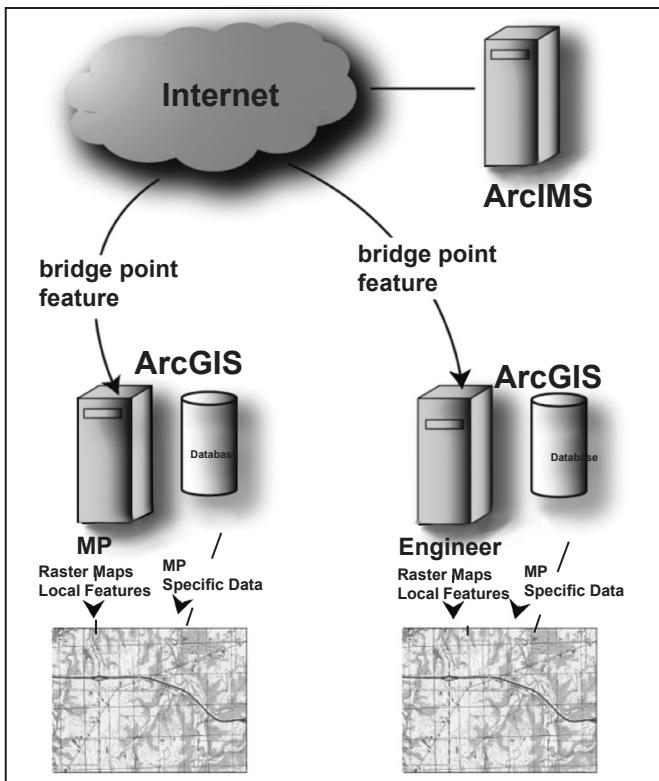


Figure 3. Normalizing Data.



**Figure 4. Final Data Model.**

Our final model (showing the flow of data for how we solved the problem) appears in Figure 4. Note we maintained all our DTOP attributes, even though we populated few of them. We did this based on access and data integrity of the original DTOP attributes. We could forward the efforts of those collecting the data higher at a later time, combined with existing attribute tables, and perhaps ultimately replace the original erroneous values.

## The Geographical Information System (GIS)

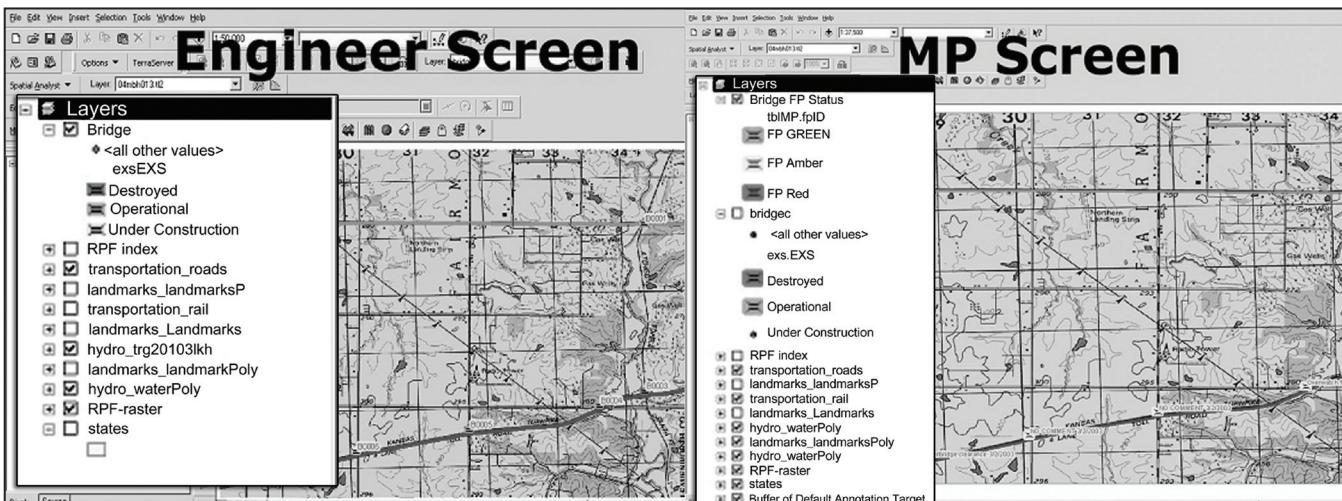
The final step to harnessing this data and building our COP was integration into a GIS. A GIS is essen-

tially an interface for querying, analyzing, and viewing spatial databases (i.e., databases with informational elements that one can tie to the surface of the earth). The power of a GIS is unlocked in its ability to analyze these features based on the attributes (for example, “show all bridges MLC [military load class] 60 and higher”) and their relationship to each other (“show all primary routes passing over bridges MLC 60 and below”).

Note that our data resides both locally and remotely (Figure 4). We stored our raster map background locally but the bridge feature is from a map server (Arc Internet Mapping Server [ArcIMS] route server).<sup>6</sup> The engineer and MP then relate their separate local database tables to the same collection of features and they can symbolize the bridge feature based on the specific needs of either BOS. In Figure 5, the engineer has the bridge symbolized based on operational status, while the MP has symbolized it based on FP status. Again, these are two different views at two different locations; the feature is served remotely over a secure Internet but specific data required by the user resides locally. As long as there is a unique identifier for the record (identification, for instance), we can build the connection.

## Systems Integration

Unfortunately, current Army Battle Command System (ABCs) and Maneuver Control System-Light (MCS-L) builds do not easily cross talk with industry-standard geospatial data<sup>7</sup> without use of a Digital Topographic Support System (DTSS) Overlay Provider. In addition, MCS-L does not allow users to relate or join external user-defined databases to overlays.



**Figure 5. Final Screens. Raster map background and vector data stored locally; bridge data served from Internet Mapping Server.**

However, the Army could easily integrate our solution into future ABCS builds as well as MCS-Engineer (under development). Our solution incorporates feature serving via ArcIMS and symbolization and analysis in ArcGIS. Since both the DTSS Map Server and Commercial/Joint Mapping Tool Kit (C/JMTK) rely on ArcIMS technology, the DTSS Map Server could also function as a feature server. In addition, since MCS-Engineer is essentially an ArcGIS extension, our symbolization methodology could function within MCS-Engineer with little modification. Furthermore, our method could further enrich other datasets such as non-NGA data (locally procured data, data from field force engineering, etc.).

The aspects that are so compelling about a GIS solution are both its potential for specificity and its ability to reach across many seeming disparate disciplines. Although our solution was built with an eye towards mobility support, the principles we set forth could also apply to other facets of engineering (construction, for instance) as well as non-engineering applications (transportation tracking via ArcIMS in U.S. Army, Europe [USAREUR], for instance). In short, when we can tie a piece of information to the ground, it becomes geospatial information; anytime we can view and analyze physical placement and spatial relationships, we are on to something bigger.

Using Microsoft™ Access rather than a larger enterprise database was only one possible solution. We endeavored to use tools on hand initially with little additional cost. Although we could also deliver features over a network (using an enterprise or larger spatial database such as Arc Spatial Date Engine (ArcSDE), we felt serving with ArcIMS gave the designer needed control. If requirements balloon (remember, our development was for only one feature, bridges, in a very small area), migration to an enterprise database or spatial data server might be necessary.

## Challenges With This Solution Set

We identified the following four challenges to this experiment. They deal with data simplicity, positional accuracy, measurement standards, and data lifespan.

**Data simplicity is a constant battle.** Any information system, including a GIS, can quickly take on a life of its own. There is not one commander who would not want to have absolutely complete informa-

	FM 5-170	DTOP (MIL-PRF-89037A)
Materials	"Construction Materials" Unknown Concrete Masonry Prestressed Concrete Reinforced Concrete Steel Stone Wood Other	material composition category (MCC) 0 Unknown 21 Concrete 62 Masonry 77 Prestressed Concrete 83 Reinforced Concrete 107 Steel 108 Stone 117 Wood 999 Other
Horizontal Clearance	In meters	In decimeters Decimeters
Underbridge clearance	Meters	

Figure 6. Bridge Data Inconsistencies.

tion, 100 percent accurate and with all possible attributes. Thus, we would need to establish standards (standing operating procedure [SOP] or policy) on what to collect, when to collect it, and to what accuracy. As collection efforts increase, so do the data storage requirements and the need for skilled database managers.

**Positional accuracy.** Changing positional information in a distributive environment is not only difficult but also fraught with potential risks. Again, there need to be standards promulgated regarding authority to make changes and quality control of the same. For the most part, positional information requires close control. We envisioned ArcIMS feature serving to be an acceptable solution for this quandary.

**Need to establish and train measurement standards.** Note that the measurement standard for horizontal and under bridge measurement is in meters for the sapper and decimeters by DTOP MILSPEC (see Figure 6). If users will potentially collect the data, they need to understand the standards.

**Data lifespan.** Despite the efforts of the 81T Topographic Analyst, NGA databases will not incorporate this data that they may greatly improve in theater. Although this may change in the future, a topographic engineer is not currently considered a “trusted source” for national-level data.

Who has the authority for feature measurement? It is not unrealistic to expect multiple parties to measure the MLC of a bridge. Consider that an MP may conduct a hasty reconnaissance initially, then a Cavalry Scout, then a detailed engineer reconnaissance, then a reach assessment by Waterways Experiment Station (a Corps of Engineers laboratory). Do we capture all the metadata about each

measurement (who, what, when, how, etc.)? What about lifespan data of a bridge based on wear and tear, damage, etc.? Who will have final authority over potentially contentious measurements?<sup>8</sup>

## Conclusion

Not until we develop a mutual understanding between the engineer and MP communities will we have assured mobility. Although we have proposed a new set of technological tools, the human dimension and principles of data-sharing we have shown are solution-nonspecific. Building a mobility generalist is not the solution; rather, if we do the soul-searching required to identify our data requirements and relate them to centrally controlled and served geographic features, we can affect positive outcome in all mobility operations (offense, defense, stability, and sustainment).

*The author thanks Major Ross Guieb, Military Police Corps, for his significant contributions to this article and the study.*



## Endnotes

1. FM 3-34 (Draft), Engineer Operations (formerly FM 5-100), 15 February 2003, page 4-36.

2. Engineers and MPs are not the “owners” of the Mobility BOS. We deliberately limited our study to two individuals: one Engineer and one MP. Others that could benefit from this study could be Chemical, Combat Service Support, etc.

3. Incidental to our research, we required a firm understanding of geospatial data (types, accuracy, and datums) as well as relational database design. See “Enabling Situational Awareness With Geospatial Data: Engineers Allowing Commanders to ‘See First, Act First, and Engage Decisively’,” **Army Engineer Association (AEA) Magazine**, PB 5-02-2, Volume 10, Number 2, March/April 2002, pages 18-21.

4. We can cartographically symbolize a bridge differently based on scale. At a large scale, a bridge may be a small line feature, while at a small scale, it will be a dimensionless point.

5. There exists a gap between these required attributes and collection methods. Since the customer receives many VPF products with unpopulated (or dated) attributes, there needs to be a systematic approach to populating them. If populated from national technical means, they are either attributed by NGA from an imagery source (not necessarily “ground-truthed”) or partially populated by the echelons above corps topographic battalion or the division terrain team.

Since technical reconnaissance is an engineer task, current engineer forces can provide assistance to terrain teams to satisfy many of these requirements. What is more, much of this data is germane to current engineer operations, whether line of communication (LOC) analysis, construction estimates, etc.

However, our research found few real-world examples of these data requirements actually worked into the reconnaissance and surveillance (R&S) plan (engineer technical reconnaissance assets notwithstanding). As a result, we identified several doctrinal and training shortfalls:

- DA Form 1249, Bridge Reconnaissance Report, identifies few of the above (useful) attributes. In addition, several attributes do not match existing military specifications (see Figure 2).
- The only detailed description of measurement standards for structures is in **FM 5-33, Terrain Analysis**. Those outside the topographic disciplines may use these standards, although dated. Neither **FM 5-170, Engineer Reconnaissance**, nor mission training plan (MTP) task books identify measurement methods and standards.
- Timing of measurements is also of valid concern. The 50 different measurements of a single bridge may not be valid during obstacle assessment but they may be during stability operations and support operations transition. Regardless, what happens to the initial limited measurements of a feature? The importance of these is not immediately relevant to initial combat operations in an area of responsibility but during transition to peace operations, they take on a life of their own.
- Finally, one relatively untapped sector of engineer integration into the reconnaissance and surveillance plan is using GIS to analyze the data culled from the collection matrix. The discipline of geostatistical analysis allows the GIS operator to develop models of trends and conditions.

6. Note: A file server and a map server are not the same. A file server merely stores any data file for prescribed access. A map server delivers either a fully composited, dynamic map or the features (either individual or bundled as map services).

7. For those unfamiliar with MCS-L, user defined overlays are possible and “georeferenced” but they do not integrate into other industry standard GIS packages. The system allows export of data into XML files but we would have to translate them back to an industry standard format such as ArcGIS Shapefiles (.shp) or MapInfo Files (.mif).

8. If the engineer community captures this data, do they then assume an additional role of “manager of all theater of operations structures”? Doctrine does not solely delineate responsibilities for objects directly relating to mobility and countermobility (e.g., roads, bridges). A cursory review of doctrine and several division and corps SOPs yielded no practice for analyzing relationships between route status and bridges. In short, mobility assessments can often be nothing more than the division transportation officer (DTO) chairing a regular movement control meeting with the Assistant Division Engineer and Division Engineer (ADE/DIVENG), Provost Marshal, G2, G3, and division support command (DISCOM) providing route information. Although human coordination is an essential battle rhythm event, it can be fraught with inaccuracies and falls short of building a COP.

*Major Jack Haefner is a graduate of Northeastern University (Boston), University of Missouri (Rolla), and the Command and General Staff Officer’s Course. He is currently assigned to the U.S. Army Pacific G2 as the Geospatial Intelligence Officer and has served in a variety of engineer and geospatial intelligence positions at Fort Bragg, North Carolina, Germany, and Fort Belvoir, Virginia.*

# An Open-Source Overview of the Technical Intelligence Collection Threat in Asia

by Sergeant First Class Wade C. Wilson

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

The technical intelligence (TECHINT) threat to government employees and civilian travelers in Asia is as prevalent today as was TECHINT targeting of Western embassies and diplomats in Moscow at the height of the Cold War. Even this comparison may be below the mark because indeed both Russia and certain areas of Asia today have far surpassed the level of targeting that one once expected between the polar antagonists of the Cold War era.

The reason for this increase in threat is not because of increased political tensions but rather for a more pragmatic reason—money, or more specifically, economic espionage. Indeed, the nature of the threat is at the heart of the reason why open sources can adequately identify the threat. During the Cold War, only very rare exposés, such as the “Great Seal” attack at the U.S. Embassy in Moscow—graphically presented by the U.S. Ambassador as evidence at a publicly televised United Nations forum—or the Soviet bugging of the then new U.S. Embassy in the 1980s, ever made it to the national press. Most other incidents were only for the purview of those with access to the classified newsreels; the rest of the world remained blissfully ignorant of the technical threat they might be facing during overseas travel.

## Background

Beginning in the 1980s, the transformation of the world’s political and economic environment changed the nature of the threat. Certainly, the threat was present as far back as the Korean War when Japanese technicians began reverse-engineering U.S. aircraft parked on their tarmacs in between sorties over Korea.<sup>1</sup> Such rumors as Air France having bugged its first-class seats with microphones to overhear con-

versations between international business executives and reports of laptops and documents copied or even stolen at French hotels give credence to this new age threat. Suddenly, the threat was neither from the United States’ traditional “enemies” nor focused on politico-military targets, allowing an open, honest examination and discussion of what this threat meant for the future of U.S. security. This short overview will sift through some of the available open-source data to uncover the technical intelligence threat facing everyone (business executive, government official, or tourist) who happens to find a trip to Asia on their upcoming itineraries.

First, one should note that the technical threat is not universally focused, prevalent, nor equivalent throughout Asia. Certain countries have a more dedicated collection program than others, either for reasons of economic espionage or political security. An open-source list of these countries (in alphabetical order) includes Japan, the Democratic People’s Republic of Korea (North Korea), the People’s Republic of China (PRC), Taiwan, the Republic of Korea (South Korea), the Russian Federation, and the Socialist Republic of Vietnam. This is not to say that technical collection does not occur in other countries of Asia, perhaps notably India and Pakistan. In fact, technical collection probably does occur in every country that maintains an intelligence service worldwide; however, either they do not direct the focus toward foreigners not deemed a domestic security threat, or the information available on the threat is not widely available in an open-source forum.

## TECHINT Collection Equipment

Indeed, the equipment needed to conduct most basic technical collection missions (microphones, cameras, and receivers) is widely available in the commercial market at prices that even amateur hobbyists could afford and thereby conduct collection missions in almost any environment. Additionally, for those hobbyists who do not have the technical nor engineering background to build their own hidden transmitters and receivers,

various Japanese and Taiwanese electronics companies produce ready-made products such as video cameras and microphone transmitters inside devices that one can install or temporarily transport into areas of interest.<sup>2</sup> These devices may appear to be smoke detectors, notebooks, alarm clocks, telephone outlets, calculators, cellular telephones, or even a pack of cigarettes. This goes to show that even if a country does not appear, at the outset, to have an ongoing technical collection mission, any country could conduct technical collection at will by simply surging the capability using a small commercial-off-the-shelf purchase and detailing a team of intelligence professionals or engineers to emplace and monitor the equipment on the target of interest. Such targets of interest might include international conferences or negotiations where collectors might monitor delegation members to determine their nation's hidden negotiating platforms. Similarly, they often monitor international companies' contract bidding process, thereby allowing local competitors to underbid them by the smallest of increments. Truly, any area that might be of national interest (economic well-being is assuredly part-and-parcel of the Asian national interest) is a valid target for technical collection.

The technical collection threat in practically any room worldwide starts with the telephones on the desk. A standard telephone contains at least one microphone, and with a simple reengineering trick, one can transform telephone speakers into microphones as well. Consider then the number of potential microphones a modern digital telephone might have: two in the handset, two for the speakerphone, and one for the ringer. What is preventing the discussion occurring inside the room from transmitting along the telephone lines? As it turns out, not much, and if one is overseas—especially in Asia—a person should always assume that his telephone is the equivalent of a live microphone.

In the past, the hook switch of a telephone physically disconnected the wires inside the telephone that established the talk path (an electrical conduit between the handset and the other party). If an adversary wanted to “bug” the telephone, there were generally only two options available:

- ❑ Rewire the telephone’s internal network to bypass the hook switch when the telephone is not in use or “on hook.”
- ❑ Introduce another transmitter, such as a radio-frequency transmitter not dependent on the tele-

phone internal wiring to transmit conversations outside the room.

The introduction of cheap, digital telephony did away with what little security the hook switch provided. Now the “hook switch” is nothing more than a computer-chip function that signals a disconnect procedure through digital commands. However, network administrators and hackers know bypasses they can use to turn telephones on while they are sitting idle in the telephone cradle. At the administrator’s level, “clicking a button” on the main control program can activate telephones controlled by PBXs.<sup>3</sup> PBXs also have numerous vulnerabilities to hacker exploitations (thus the billion-dollar-a-year toll fraud problem in the United States), which make any telephone controlled by a PBX a potential threat to external exploitation as well.

### **Asia-Specific TECHINT Collection**

The threat in Asia, however, is a little more simplistic and common than an exotic hacker attack. Many hotels in Japan, China, and South Korea have permanent wiring so that the telephones receive and transmit audio even when they are not in use.<sup>4</sup> In China, at least one agency of the PRC Government owns most if not all of the executive-level (three or more stars) hotels. Foreign hoteliers need government permission to build and conduct business in China, something more easily accomplished with a PRC agency pushing the contracts through the labyrinthine Chinese bureaucratic process. Granting partial ownership to the PRC agency willing to support the project—as well as granting the government certain concessions, one of which is general oversight and liberal leave during the construction—can facilitate this process. With this power, the Chinese Ministry of State Security can lay extra wire in the hotels during construction to either permanently tie-in microphones or make plug-and-play installation as easy.<sup>5</sup> They can then establish permanent surveillance and technical monitoring posts near the hotel to keep track of the guests’ conversations, actions, and associations. Hotels in North Korea and Vietnam most likely follow China’s lead in monitoring foreigners from a largely internal security standpoint.

Japan and South Korea have a completely different perspective for monitoring foreigners’ business in their hotels—economic espionage. U.S. Ambassador to Japan, Michael B. Smith, noted that Japan permanently bugged and monitored entire floors of many

prominent hotels and that “*Nobody in his right mind would make a telephone call [from a hotel in Tokyo].*” Rather, “*if you wanted to talk about something sensitive, you always went outside*” because “*They can’t bug the parks.*”<sup>6</sup> In a classic example of Japanese hotel bugging, a U.S. telecommunications company executive traveled to Japan to test his company’s prototype scrambler telephone. He plugged the telephone into the hotel room’s telephone jack and two hours later, “*a very polite but insistent serviceman from the telephone company appeared, unsolicited, at his door.*” Their conversation went something like this:

*Serviceman: “There is something wrong with your telephone.”*

*U.S. Businessman: “No, it works fine.”*

*Serviceman: “But we cannot understand what you are saying.”*

*U.S. Businessman: “That is the point.”*

*Serviceman: “It is not compatible with Japanese standards.”<sup>7</sup>*

The fact that technical collection is as commonplace in Japan as in any other country on Earth should not come as a shock. Japan does not have a national intelligence service per se, because every Japanese business executive is an ad hoc collector for the Japanese Ministry of International Trade and Industry, an economic intelligence clearinghouse that assembles and distributes intelligence to the companies that could most benefit from it. The Japanese even built an industrial espionage school, the Institute for Industrial Protection, with government money to teach businesspersons the art of spying.<sup>8</sup> It is therefore unsurprising that Japanese hotels might cooperate with their government’s efforts to keep tabs on all foreign guests for the “good” of the nation. Foreign businesses should likewise consider every telephone in their buildings and personal residences actively tapped by the telephone company as it would be highly unlikely that the only economic espionage targets of interest in Japan would be of those persons temporarily residing in a downtown hotel. After all, a Japanese automaker would be interested in the preliminary plans of U.S. American auto dealerships in Japan; there are hundreds of other similar scenarios.

Certainly, the fact of businesses bugging other businesses is an everyday matter in Japan, where neither the perpetrator nor the target might necessarily be foreign. In fact, politicians use the services of private

investigative agencies to place bugs in strategic locations to collect on their political rivals, as do smaller businesses and domestic dispute clients.<sup>9</sup> On the other hand, if the person is so inclined, he could just as easily purchase a bugging device himself in the Akihabara electronic district in Tokyo where a plethora of different devices and how-to manuals are available. These Japanese-made devices, as well as Taiwan-made devices, find their way to similar electronics markets throughout Asia including South Korea and Thailand. Such clandestine surveillance devices are illegal to import into the United States—although there are numerous loopholes that spy and electronics shops in the United States are able to use to offer similar items for sale. In Asia, however, the limitations on importation and use are virtually nonexistent. Amazingly, an international air traveler will likely have a harder time importing and exporting commercial radio equipment (amateur “ham” radio, citizen’s band [CB], etc.) from an Asian country than carrying illicit listening devices through customs and security checkpoints.

It is generally well known that we all should guard our conversations in Asian hotels from the prying ears of the host nation, but what about the threat from neighboring Asian nations? Should a U.S. business executive in the Philippines be worried about telephone tapping efforts from the Chinese or Japanese in addition to Filipino security agencies? As it turns out, the answer is yes. The Chobetsu is Japan’s signals intelligence service and “*has the capability of eavesdropping on all of Japan’s neighbors...in addition to Japanese telephone lines.*”<sup>10</sup> In China, the Third Department of the People’s Liberation Army has approximately 20,000 trained foreign linguists working at signals intelligence (SIGINT) collection sites throughout China, as well as in extra-territorial sites in Burma, Laos, and the Paracel Islands (near Vietnam).<sup>11</sup> These sites provide complete SIGINT coverage of radio, telephone, and satellite communications, targeting all of China’s neighbors and many others beyond its immediate borders, but generally within its area of interest, covering Asia (in all directions), the South China Sea, and Pacific Ocean.<sup>12</sup>

China’s newfound economic prowess has also helped the PRC more efficiently conduct its SIGINT collection mission. The Chinese Government, a major shareholder in the Iridium satellite consortium, helped launch (or will launch) 22 of the planned 66 satellites in the Iridium constellation, and will provide

a major gateway in China to connect Iridium satellite telephone calls with the universal, public, switched telephone network.<sup>13</sup> When a country owns or controls domestic, international, and satellite telephone switches, no modifications need to be made to a telephone instrument to intercept, record, or exploit the discussions made between it and another party. This capability is a natural function of the switch, making all such communications subject to host-nation interception. The Chinese-Iridium gateway is not only an essential component of the Iridium business model, thereby allowing connection of Iridium users to virtually any telephone in the world, but would also allow Chinese SIGINT elements immediate, real-time access to virtually any Iridium user's communications (although as already mentioned, collections go beyond Iridium telephones).

A look at the major clientele list of Iridium might provide a small insight into the impact such a gateway could have on regional security issues. After nearly going bankrupt from the high costs of developing and launching satellites, Iridium was bought out and the new company partially kept in business through the help of major government contracts, such as with the Department of Defense, and in the Pacific theater with U.S. Pacific Command (PACOM)—the United States' front-line defense, guarding against any futuristic "Pearl Harbor," potential North Korean hostilities, the cross-Taiwan Straits crisis, or other such military contingencies. While PACOM may have access to secure encryption equipment to use in conjunction with its Iridium satellite telephones, the average businessperson probably would not, and neither would the average U.S. citizen get authorization to transport such encryption technology outside the United States. Therefore, without the inclusion of some means of encryption or secure voice scrambling, a business executive, government representative, or military official should function under the presumption that someone is monitoring all of his telephone communications made in a foreign country.

## Final Thoughts

This short article has highlighted some of the open-source information on threats that await business travelers, tourists, and government personnel alike in their travels and work in the Asian-Pacific Theater. Although the TECHINT threat is prevalent, they should not disregard the human intelligence (HUMINT) threat. Perhaps a rule of thumb that one would be well advised to follow is not to engage in

any activities or discussions that one would not like to become public knowledge. Furthermore, even though a person's travels may take him to a so-called friendly country, this is no guarantee that either that country is not interested in his activities or that other countries do not have the means to collect outside their own territories. In this regard, a popular military motto seems appropriate: "Vigilance is my watchword."



## Endnotes

1. To cite just one example, Japan studied and improved on the technology behind disc brakes employed on F-104 fighters according to John J. Fialka, **War by Other Means: Economic Espionage in America** (New York: W.W. Norton and Company, Inc., 1997), page 43.
  2. Ibid., pages 114-116.
  3. PBX is Private Branch Exchange, a computerized telephone switch used by businesses and government agencies as a cost-saving measure while incorporating numerous features like call waiting and call forwarding to support their customer-relations needs.
  4. Ibid., page 14.
  5. Eftimiades, Nicholas, **Chinese Intelligence Operations** (Annapolis, MD: Naval Institute Press, 1994), page 45.
  6. Schweizer, Peter, **Friendly Spies: How America's Allies Are Using Economic Espionage to Steal Our Secrets** (New York: The Atlantic Monthly Press, 1993), page 85; also Fialka, **War by Other Means**, page 114.
  7. Fialka, page 118.
  8. Schweizer, page 23.
  9. Fialka, page 114.
  10. Ibid., page 118.
  11. Stokes, Mark A., **China's Strategic Modernization: Implications for the United States** (Carlisle, PA: Strategic Studies Institute, 1999), pages 33-34.
  12. Ibid. "Lanzhou collects on Russia. Shenyang covers Russia, Japan, and Korea. Chengdu monitors India, Pakistan, and Southeast Asia. Nanjing monitors Taiwan. Guangzhou covers Southeast Asia and the South China Sea. Sites in Jilemutu, Erlian, and Hami as well as other Northwest China locations cover Central Asia, Russia, and Mongolia." Stokes lists sites in Shanghai, Beijing, plus Burma, Laos, and Rocky Island in the Paracels but does not mention their actual targets.
  13. Ibid., pages 48-49.
- Sergeant First Class Wade Wilson is a certified Technical Special Agent assigned to B Company, 205th MI Battalion, Fort Shafter, Hawaii. Special Agent Wilson is working towards a Master's degree in Strategic Intelligence through American Military University. Readers can reach him at [wade.wilson@us.army.mil](mailto:wade.wilson@us.army.mil) and telephonically at (808) 438-6887.*

# OPERATION SHADOW GUAM

by First Lieutenant Catharine T. Wentz, First Lieutenant Dan Ma, and Second Lieutenant Kelley Calene Woods

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

The Shadow 200 Tactical Unmanned Aerial Vehicle (TUAV) system is one of the newest assets for tactical-level Army Intelligence. With its day-time camera (electro-optic) and infrared capabilities, it provides imagery and video allowing U.S. and allied forces a near-real-time (NRT) picture of the battlefield. The system supports intelligence collection in reconnaissance, surveillance, and target acquisition (RSTA) and the battle damage assessment (BDA) process. The TUAV system provides support for maneuver operations and fires, and sup-



Specialist William Wright operating the portable GCS.

2003, Charlie Company, 102d MI Battalion, began fielding the Shadow system for operations in the 2d Infantry Division (2ID). Normally used as a brigade asset, the 102d MI Battalion is using Shadow TUAV in a general support role for 2ID. The Shadow system's relatively small air vehicle (AV) measures only 11 feet 4 inches in length and has a wingspan of 12 feet 8 inches. The AV has an optimal cruise speed of 70 knots and has the ability to stay on station for approximately 4 hours at a range of 50 kilometers from the Ground Control Station (GCS). Unlike other UAV systems, the Shadow 200 launch is by pneumatic/hydraulic launcher.

The Shadow 200 operates with several systems. These include the—

- All-Source Analysis System (ASAS).
- Joint Surveillance Target Attack Radar System (Joint STARS) Common Ground Station (CGS).
- Advanced Field Artillery Tactical Data System (AFATDS).
- Automated Deep Operations Coordination System (ADOCS).

## Operation SHADOW GUAM

The operators of the Shadow TUAV system train much as manned aviation pilots do. In order to maintain proficiency, it is necessary for TUAV operators to conduct live or simulated flight operations and log flight hours in various types of weather conditions. The 2ID leadership selected the U.S. Territory

Photographs courtesy of Joe Cerretta and Captain Mark Denton.



Shadow 200 TUAV has a launch speed of 70 knots per hour.

port in developing friendly courses of action (COAs). This unique system also provides an early warning and force protection capability to the commander and allows for timely decisions on the battlefield. The TUAV system enables the ground maneuver commander to understand the ground situation by allowing sightings of obstacle positions and where the best maneuverability would be.

## Background

A relatively new Army system, the Shadow 200 TUAV made its debut only two years ago with its fielding to the 104th Military Intelligence (MI) Battalion at Fort Hood, Texas. In September



Sergeant Brett Horner and FSRs Ramonna Ennenga and Mark McGinn conduct engine starts as a C-17 flies by.

of Guam as the optimal training environment and, in January 2004, the Charlie Company “Shadow Warriors” deployed there to conduct their training.

Much preparation was necessary in order to commence flight operations in Guam. The deployment was a learning experience for everyone involved given that this would be the first time an entire unit had ever deployed from Korea to train away from the Peninsula. The TUAV Company deployed to Guam on a C-5 Galaxy cargo plane loaded with all personnel and equipment from its two Shadow TUAV systems.

Setting up headquarters at Andersen Air Force Base (AFB), the Company began extensive preparations for the first day of flight. First, the unit’s standing operating procedure (SOP) needed rewriting in accordance with Guamanian airspace restrictions and operations. Once the SOP revision was complete, soldiers moved on to the task of maintenance. Perhaps the most time-intensive part of flight preparations is magnetic calibrations. Since the AVs would be flying in Guam rather than Korea, every AV needed recalibration and testing. While the maintainers and field service representatives (FSRs) prepped the AVs, the operators

prepped the runway(s). Operating on an old B-52 airstrip, the operators took on the task of conducting site surveys and emplacing all the equipment. In addition, the TUAV technician was busy coordinating airspace and resolving datalink and other communications frequency conflicts. Operating from Anderson AFB was a unique situation for Charlie Company because for the first time, they had air traffic controllers specifically dedicated to the TUAV mission. Having dedicated controllers was invaluable. They aided the operators who had never operated in Guam as well as U.S. Air Force personnel, who had never worked with the Shadow system.

Once we completed all of the preflight issues, it was time to fly. Using two full TUAV baselines of equipment, the company operated on one runway beginning with daytime flights only. The second week the company decided to “train as you fight,” breaking the company into two separate platoons operating on parallel runways. This entire exercise tested the abilities of the mission commanders, many of whom conducted their first missions in Guam.

While Charlie Company was conducting operations, the 31st Marine Expeditionary Unit (MEU) was also conducting close-quarters combat training on Guam. The two units decided to work together to achieve mutual training objectives. Charlie Company operators needed more training conducting the BDA process and surveillance operations, while the Marine Commander wanted to watch the battle from his operations center. In the first-ever joint U.S. Pacific



Soldiers of Charlie Company (left) are observing the video feed from the UAV on the portable GCS.

Command (PACOM)/Pacific Rim (PACRIM) Army TUAV-Marine exercise, the two units worked together to provide the MEU Commander with NRT imagery. On board the USS Essex, the TUAV operators were able to connect the Remote Video Terminal (RVT) to 23 different screens throughout the ship, giving live video feed to the MEU Commander and his battle staff.

The joint operation proved to be a huge success and flight operations continued. Midway through the training exercise, however, the weather in normally sunny Guam began to change. For a week straight, rainstorms allowed for only sporadic flights throughout the day; however, this did not stop training for Charlie Company. The downtime allowed for training in the Ground Control Station (GCS) via its embedded simulator capability. Using the simulator capability allowed both the instructor pilots (IPs) and the operators to gain experience in emergency situation procedures and unforeseen events. The time spent in the GCS using the simulators continued to add to air vehicle operators' (AVOs) flight hours and brought them closer to their Readiness Level One (RL 1) progression. (Note: RL 1 is the level of training that each AVO must reach in order to conduct flight operations without an IP inside the GCS shelter with them and is the highest flight readiness level in TUAV training.)

By the fourth week, the weather began to cooperate, allowing for the culminating exercise of the deployment: 24-hour surge operations, to include on-station relief. Many of the AVOs were recent graduates of advanced individual training (AIT)



Crew Chief Specialist Adrienne Robinson updates log books, a continual process.

and, therefore, did not have much experience in surge operations or night flights. This forced the less experienced operators and maintainers to work together as a team to complete the mission.

By the end of the fourth week, Charlie Company had logged 88.6 flight hours, flying 47 sorties. Additionally, the Company had achieved its goal of qualifying four IPs and allowing 12 operators to progress to RL 1. After the successful deployment, the TUAV Company packed up and returned to Korea on the Army's new High-Speed Vessel (HSV).

## Lessons Learned

**Emplacing/Displacing Time for a TUAV Baseline.** Charlie Company is constantly growing and learning. The deployment to Guam yielded many important lessons that the Company hopes to incorporate into future operations. One significant observation



Specialists Jason King, Steven Kambouris, and Kelsey Fort (left to right) loading AV on launcher in preparation for flight.

was the amount of time it actually took to emplace and displace one entire baseline system. The current standard is a 1-hour emplacement and a 30-minute displacement. This is one goal that Charlie Company has yet to meet.

*U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM) Aerial Common Sensor/Air Sensor Note: Other units equipped with TUAV today are meeting the set-up/teardown standard; the difficulties probably are due to the unit being new to the system.*

**Maintenance Challenges.** Another problematic issue during the deployment was that of maintenance. With the Shadow system still being relatively new, there were many unforeseen maintenance problems experienced in Guam. Things happened in Guam that even the UAV's Project Manager Office (PMO) had never seen. In order to overcome any potential "showstoppers" under this training experience, it was decided to set up two separate TUAV system baselines on parallel runways. This allowed the unit to continue with flight operations on one baseline even if maintenance problems grounded the other baseline.

*TSM ACS/Air Sensors Note: This technique (two systems set up on parallel runways) was unique to this unit; it is not a doctrinal technique.*

**AV Tolerance of Inclement Weather.** Maintenance was not the only obstacle to overcome in Guam. Along with the systematic mechanical and technical problems experienced, there was also the issue of the AV's capabilities to operate in inclement weather. The Shadow 200 AVs are definitely fair-weather aircraft. This fact could leave ground maneuver commanders at a severe disadvantage in poor weather conditions if they are dependent upon the TUAV. The weather, however, does not affect the simulation capability for training inside the GCS. During the one-week weather delay, the simulators were an invaluable training resource for both the operators and the IPs, allowing each to log flight hours in their records.

**Contractor Logistical Support.** One advantage that the TUAV system has is that of contractor logistical support. The FSRs proved to be invaluable during surge operations. Having the contractor maintenance support on-site facilitated resolution of the majority of the maintenance

problems the day we identified or found the fault. The FSRs allowed the unit to overcome many showstoppers caused by technical problems.

**Needed TUAV Modifications.** Based on what Charlie Company saw in Guam, it appears that there are a number of modifications needed on the Shadow TUAV system, to include improvements on the Datalink Interface Box (DIB) and the Tactical Automated Landing System (TALS). There are a series of upgraded Shadow systems due out in the next few years. Hopefully, these newer Shadow TUAV systems will remedy the maintenance challenges experienced in Guam.

## Current Operations

The 102d MI Battalion's Charlie Company successfully accomplished its mission and is now back in Korea preparing for future 2ID exercises. The unit continues to grow and build on lessons learned from the deployment to Guam. Charlie Company is in the process of integrating completely into 2ID's battle plan. Future challenges include educating others on the capabilities and limitations of the system so that the 2d Infantry Division can use the Shadow TUAV more effectively in tactical collection efforts.



---

*First Lieutenant Catharine Wentz is moving to Fort George G. Meade for an assignment with the 704th MI Brigade. During Operation SHADOW GUAM, 1LT Wentz was a TUAV Platoon Leader with the 102d MI Battalion, 2d Infantry Division (2ID). A graduate of John Carroll University in Cleveland, Ohio, she earned a Bachelor of Science degree in Sociology and Criminology. Readers can contact her via E-mail at [catharine.wentz@us.army.mil](mailto:catharine.wentz@us.army.mil).*

*First Lieutenant Dan Ma is the 1st Platoon Leader, 102d MI Battalion, 2ID, and held that position during Operation SHADOW GUAM. He holds a Bachelor of Science degree in East Asia Study and Japanese from the University of Arizona. You may contact him via E-mail at [dan.ma@us.army.mil](mailto:dan.ma@us.army.mil).*

*Second Lieutenant Kelley Woods is the 2d Platoon Leader, 102d MI Battalion, 2ID. She has a Bachelor of Science degree in English and Education from the College of the Ozarks in Missouri. Readers may contact 2LT Woods via E-mail at [kelly.calene.woods@us.army.mil](mailto:kelly.calene.woods@us.army.mil).*

# The Reserve Component Military Intelligence Linguist: A Historical Perspective on a Multicapable Asset

by Lieutenant Colonel Jeffrey F. Mitchell, UT ARNG

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

In a memorandum dated 12 January 2004,<sup>1</sup> Lieutenant General (LTG) Keith B. Alexander, U.S. Army Deputy Chief of Staff, G2, stated that he would like all existing 97L (Interpreter/Translator) structure converted to 97E (Human Intelligence Collector) and 97B (Counterintelligence Agent). What is the significance of this request? How does it affect the Army as a whole? To answer these questions, it is worth looking at the recent history of the Military Intelligence (MI) linguist.

## The Advent and Growth of 97L, Interpreter/Translator

The 300th MI Brigade (Linguist), a U.S. Army National Guard (ARNG) unit with a headquarters and two battalions in Utah and other battalions spread across the United States, had the ability to recruit relatively large numbers of skilled linguists in a variety of languages "off the street" to fill 97E (HUMINT collector), 97B (Counterintelligence Agent), and 98G (Voice Interceptor) positions. At that time, however, it took in excess of two years to train most of these linguists in one of the linguist military occupational specialties (MOSs). By the time the soldier completed training, it was nearly time for reenlistment, and the unit had not been able to employ the soldier for a single mission-oriented assignment.

In the early 1990s, the 300th MI Brigade (Linguist) recommended the creation of a linguist MOS to the U.S. Army Intelligence Center and Fort Huachuca (USAICS&FH). The reason for this recommendation was the Brigade's frustration in qualifying prior-service soldiers who were requalifying in one of the MI hard-skill linguist MOSs at the time. It was, and still is, common to retrain prior-service soldiers in the Reserve Component (RC). The RC MOS qualification schools for 97E and 97B typically ran two years, which equated to a year of weekend drills (one weekend a

month), one two-week annual training period, and the same time requirement repeated the following year. This had huge implications on unit readiness and still does. Only recently has USAIC&FH been moving toward creating a one-year program of instruction (POI) for these MOSs, with 96B (Intelligence Analyst) being the first.

The recommendation was to create a linguist MOS so the Army could train these linguists in a minimal amount of time with plans to transition them into one of the MI linguist MOSs. This would allow the 300th MI Brigade—with battalions in Utah, California, Florida, Washington, and Louisiana, and companies in Chicago and Boston—to show a higher readiness status while servicing many of the Army's documented and undocumented pure linguist requirements. The Brigade eventually converted 40 percent of its force structure to 97L.

In an off-site agreement around the same time, the U.S. Army Reserve (USAR) and Army National Guard agreed to a force restructuring. The USAR basically signed up to provide forces to echelons corps and above while the Guard agreed to focus on echelons corps and below. As a result of the off-site agreement, the USAR saw the reduction of approximately 10,000 MI slots to around 2,500 in 1995. In an effort to salvage some of this MI structure, and under the direction of LTG Claudia J. Kennedy, then the Army Deputy Chief of Staff for Intelligence, the USAR created eight MI companies comprised primarily of the 97L MOS. Two years later, they "grew" the structure to six battalions, but by 1999, the USAR reduced that number back to eight almost entirely pure 97L companies.<sup>2</sup>

## 97L: A Good Idea Gone Bad?

The 97L MOS had potential. However, it suffered many obstacles throughout its relatively short life span, not the least of which was the reluctance of the Active Component (AC) to support any 97L force structure. The other issues with 97L snowballed from there. The linguist doctrine never materialized even though 97L

had been in existence for nearly eight years. Since there was no solid doctrine, commanders never understood how to use 97L soldiers as became clearly evident in operations since 11 September 2001.

Other seemingly insurmountable issues existed like the lack of any noncommissioned officer (NCO) courses, no grade structure above E6, and no documented warrant officer positions, thus creating no logical or possible career progression. The RC could recruit only “heritage” linguists into 97L. In other words, 97L soldiers had to come into the Army with a language. This became a virtually impossible task from the start when taking into consideration the vast requirement for Arabic and Persian Farsi linguists. Where was the RC to find a recruiting pool large enough to fill these requirements?

The 97L MOS qualification process had only been ironed out around the year 2000. By this time, the USAR had already earmarked their linguist units for transition to hard-skilled MI units (97E, 97B, 98G, etc.) in support of the new theater intelligence brigade/group and corps support battalion structures, thus moving away from the 97L mission.<sup>3</sup> This left the 300th MI Brigade (Linguist) as the only organization in the Army possessing this MOS. At this point, the 97L MOS had grown into far more than what it was originally intended to be: an apprentice MOS for 97E, 97B, and later 98G, and was mired in too many issues to make it truly viable. It was time for the National Guard—specifically the 300th MI Brigade—to join its RC sister, the USAR, and transition its force structure into something more viable.

## The RC Multicapable MI Linguist

*“Modular, capabilities-based Army force designs will enable greater capacity for rapid and tailororable force capability packages and improve the strategic responsiveness of the Joint Force for full spectrum operations.”*

—The Way Ahead, General Peter J. Schoomaker,  
Chief of Staff of the Army

The intent of LTG Alexander’s memorandum is to transition the existing 97L force structure into assets that are a better solution for the Army by providing a soldier capable of meeting a number of requirements. This concept proved to be invaluable during some of the 300th MI Brigade’s recent mobilizations. By January 2002, the Brigade had mobilized approximately 700 soldiers. Of those soldiers, 3 percent served in linguist-only missions, 4 percent required

language and an MI MOS skill (97E, 97B, or 98G), while 93 percent required only MI skills! Imagine if these soldiers had been 97Ls. They would have been able to satisfy at the most seven percent of the mission requirements leaving the remaining very capable soldiers in the brigade at home waiting for their language requirement to pop up. If the Brigade had more Arabic linguists, the Army would have deployed them to use their language skills. However, the Brigade is not programmed under the auspices of the Army Language Master Plan (ALMP) to have more than 17 percent of its force structure dedicated to any one language.<sup>4</sup>

The idea of a multicapable soldier fits nicely into General Schoomaker’s plan of creating soldiers who are flexible, adaptive, and competent. The mission of the 300th MI Brigade (Linguist) is generally agreed to be a pool of MI linguists that the Army could package for any operation or contingency. The brigade has nicely structured derivative unit identification codes (UICs) so we can tailor it easily to meet any size requirement. Brigade soldiers have served in the most recent conflicts in a variety of force packages in a variety of roles.

Other than in the 300th MI Brigade, all the other MI linguist billets in the ARNG and USAR serve with MI divisional battalions, MI companies in the enhanced separate brigades, tactical exploitation battalions, corps support battalions, theater support battalions, Special Forces units, and other specific MI organizations. These linguists are already required to serve as multicapable MI linguists as well as being HUMINT Collectors or Cryptologic Linguists.

There are some who believe the RC soldier is not capable of being a good linguist and functioning simultaneously in a hard-skill MI MOS. History has proven the contrary. The fact is those linguists who are engaged in real intelligence missions requiring their language skills are better qualified. Many are comfortably working at the higher language proficiency standard and some are even experts in many dialects. Technology has greatly enhanced the ability for RC soldiers to work HUMINT and signals intelligence (SIGINT) missions even on drill weekends.

Those who argue that linguist readiness is lackluster in the RC may not realize how successful they have been given their extremely limited resources. RC soldiers only receive 4/30th (the equivalent of four days a month) of Foreign Language Proficiency Pay

(FLPP) (about \$13.00 per month) while still maintaining the same proficiency standard as those linguists on active duty. Another example indicates the funding of RC has historically only been around 30 percent of their requested budget from the Total Army Language Program (TALP). This caused one officer to exclaim to the former Department of Army (DA) G2, LTG Robert W. Noonan, Jr., *"This is a good news story. If the Reserve Component can maintain the current level of proficiency while only being funded 30 percent of TALP, imagine what it could do with increased funding."*<sup>5</sup>

There are many other unique capabilities that RC MI linguists bring to the fight. Consider the following points.

**Some of the most talented linguists are in the RC.** Many RC linguists have not only learned one second language but, in some cases, multiple languages. Many gifted linguists work in the ARNG or USAR. There are many linguists who have expressed a desire to learn additional languages at the expense of leaving their civilian employment for up to a year, learn one of the difficult Category III or IV<sup>6</sup> languages, and even risk the possibility of deploying for a year.

**RC soldiers do not move very often.** Unlike AC soldiers, RC soldiers typically only change units when they move because of a civilian job, they are seeking promotion, or they just want a change. It is not uncommon for RC soldiers to stay in the same unit throughout their entire careers. This can be very beneficial considering that an RC linguist can work the same target area for years. For example, reflect on the rotation AC soldiers make through Korea. AC soldiers will spend one to five years total on the Peninsula, while an RC soldier has the potential of focusing on Korea during his or her entire career. It is not uncommon to see RC soldiers with a 10-year device or higher on their Reserve Components Overseas Training Ribbon denoting they have served at least that many assignments in country. One warrant officer in the 300th MI Brigade, for example, proudly wears a "27" on his ribbon, while the Brigade Command Sergeant Major also has in excess of 20; both are Korean linguists.

RC HUMINT collectors are linguists from the start. Based on the Military Occupational Classification and Structure (MOCS) packet that has been circulating for approval, the future 97E HUMINT Collectors will not receive language training until completing their first terms of enlistment except under certain conditions. RC lin-

guists will fall into that exception because the Army slots them against language-coded billets. In addition, RC linguists must receive language training during initial training. What this implies is that the E5 97E soldier from the RC will have been speaking the language since entering the Army, while the E5 97E active duty soldier will have just completed language training.

## The Future

MI linguists in the ARNG and USAR uniquely serve the Army. Their future readiness depends on leadership from all levels of the Army. The following are four recommendations to improve MI linguist readiness in the Reserve Component.

**USAIC&FH must continue to pursue the development of a one-year RC program of instruction (POI) for MOSs 97E, 97B, and 98G.** We must qualify our soldiers quicker so they can more rapidly serve the Army. The U.S. Army Training and Doctrine Command (TRADOC) and USAIC&FH must employ more effective methods of training such as the use of distributed learning. They should not build courses based on the standard hours of instruction but should focus more on whether soldiers can perform the tasks.

**The Army must resource the Reserve Component better to improve language skills.** There are a number of potential areas for improvement. Some include the following:

- ❑ As language requirements shift due to the changing world situation, the Department of Army must adjust the language mix in the ALMP. As units change language force structure to adhere to the ALMP, DA must adequately fund RC linguists in new language acquisition.
- ❑ Find something better than the current Foreign Language Proficiency Pay. The RC has fought to get full FLPP for years with no success. The current prorated proficiency pay is somewhat of an insult and is the brunt of much ridicule. Many good ideas have been under discussion for many years from bonus pay to additional drill pay. The Army needs to have a better means of rewarding soldiers for their efforts to maintain language proficiency, especially RC linguists who must study almost exclusively during off-duty periods and still maintain the same proficiency level as active duty soldiers.
- ❑ Develop new sources of funding to send RC linguists to the Defense Language Institute (DLI) and other language acquisition institutions to

learn additional languages and dialects. RC soldiers are worth the investment and in many cases have a longer “shelf life” than an AC soldier.

- ❑ Keep the TALP dollars coming. This has been an effective means for units to resource language training as its developers envisioned. The Army must hold commanders accountable for the effective use of these dollars.

### **Use technology more extensively to enhance language skills in training and operations.**

- ❑ **Training.** The DLI is obviously the first source to consider for language maintenance materials. However, a number of commercial off-the-shelf products such as Rosetta Stone and Auralog are in use by the Army and are very effective. One of the most exciting language training opportunities incorporating technology is the Broadband Intelligence Training System (BITS) developed by USAIC&FH. BITS allows an instructor to reach students anywhere in the world through the Internet. This has the potential of being especially beneficial to the RC linguist because it works well for geographically dispersed participants.
- ❑ **Operations.** ARNG and USAR units should continue their current support of SIGINT missions. These missions have produced the best-qualified and most motivated linguists in the National Guard and Reserves. The Defense Intelligence Agency has established a similar approach with the Reserve Language Support Program. This program to translate open-source materials has the potential of producing the same positive results as SIGINT missions if properly implemented. It is especially beneficial for HUMINT soldiers involved in document exploitation missions.

It is imperative for RC commanders to establish well-managed command language programs (CLPs) as specified in **AR 350-16, Total Army Language Program**. It is called “command” language program for a reason. When properly administered, the CLP can service the soldier properly and help that soldier to improve language proficiency over time. Commanders and first-line leaders must be fully familiar with this regulation and employ it as written. Many of the language readiness issues are attributable to the lack of command emphasis. This is especially true in the Reserve Component with such limited training time.

## **Conclusion**

The U.S. Army National Guard and U.S. Army Reserve have proven their value since 11 September 2001. At one point, the USAR had mobilized more than 90 percent of its MI force structure.<sup>7</sup> Many of those soldiers are serving in back-to-back mobilizations. The ARNG is under similar strains, serving not only in the Middle East but also in Bosnia-Herzegovina, Kosovo, the Sinai, and other regions. All have proven to be multicable, adaptable, and willing to accomplish the task at hand. The future of these great assets depends on how well we understand their value and take care of these soldiers in the near- and long-term future. The Army needs these linguists trained and mission ready, maintaining their perishable language skills. This is an investment the Army cannot afford to neglect.



### **Endnotes**

1. Memorandum for Deputy Chief of Staff, G3, Subject: Conversion of MOS 97L (Interpreter/Translator) Structure, from LTG Keith B. Alexander, DCS G2, dated 12 January 2004.
2. Major (MAJ) Elizabeth Coble, Deputy Chief, Force Management Division, U.S. Army Intelligence and Security Command (INSCOM) G3, interviewed 28 January 2004.
3. Ibid.
4. Lieutenant Colonel Russell Long, Executive Officer, 300th MI Brigade (Linguist), interviewed 19 February 2004.
5. MAJ Gregory Hadfield, Chief, Intelligence Branch, Army Operations Division, National Guard Bureau, interviewed 27 January 2004.
6. Category III languages include Czech, Filipino, Greek, Hebrew, Persian Farsi, Thai, Polish, Russian, Serbian/Croatian, Turkish, and Vietnamese. Arabic, Chinese Mandarin, Japanese, and Korean are all Category IV languages.
7. Coble interview.

*Lieutenant Colonel Jeffrey Mitchell is currently a Senior Service College Fellow at the University of Texas. He is a U.S. Army National Guard (ARNG) officer who has served in a variety of command and staff positions in Military Intelligence, Infantry, and Field Artillery. He worked force structure issues at the Directorate of Combat Developments, USAIC&FH, at Fort Huachuca, Arizona, from July 2001 through September 2002 while simultaneously commanding the 142d MI Battalion (Linguist) in Utah. LTC Mitchell holds a Bachelor of Arts degree in German and a Master of Science in Instructional Technology, both from Utah State University. He is a graduate of the Command and General Staff College, Combined Arms and Services Staff School, MI Officer Advanced Course, Infantry Officer Transition Course, and the Field Artillery Officer Basic Course. Readers can reach the author via E-mail at jeffrey.mitchell2@us.army.mil and telephonically at (512) 232-4560.*

# **EXCESS REPORTING—**

## **HAND OFF ISSUES FOR BOTH HUMINT COLLECTIONS AND CI AGENTS**

by Master Sergeant Lisa A. Connors

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

As Phase IV operations (stability operations) in Iraq continue, counterintelligence (CI) agents and human intelligence (HUMINT) collectors should heed lessons from previous long-term rotational operations. Operations in Bosnia-Herzegovina and Kosovo have been ongoing long enough for collection patterns to become readily apparent. Similar patterns are emerging in Afghanistan and Iraq.

### **The Problem**

Analysts covering regions where several rotations have occurred notice a flood of reporting when new collectors begin working. Part of the increase in activity is likely due to the enthusiasm of newly arrived collectors. Perhaps the collectors have no experience in the region or several rotations have passed since the collectors were last in country and the situation has changed considerably. However, much of this excess reporting is due to repeat reporting or information from unreliable sources. When collectors can correctly identify some of the factors contributing to the excess of reporting at the rotation, the analysts can better focus on more valid reporting and they can greatly enhance the analysis. These factors can include foreign intelligence security service (FISS) interference, the sympathetic ear, talk radio and yellow journalism, and coalition complexities.

**FISS Interference.** Foreign governments may see the new collectors' relative inexperience with the current situation as an opportunity to influence U.S. interests in the region or mislead U.S. policy makers. They may also see it as an important opportunity to inject deceptive information.

Compared to the United States, many countries exercise a greater degree of internal control over their civilian populations, and their FISSs frequently extend further into the local community in other countries than they do into the United States.<sup>1</sup> FISSs, even those from friendly nations, routinely are aware of and observe U.S. intelligence activities. Governments desiring to place bogus or biased information into U.S. collection efforts can

task their intelligence services to do so. A FISS operator could contact the U.S. collector directly, making use of the new collector's lack of familiarity with local FISS methods and operators, or, more likely, could use an intermediary to feed information to the collector.

Other organizations can use similar methods. They may include opposition political parties, national liberation movements, organized crime factions, and extremist groups.

**The Sympathetic Ear.** Every town has its fanatics, drunks, gossips, and rumormongers. They will go out of their way to approach collectors and share their points of view. New collectors often provide a sympathetic ear. Veteran collectors know which of these people to avoid; however, this realization may come only after they have fed several reports, based on information provided by these dubious sources, into the system.

**Talk Radio and Yellow Journalism.** Another factor contributing to the excess of reporting immediately after a rotational change is the repetition of media reports. Initially difficult to detect, rote repetition of media reporting can flood message traffic with biased opinion or fabrication reported in the media as fact by sincere and otherwise reliable sources. Too much reporting that repeats media information adversely affects the credibility of the collector in the eyes of the all-source analyst, who may then discount legitimate collection by that team or unit.

For example, in 1996 the Serbs in Bosnia had an active, well-organized information campaign targeting North Atlantic Treaty Organization (NATO) members using a seamless military-political-media continuum. The majority of the population was literate and trusted the established local media sources.<sup>2</sup> The new lack of centralized media control and freedom of the press led to uncorroborated reporting that many believed and passed on as fact.

**Coalition Complexities.** U.S. forces are conducting operations with increasing frequency in a coalition environment, adding to the possibility of duplication of effort and same-source reporting from more than one organization. In addition, collectors obtain information from varying non-traditional sources such as civil affairs and psychological operations personnel

who may be speaking to the same sources, such as political or media figures.<sup>3</sup>

## Solutions

Stemming the tide of excess and irrelevant reporting surrounding unit rotations requires the one commodity most in demand during periods of high operations tempo—time.

Collectors must spend time before deploying to study Intelligence Community publications regarding the FISS objectives, activities, and personnel in their area of operations to identify better the FISS attempts to influence collection. Once CI agents identify the FISS influence, the agents can neutralize it.

While time consuming, longer and more detailed hand-offs involving experienced and new collectors physically visiting collection sites together so that they can visually identify known unreliable sources can reduce effort wasted as the “sympathetic ear.” Lists or databases of confirmed “non-sources” with names, locations, and physical descriptions can further aid new collectors in identifying gossips and rumormongers; the analysis and control element (ACE) or 2X staff can maintain these databases to ensure continuity between rotations.

Media awareness is essential to quell the persistent problem of media report repetition. Language barriers often prevent collectors from following radio and television broadcasting or reading periodicals; however, collectors should check the Federal Broadcast Information Service (FBIS) or in-theater media exploitation assets regularly. The Task Force Eagle maintains the *Tuzla Night Owl*, an excellent model of a daily media exploitation database. In addition, collectors must verify the initial source of in-

formation, particularly if the same story, practically word for word, crops up from widely disparate sources.

Other nations are often reluctant to share source information making it difficult to determine if same-source reporting is occurring. However, by clearly defining the geographic locations and elements of society where each nation will focus their collection efforts, the G2X can deconflict collection operations.

## Conclusion

As long as CI agents and HUMINT collection teams continue to collect in rotational operational environments, the problem of excess or irrelevant reporting after a rotation shift will persist. Only after we devote additional time to collector preparation and the collectors learn to adapt to new work environments will the problem gradually ease.



### Endnotes

1. Ibid.
2. Wentz, Larry K., Contributing Editor, **Lessons From Bosnia: The IFOR Experience** (Fort McNair, Washington, D.C.: National Defense University, 1998), Chapter IV, Intelligence Operations.
3. Ibid.

*Master Sergeant Lisa Connors is a U.S. Army Reserve soldier currently on active duty with the Department of Defense and assigned to Camp Zama, Japan. Previously, she served as Course Manager for the Reserve Component Defense Strategic Debrifee Course. MSG Connors attended both the Russian Basic and Polish Basic courses at the Defense Language Institute and holds a Bachelor of Arts degree in Eastern European Studies. Readers can reach the author via E-mail at lisa.a.conners@us.army.mil or at DSN 315-263-3354.*

## Doctrinal Notes

*The following is provided to avoid a possible misunderstanding of the fundamental nature of HUMINT and CI.*

CI agents and HUMINT collectors support the commander in different ways. The CI agent's goal is to deny the enemy a clear picture of the activities and plans of friendly forces. The HUMINT collector's goal is to gather information that provides the commander with a picture of the activities and plans of the enemy. In other words, CI shapes Red's (Threat Forces) picture of Blue (Friendly Forces); HUMINT shapes Blue's picture of Red.

CI agents and HUMINT collectors are soldiers who have received different training to conduct different missions. CI agent training focuses on methods to detect and counter enemy intelligence efforts and to conduct investigations. They carry federal credentials as Special Agents.

HUMINT collectors are trained in questioning, elicitation, debriefing, and interrogation techniques. They are not credentialed.

Unfortunately, a continuing shortage of HUMINT collectors often requires commanders to rely on CI agents for missions for which HUMINT collectors are better suited. Commanders faced with a shortage of HUMINT assets may have to task organize CI agents or other personnel (MI and other specialties), and HUMINT collectors into non-doctrinal Tactical HUMINT Teams (THT) in order to meet the HUMINT collection requirements within their Area of Operations (AO). In spite of this shortage, commanders should make every effort to employ their CI and HUMINT assets in accordance with their training and capabilities, not as interchangeable parts.

# **Lessons Learned From OIF: An SF Battalion S2's Perspective**

by Captain Brian Gellman

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

The purpose of this article is to offer some lessons learned from my tour in Operation IRAQI FREEDOM (OIF). Due to the unique nature of my job as a Special Forces battalion S2, I had the opportunity to observe and participate in the tactical, operational, and strategic levels of intelligence. The observations below are not restricted to any specific part of the country or any specific phase of the war; rather, they are general observations noted by the author and others in the theater.

While the target audience of this article is tactical-level intelligence professionals operating or planning to operate in the Iraq Theater of Operations (ITO), many of these lessons are applicable at all levels of the intelligence community. This article begins with some comments that are generally applicable to S2s and then moves to some specific to the ITO. The topics covered include networking, selling your assessment, intelligence support to information operations, dissemination versus fusion, targeting and exploiting, insurgency targeting cycle, reporting standards, conveying locations in populous areas, naming conventions in OIF, and spotting foreign fighters.

## **Networking**

Networking is an invaluable tool for an intelligence officer in OIF. After eight months in theater, the author developed contacts in almost every intelligence element in theater, to include coalition partners and interagency personnel so when an issue or problem arose, a contact was available in nearly every case who could work with us to solve it. I made it a point to meet everyone with whom I corresponded via E-mail on a regular basis (when practical), which aided the flow of information.

Networking is not an easy task to accomplish in a nonpermissive environment (that is, where we

lack freedom of movement). Take every opportunity available to get out of the work area to visit other units. Find a good reason to visit your higher headquarters and any other intelligence-producing element in theater.

## **Selling Your Assessment**

An S2 section does an analysis of the city of Baghdad and determines that a specific highway is critical to coalition operations. The S2 then recommends that efforts focus on the least stable district(s) along the highway to ensure the route remains open. However, no action is taken until after an improvised explosive device (IED) attack shuts down the highway for a 12-hour period.

Intelligence is useless if your commander does not accept it. One can discover the "golden nugget" of intelligence that will lead to the capture of Saddam Hussein and Osama bin Laden and a suitcase nuclear device, but if you cannot sell it to the commander, one will never truly know what could have happened.

Here are some tips for making your first "sell":

**Establish Credibility.** There are multiple ways to establish credibility and rapport with your commander. The first, and most obvious way is to make correct assessments. This will come with time but will not help your first sell. As an intelligence professional, you will be wrong more times than you are right. However, here are some things that S2s can do to establish credibility without being right all the time.

- It is imperative to speak the language of the commander. Generally, that language is doctrine. Impress the commander with your understanding of operations and of doctrine.
- Understand operations and the decisions your commander has to make. If your reporting and

assessments are not relevant to the commander's mission, why are you briefing them to him or her?

- ❑ Tell the commander what he needs to hear, not what he wants to hear. A commander must understand the situation from different perspectives, and the S2 brings the commander the threat's perspective. If the commander does not agree with your assessment, do not back down but respectfully "agree to disagree."
- ❑ Prepare yourself and the S2 analysts for the brief. Rehearsals are important for anyone conducting the brief. Rehearse the brief with others and "sharp shoot" each other. One goal of this rehearsal is to predict any follow-up questions the commander will ask you. Be prepared to answer these questions when asked, or simply brief it before the commander has the chance to ask.
- ❑ Know your commander as you know your enemy. Know what your commander expects. For example, some commanders want to know the source of every report. Every commander also has pet peeves, quirks, and peculiarities. Be aware of them and try to minimize their impact.

**Presentation.** Presentation is everything. A poorly presented assessment will affect your credibility and will greatly decrease your chance of getting the assessment accepted by the decision makers. Keep it simple, logical and easy to follow. Explain your thought process step-by-step, leading the commander to the most logical, threat-based assessment available, yours.

For difficult situations, use terms and formats with which the commander is comfortable. For example, S2 analysts may assess that threat forces are using school assemblies to plan operations and recruit, and your recommendation to the commander is to break up the assemblies. When conducting mission analysis, use a format that he is used to hearing, such as OAKOC (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment).

- ❑ **Observation and Fields of Fire.** The threat elements conducting the assembly have clear observation and a clear field of fire to their targets, the students (potential recruits). This forum favors the threat because it isolates the key terrain. During operations in cities, streetlights at

night affect observation, countering the advantage of night vision.

- ❑ **Avenues of Approach.** The threat spreads lies about the coalition forces and instills fear; this appeal to the students' fear and gullibility is the major avenue of approach. This element favors the threat because they better understand the needs and desires of the youth, and can therefore manipulate them more effectively. Do not forget that an urban environment is a three-dimensional world so underground tunnels, subways, and storm drains should be considered avenues of approach as well.
- ❑ **Key Terrain.** In this situation (the school assembly), the hearts and minds of the youth in the community are the key terrain. Who are the key leaders or sheiks in the community? Whoever seizes this terrain is favored in the long term.
- ❑ **Obstacles.** Obstacles could include rules of engagement (ROE), a language barrier, or cultural misunderstandings that may lead to second and third order effects on a given course of action (COA). These obstacles favor the threat and hinder our ability to prosecute the target. In addition, vehicular or pedestrian traffic is an obstacle during certain hours of the day.
- ❑ **Cover and Concealment.** To conceal their intent, assemblies may be in schools because they are beyond our intelligence, surveillance, and reconnaissance (ISR) collection capabilities. A school meeting serves as cover for their true intent. This cover and concealment limits our ability to collect and then justify an offensive mission (justification may be required to accept the risk of losing favor in the community).

**Facts, Figures, and Historical Examples.** Sometimes one bases assessments on patterns and probabilities; sometimes intuition rather than actual hard fact forms the basis. Commanders may consider this to be "gray" when they want "black or white." Something more concrete to back your assessment is helpful.

First, commanders in general are students of history. Use historical examples from current or previous conflicts to back your assessment. Second, beware of statistics. Statistics can "lie" if users produce or manipulate numbers to prove or disprove any theory

they want. If you are careful, statistics can be effective in the absence of other data, but again, this S2 stresses caution.

Note that intuition is a critical ingredient in the success of an intelligence professional. Intuition is the result of the combination of knowledge (e.g., schools, doctrine, and history books) and experience. Do not be afraid to use intuition—many times it will be all you have on which to base your assessment. However, if you do base an assessment purely on intuition, you should let your commander know.

## Intelligence Support to Information Operations (IO)

Intelligence did not drive IO; often, political issues or reactions to bad press drove it. IO planners failed to tap the greatest collection resource available in Iraq, the “presence patrols.” Planners did not issue relevant talking points to these patrols. (For example, at a time when electricity and water were still major concerns in the city, IO planners wanted presence patrols to talk about when and how the Iraqis would exchange old currency for new Dinar.) They did not order IO-driven information requirements. When issues regarding IO appeared in reports, there was no system in place to route these issues directly to IO planners quickly and then in turn send authorized responses to the presence patrols.

Intelligence must also provide IO with the threat’s IO plan. During the military decision-making process (MDMP), intelligence planners should develop most probable and most dangerous COAs for the threat’s IO response. This can allow IO planners to be proactive instead of reactive. Intelligence can also provide summaries of the threat’s IO message delivered through electronic and print media. Tactical human intelligence (HUMINT) teams (THTs) on the streets can report threat IO messages circulated through rumors and public assemblies (sermons). However, we cannot rely on THTs alone to provide ground truth reporting. The best and most plentiful intelligence collectors on the battlefield are the presence patrols.

Presence patrols can also assist by providing “ground truth” information and measures of effectiveness. These patrols can determine whether an IO theme or message is reaching the target population, and then report this feedback to IO

planners. IO planners can then determine the effectiveness of their means of delivery. This entire process can be accomplished in a four-stage continuous cycle.

- ❑ Stage 1. IO planners task presence patrols to collect information on issues and concerns of the local population. This information goes directly to IO planners through dedicated channels to ensure timeliness of information receipt.
- ❑ Stage 2. IO planners process information sent from presence patrols and determine what the primary issues are on the street. The planners staff the issues and develop responses that they formulate into IO themes and messages for delivery via multiple means (e.g., psychological operations [PSYOPs], media, and the public affairs office [PAO]). They issue talking points as an order to the presence patrols to help spread the message as well.

Measures of effectiveness are critical to the success of IO. IO planners measure success by determining what percentage of the population must receive and understand the message to consider the IO mission a success.

- ❑ Stage 3. Presence patrols simultaneously deliver the message to the targeted population, gather feedback, and collect new issues. The patrol will determine if the target population received and understood the message. If the message is not reaching the desired audience, the patrol can make an assessment of why it did not. They will send this information directly to the IO planners.
- ❑ Stage 4. IO planners analyze the feedback to determine what percentage of the target population received the message. If the standard is met, the planners may decide to discontinue the message. If the standard is not met, the planners may reevaluate the method of delivery and the message itself—they can only do this effectively with the feedback from the presence patrols. Planners also receive new issues from the collectors and the cycle starts again.

This is nothing more than a modification of the intelligence process. Since units at the brigade level and lower usually do not have IO officers, the intelligence officer must become the IO officer by default. The intelligence officer needs to incorporate these talking

points into his or her collection plan and also the daily patrol debriefs. (Another candidate as the IO officer is the fire support officer [FSO]).

Detainees will provide much information that is of value to IO. If you want to know why the bad guys are fighting, ask a detainee. S2s should assess second and third order effects of tactical operations and civil-military operations (CMO). In a land where nobody speaks English, actions are the IO operation.

Understanding local history, culture, and geography is critical to successful IO. First, an S2 must realize that all people have certain needs. People across the board, regardless of race, religion, or creed, will first worry about the basic necessities: food, shelter, water, and the safety of their families. Once these things are taken care of (and only after they are taken care of), will other factors in their lives come into prominence. Second, an S2 must know the local culture. This is crucial to ensuring that the IO plan works and is important to all other aspects of the fight.

## Dissemination Versus Fusion

Dissemination is the act of getting intelligence to the consumers. Dissemination does not guarantee that the consumer who needs the intelligence will get it and tends to be unidirectional. One can define "fusion" as "intelligence disseminated to the consumer who needs it," which allows a synergistic effect of shared intelligence. Good fusion is multidirectional and allows for exchange of ideas and analysis both horizontally and laterally.

Intelligence is useless if we do not disseminate it to the consumer who needs it. Intelligence dissemination can be active or passive and "push" or "pull" is often how we describe it. "Push" intelligence is intelligence that the generating unit sends to the consumers while "pull" intelligence requires the consumer to retrieve the intelligence.

Having to go to a unit's tactical website or web information center is a perfect example of "pulling" intelligence. The consumer must surf through multiple pages and menus to find the intelligence that he is seeking. If the consumer does not know what exactly he wants (or the right terminology to use) or is not familiar with the tactical website, it can be a slow process. This also assumes that consumers outside the tactical site can even access it. Often bandwidth restrictions, firewalls, and other security measures make it very difficult and slow

for outside consumers to "pull" intelligence from such a site. Of course, the consumer may not even know that the intelligence exists. (This should not be considered tactical website bashing; it is a good tool but is a very passive means of disseminating intelligence).

"Pushing" is a very proactive process, and we found this is the best way to get the intelligence to the specific consumers who need it. It requires a soldier who understands the mission of other friendly units in the area of operations, knows their priority intelligence requirements (PIRs), and has a point of contact and means of disseminating the intelligence to that consumer in a timely manner.

One way of accomplishing this is to have liaison officers (LNOs) from the consumer units in your section. However, this is impractical because you would need an LNO for every unit in the theater. This author thinks that a huge "fusion pit" located at the joint task force headquarters is a waste of personnel resources; it slows the process down and is ineffective. This would be an attempt to centralize control of intelligence in a decentralized war.

It is more practical to designate one soldier (or a small section) as the dissemination specialist for a unit. The job of the dissemination specialist is to ensure that intelligence reaches the consumers, both horizontally and vertically across the chain of command. The tactical website has its uses, and is effective for internal sharing, but the dissemination specialist needs to help out the external intelligence elements by disseminating specific intelligence to the unit that needs it; the specialist can accomplish this through good sharing of operational information between units. The unit's dissemination specialist needs an address book or access to a courier that can contact as many units in theater as possible. The dissemination specialist should have access to information on each units' mission statement, area of responsibility (AOR), and PIR. Also, it is not enough to simply understand other military units' missions. There is currently little in the way of formal information sharing between military and civilian agencies. This is where personal networking is really important and can pay huge dividends for the unit.

This is a huge job but it can be done, we did it on a smaller scale. While we did not need to understand the mission of every unit in theater, this S2 did have a long list of contacts throughout the country, and anytime a detachment in the battalion collected pertinent intelligence, that specific report went directly to the point

of contact who worked that AOR or that mission. For example, if a detachment collected information on a mosque, the S2 section did analysis and we passed that intelligence via Secure Internet Protocol Router Network (SIPRNET) directly to the brigade or division responsible for the AOR containing that mosque.

We also found that the points of contact that received our intelligence were more willing to help answer our PIRs and sent intelligence directly to us. This is decentralized fusion for decentralized warfare. Someday some great supercomputer database, perhaps a future joint interagency All-Source Analysis System (ASAS) version, will figure out how to do this for us. Until then, thinking, breathing soldiers will need to accomplish this task.

## Targeting and Exploiting

A successful raid captures a targeted individual. The raiding element leaves the objective with a cell member, a small bag of money and smiles on their faces. The next day, the source that led the unit to the target reports that the cell leader lived next door and has already left town as a result of the raid. The smiles are gone.

The raid is not over once you have positively identified the target. Intelligence exploitation of the objective is critical to the targeting process and maximizes our efforts. Threat personnel usually do not work alone and the raiding element can derive a lot of information from site exploitation. To assist raiding units during exploitation, S2s should develop and enforce a standing operating procedure (SOP) that clearly defines what actions should take place during exploitation. The following is a short but not exhaustive checklist for site exploitation.

*Editors Note: Combined Arms Doctrine Directorate (CADD) is developing ST 3-90.15, TTP for Tactical Operations Involving Sensitive Sites. Publication data is unknown at this time.*

- ❑ An initial battlefield interrogation by HUMINT collectors of the target can yield information that the unit can act on immediately if the ground commander is prepared to do so.
- ❑ What do the neighbors know about the target just hit? If the locals felt secure enough to talk to you, they might say, “*go hit that house right across the street, all of your target’s friends are in there.*” Talk to everyone you can.

- ❑ Anything that stores information has potential intelligence value. Grab it, bag it, and label it. It is imperative to label bags with a list of contents, date and location of capture, and circumstance of capture at a minimum, and ensure that the exploitable materials reach the appropriate entity. The S2 must be involved in the “chain of custody” of detainees and exploitation of materials. The operations order (OPORD) must spell out what the raiding element is seeking, how to handle captured items, and where they should go.

Occasionally S2s failed to recognize that the small cell in their city has connections to larger cells elsewhere. In this decentralized war, it is important for intelligence officers at the lowest level to have a basic understanding of the “big picture.” The S2s can then determine how their little piece of the war ties into that picture. In counterinsurgency, the lines between tactical, operational, and strategic levels are completely blurred. A cell leader can at one time have strategic intelligence value and be planting IEDs at night, etc.

## Insurgency Targeting Cycle

The following discussion is a modification of the technique used by 1st Brigade Combat Team (BCT), 1st Infantry Division. It covers the detect, decide, deliver, and assess phases of the cycle.

**Detect.** There are three types of targets you can detect using multiple disciplines; however, at the tactical level most of the collectors will be HUMINT. At higher levels, more all-source integration is available including reach capabilities to national agencies like the National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA, formerly NIMA [National Imagery and Mapping Agency]), Defense Intelligence Agency (DIA), etc. These types of targets include—

- ❑ Target personalities.
- ❑ Target areas commonly targeted by insurgents where we can conduct counterambush operations.
- ❑ Local CMO opportunities.

**Decide.** This phase uses tools including link diagrams and association matrices for personalities. These tools help the commander determine if and why the unit should prosecute a target. Then the commander needs to decide—

- ❑ If sufficient credible intelligence is available to hit a target. Locals will use U.S. forces to sort out their local politics. Source deconfliction and reporting from multiple intelligence disciplines can resolve this.

- Which targets to prosecute, where and when. In a target rich environment, it is crucial that the S2 assists the S3 and commander in deciding which targets to go after first and how to allocate limited resources to achieve desired effects. (For instance, counterambush operations are an effective and proactive means of hunting IED cells, but they are personnel intensive. Figuring out which house to hit is another example.)

**Deliver.** Use aerial observation (preferred), HUMINT sources, and/or observation posts (least preferred) to determine target patterns. Then conduct the raid, put out the counterambush force, or do the CMO project.

**Assess.** For raids, this consists of interrogation and document exploitation. These are extremely important because they confirm who you caught, provide needed evidence to hold the target(s), and nearly always lead to another target. For counterambush operations, the assessment would be dead and captured insurgents and a change in the attack trends in the targeted area. For CMO, the usual feedback is gathering information through PSYOPs surveys. For instance, we knew that our operations to counter black marketing were working when locals reported the price for black market fuel was down to almost the same level as legal fuel.

## Reporting Standards

Reporting during the initial phase of OIF operations following the fall of the Iraqi regime was poor and there was no standard in use. The senior leadership quickly recognized this problem and the SALUTE (size, activity, location, unit, time, equipment) report became the standard. This improved our ability to determine what time of day and what parts of town were more likely for attacks. While the attacks still seemed random, they were not. The majority of the attacks were against civil affairs and engineer units, while attacks on infantry and Special Forces elements were very rare. (This trend changed over time as the attacks became more sophisticated.)

The SALUTE report has been the Army standard for decades. It is a simple and effective report for most operations. It is an excellent format to use for initial reports but reporting has a tendency to stop there. The SALUTE report, designed in a time when means of conveying battlefield information were very limited, conveys the information on who, what, when, and where. On a linear, symmetric battlefield, enemy action is often to disrupt the timing of our operation

- Date-time group (DTG).
- Location.
- Reporting unit.
- Patrol mission.
- Activities conducted by patrol prior to attack
- Mounted or dismounted? What was the size of the patrolling element?
- What types of vehicles or weapons systems were in the patrol?
- Route used by patrol? Has the patrol used this route in the last week and at what times?
- Patrol stationary or moving?
- Was fire returned?
- Description of attackers (numbers, dress, weapons, tactics, techniques, and procedures (TTPs), etc.)
- What was the result of the contact (enemy and friendly)?
- Were there civilian bystanders? What were their reactions?
- Detailed description of attack site.
- Why was the patrol attacked (patrol's assessment)?

Figure 1. Other Suggested Reporting Requirements.

or to protect or seize specific terrain. The where and when of these attacks helped to explain the why. On the linear battlefield, the SALUTE report is usually enough for any intelligence analyst to figure out the last, most important piece, the why.

For example, a report may say two BTRs (armored personnel carriers), a T-72 tank, and 30 dismounted soldiers (unit unknown) at this grid and time fired upon the reconnaissance patrol. From this report, the analyst can assess that the enemy fired on the patrol because the enemy unit is a part of an integrated defense and is conducting a counterreconnaissance mission. The analyst can go a step further and assess that the reported element matches a template for a combat security outpost and can then use this information to template the entire defense using a doctrinal template.

Now try this example: Two unidentified individuals wearing disdashas dropped an IED on a U.S. convoy at this grid and at this time. More information is necessary for pattern analysis than simply time and place. Pattern analysis may help us determine what time of day or where these attacks are more likely to occur, but we still have not determined why. Why was

that convoy attacked instead of the one that passed that location ten minutes earlier?

On a nonlinear battlefield the threat is not overly concerned with terrain and often can dictate the tempo of the battle. The threat, by the definition of "asymmetric," has a smaller force and therefore must be risk-aversive to persist. They choose the time and place of their attacks, they pick a fight that they know they will not only win, but also from which they can escape. So how do they choose it and why do they attack one convoy or element instead of another? The threat is targeting easy or "soft" targets. So how does an analyst determine what the enemy considers a "soft" target? Information using the SALUTE format alone does not provide sufficient information to permit this type of assessment. Figure 1 includes some other suggested reporting requirements.

These reporting requirements are not ones to answer at the time of contact; rather, intelligence personnel should pose these questions to the patrol during the debriefing after the mission. Your unit needs to conduct regular patrol debriefs using a unit SOP (the questions in Figure 1 can be part of the debrief SOP). Using this level of detail, an analyst can assess why the threat targeted that particular convoy or patrol.

If the analyst sees a pattern emerging, that pattern can turn into engagement criteria. The analyst can then advise the commander of force protection measures to ensure that the convoys are outside the threat's engagement criteria, and are therefore at lower risk of attack. Engagement criteria can also serve as one piece of the puzzle in linking attackers to organizations. If we observe similar engagement criteria over a large area, this can be a useful indicator that some level of organization or training exists.

When possible, units should do full investigations and studies of attacks to learn as much about the threat as possible. With digital cameras and PowerPoint™, it is very easy to put together a graphical description of exactly how they conducted the ambush. It is also important to note that unsuccessful attacks require at least as detailed an analysis as successful ones do. Learning why an attack was unsuccessful can be extremely valuable in developing tactics, techniques, and procedures (TTPs) to defeat the threat.

## Conveying Location In Densely Populated Environments

Street addresses as we know them do not exist in Baghdad. Residential streets very rarely have

names unless they are major roads. There are no street addresses in Iraq because people define the terrestrial geography using human geography. In Al Anbar province (Governorate), names for locations on a map are based on the tribal group living there. This means that to figure out where a person lives, an S2 must understand the tribal history of the area. When asking a person where a target lives, a common type of answer is "*in the Nimr tribal area near Mohammed's house down the street from the mosque where Imam Hassan preaches.*" It may be twenty feet from the Euphrates River, but the source will not think to use that as a landmark because human geography is more important to their culture.

Without street addresses, units resort to the Military Grid Reference System (MGRS). A good HUMINT report may have an eight-digit grid of the target or better. However, we found that even ten-digit grids are not accurate enough pinpoint target locations in a densely populated environment. There are several reasons for this:

- Buildings are so close together that there is no room for error. If your grid is off a meter or two either way, the raiding element may be targeting the wrong house.
- A soldier using a Global Positioning System (GPS) usually cannot get close enough to the target for an accurate ten-digit grid.
- Imagery that is not orthorectified will not line up with a grid obtained on the ground. The variation can be 50 meters or more.

There are several things that can improve the location of targets in populous areas like Baghdad. They include:

- Always include a physical description of the target. This should contain enough detail to permit identification of the target from FalconView imagery and on the ground (day and night). The collector must provide a detailed picture, for example:

*"The target is a two-story house connected to other houses on both sides. The front door faces the street (north) and there is one window right of the front door. The second story has three windows facing north. The house is red-orange and made of plaster, with ceramic orange shingles and a six-foot white stone wall with an iron gate. The iron gate is black, opens toward the street, and has no visible lock."*

- Use digital photographs or video.
- Use a landmark. Acquire a ten-digit grid location of a landmark easily picked out on imagery such as a road intersection. The ten-digit grid number will likely not match up perfectly with the landmark; however, it should be close enough to pinpoint the landmark to be useful as a reference point. Using this reference point, report directions to the target from the landmark. For example, *“From the four-way intersection at MB1234567890, face north. The target is the third house on the left.”*
- If you cannot achieve clarity of intelligence and cannot pinpoint the target location, consider a larger cordon and plan on entering multiple houses. You can recommend a “cordon and knock” procedure to the commander to search all the potential targets until the patrol locates the target individual.

## Final Thoughts

How many times have you heard, *“Intelligence drives operations”*? It is a common catch phrase often quoted, but rarely realized. Here is the bottom line: Intelligence is at the center of everything we do, yet it is understood less than any other discipline in

warfare. We must collect and analyze information, put it into a package the consumers can understand, disseminate, and constantly reevaluate. All these tasks are mandatory for intelligence to drive operations, and if we as intelligence professionals do not do this, who will?




---

*The author developed the observations and recommendations above on collaboration with other intelligence professionals in theater including Captain Bret Woolcock, Combined/Joint Task Force (CJTF)-7 (now the Multi-National Force Iraq [MNFI]) Analysis and Control Element Targeting; CPT Mark Rowan, Ranger Regiment MI Detachment Commander; First Lieutenant Noel Cline, HUMINT Operations Cell, 1st Armored Division; CPT Kyle Teamey, Brigade Assistant S2, 1st Brigade, 1ID; and many others.*

*Captain Brian Gellman is currently serving as the S2 for 3d Battalion, 5th Special Forces Group Alpha (SFG(A)). He deployed to OIF after graduating from the MI Officer Transition Course and MI Captains Career Course. His earlier assignment was a branch-detail to the Infantry with the 1st Battalion, 27th Infantry Brigade, 25th Infantry Division (Light). CPT Gellman has a Bachelor of Arts degree in Psychology from the University of Texas at Arlington. Readers may contact the author via E-mail at brian.gellman@us.army.mil.*

## Doctrinal Solutions

Captain Gellman’s article highlights several crucial issues and procedures that recent doctrinal publications should solve.

**FM 2-0, Intelligence**, approved in January 2004, incorporated many of the recommendations included in the article. FM 2-0, defines “PIRs” in paragraph 1-32 as—

*...those intelligence requirements for which a commander has an anticipated and stated priority in his task for planning and decisionmaking. PIRs are associated with a decision based upon enemy action or inaction or the battlespace that will affect the overall success of the commander’s mission.*

Based upon the new definition, PIRs are what the commander needs to know about the enemy or environment. They focus the unit’s intelligence, surveillance, and reconnaissance (ISR) plan in order to support the commander’s situational understanding. Doctrine ties PIRs to a decision, not to a decision point.

PIRs still focus the unit’s overall ISR plan and higher echelons use them in developing their over-

all schemes of intelligence support. Greater use of intelligence requirements—those requirements for the Intelligence battlefield operating system (BOS) to fill a gap in the commander’s and staff’s knowledge or understanding of the battlespace or threat—better focus the intelligence support. During stability operations and support operations, these intelligence requirements have greater importance and emphasis.

FM 2-0 provides additional ISR guidance. Chapter 1 details ISR synchronization. This section explains staff participation within the synchronization process and the S2/G2’s role within the intelligence synchronization and ISR integration processes.

**FMs 3-0, Operations, 6-0, Mission Command: Command and Control of Army Forces**, and the draft version of **5-0, Army Planning and Orders Production**, all follow this thread. Units, leaders, and soldiers must incorporate these FMs into their section and unit standing operating procedures (SOPs) in order to benefit from this latest doctrine.

# The Intelligence and Electronic Warfare Tactical Proficiency Trainer— A Capability That Is Long Overdue



by Paul Menoher (Lieutenant General, U.S. Army, Retired) and Roger McNicholas

The Intelligence and Electronic Warfare Proficiency Trainer (IEWTPT) is absolutely critical to the Army and especially to Army Intelligence. It is imperative that Army Intelligence provides operational commanders the best support possible, and attendant to that requirement is the need to provide the best possible training to military intelligence (MI) soldiers. Looking forward to the Army's Future Force—which is underpinned by great situational understanding and precision targeting provided by vastly improved intelligence, surveillance, and reconnaissance (ISR)—the need for intelligence training expands exponentially.

## The Problem

A longstanding issue facing the Army is that there is only a limited amount of Army institutional training time available to produce fully trained operators, analysts, and intelligence staff officers. The fact that digital skills are perishable and will atrophy without a high-fidelity, multidiscipline in-unit training capability exacerbates this situation. Until now, Army Intelligence has lacked a multidiscipline, in-unit training capability to bring our MI soldiers (enlisted, noncommissioned officers [NCOs], and officers) up to, and maintain them at, the high levels of proficiency required to support their commanders. While in the past, talented and dedicated soldiers have done great things through commitment of extraordinary time and effort, it is clear that an effective in-unit training capability allows units to train and maintain their entire intelli-

gence teams at maximum proficiency and thereby improve intelligence and targeting support to commanders. IEWTPT provides this capability.

The need for this type of in-unit training system has existed at least since LTG(R) Menoher commanded the Army's Intelligence Center in the early 1990s and if anything, the need has grown since that time due to reduced budgets for institutional training time. We recognized and articulated the requirement for a viable, multidiscipline, in-unit training capability—which we defined as “IEWTPT”—in the 1990-1991 time frame; however, we could not get the needed funds. We even tried to build a prototype IEWTPT with the help of the U.S. Army Electronic Proving Ground (EPG) at Fort Huachuca, Arizona, in order to show the benefits that would accrue (*“build it and they will come”*—with funding). The author is happy to report that in December 2000, the Army funded the IEWTPT program and let a contract.

Now, early in 2004, the contract IEWTPT team is fielding the first iteration of the system



Operator (Systems Engineer Kevin Mullally) controlling the IEWTPT system during developmental testing.

Photographs courtesy of Roger McNicholas.

	FY02	FY03	FY04	FY05	FY06	FY07	FY08	FY09	TOTALS
QTRS	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	
<b>Phases:</b>	<b>System Dev &amp; Demo</b>				<b>Production</b>				
<b>Milestones:</b>									
Contact Awarded	▲	28 Nov 2000							
Systems Design Review	▲	11-13 Dec 2001							
TCC Development/Integration	▲						△		
Intel Software Design Review		▲ 22-23 Jan 2003							
Hardware Design Review		▲ 22-23 Jan 2003							
Incr 2 Software Design Review		▲ Mar 2003							
Integration Events (IE)		▲▲▲ IE-1 Mar 2003, IE-2 Jun 2003, IE-2 Jul 2003, IE-3 Aug 2003							
System Test		▲ Sep & Nov 2003							
DT&E Events		▲▲ Nov 2003 & Feb 2004							
Training Courses			Mar-Apr 2004						
Operational Event (OE) Testing		△ May 2004							
Milestone C (Oct 04)		★ Oct 2004							
MR/IOC FT Huachuca (Oct-Nov 04)		★ Oct-Nov 2004							
Production Contract Award		★ Jan 2005							
Field FT Hood, TX		△ Sep 2005							
Field FT Bragg, NC/FT Lewis, WA			△△ Aug & Oct 2005						
Field FT Irwin, CA/FT Polk, LA				△△ Aug & Oct 2007					
Field V Corps/CMTC					△△ Jun & Aug 2008				
FOC						★			
<b>Key:</b>									
CMTC – Combat Maneuver Training Center									
Demo – Demonstration									
Dev – Development									
DT&E – Developmental Test and Evaluation									
FOC – Full Operational Capability									
FY – Fiscal year									
IOC – Initial Operational Capability									
MR – Material Release									
QTRS – Quarters									

Figure 1. IEWTPT Schedule.

to Fort Huachuca and has begun the essential testing and evaluation phase of the IEWTPT. We anticipate this will lead to a positive Milestone C decision this year (see Figure 1), resulting in additional fielding to III Corps, XVIII Airborne Corps, V Corps, and the National Training Center for starters.

## What Is IEWTPT?

First and foremost, IEWTPT is “MI Gunnery.” Just as the Armor Force has its Tank Gunnery Tables to qualify tank crews, IEWTPT will enable

us to qualify Army intelligence system operators and analysts fully. However, IEWTPT is much more than just a qualification tool for individuals and teams. Successful intelligence depends on a seamless architecture from “mud-to-space.” No echelon, Service, Joint command, or task force has all the intelligence assets it needs to satisfy all of their intelligence and targeting requirements. This dictates that IEWTPT must also be a vehicle through which the Army can accomplish multi-echelon training to train multiple systems’ operators, teams of analysts, intelligence and

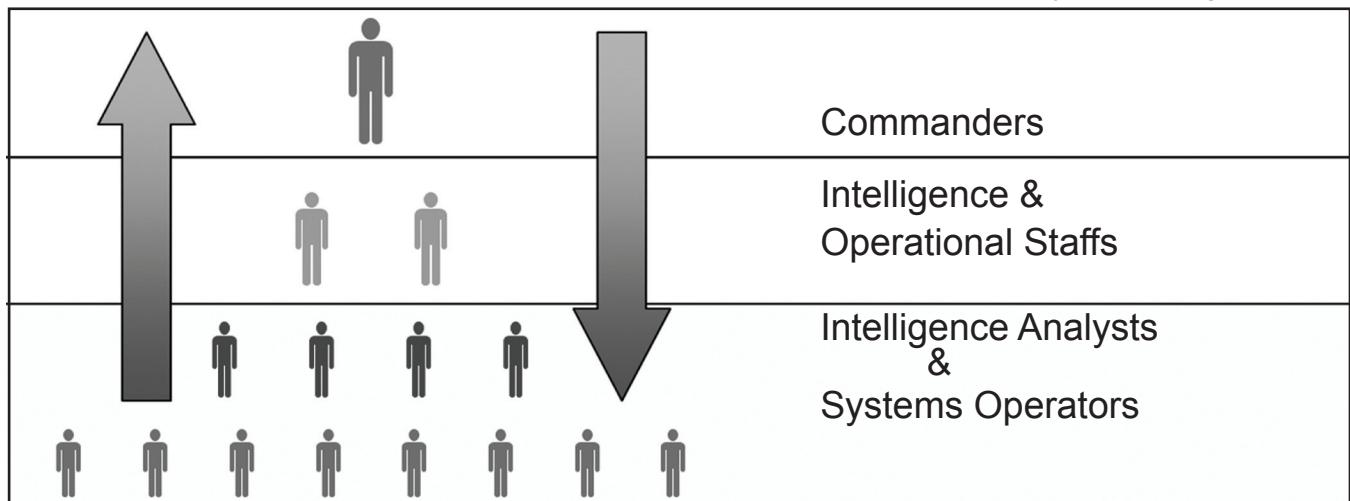


Figure 2. IEWTPT Trains the Entire Intelligence Chain of Command.

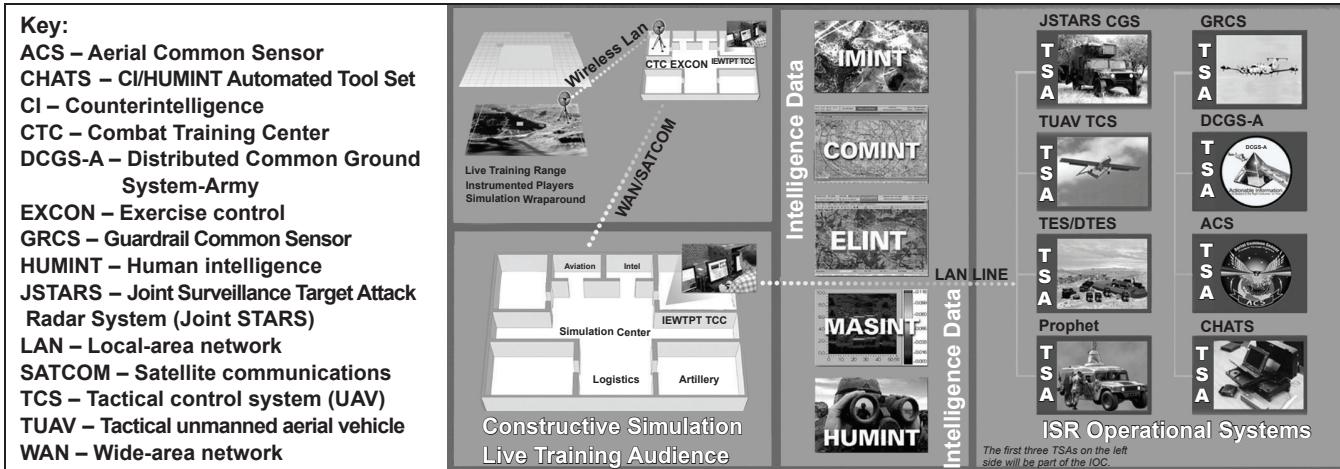


Figure 3. IEWTPT Data Flow Diagram.

manders on how to employ their IEW assets optimally and to understand their roles in doing so (see Figure 2).

Army Intelligence doctrine starts with the tenet that “*The commander drives intelligence.*” That is, at each echelon, the operational commander must focus the intelligence effort to provide the intelligence, situational awareness, and targets he or she needs for success. To the extent the commander does this, the better focused the intelligence effort will be and the greater the potential for satisfaction of his requirements. The flip side of this equation is that if a commander fails to focus the intelligence effort, there is far less potential that the intelligence system will provide him what he needs, when he needs it.

When one considers the premise behind the Army’s Future Force and Future Combat System of trading armor protection for better intelligence, the importance of focusing the intelligence effort becomes clear. As a consequence, IEWTPT provides a multi-echeloned training capability that can include commanders and their staffs.

Acknowledging the “Joint” imperative in how we fight

and will fight in the future, IEWTPT must and can expand to the Joint arena as a high-fidelity training vehicle for Joint intelligence and operations staffs and their commanders. The other Services and the new Joint National Training Capability (JNTC)<sup>1</sup> would be well served to embrace IEWTPT as a viable training tool for this purpose.

### How Does IEWTPT Work?

IEWTPT consists of a Technical Control Cell (TCC) and multiple target signature arrays (TSAs) interfaced at the front end to constructive



The IEWTPT Technical Control Cell.

simulation and live-instrumented training-range players and at the back end to actual MI systems. The constructive simulation is a computer model that simulates the roles of large numbers of participants on the battlefield. This allows for the creation of complex scenarios involving tens of thousands of soldiers, vehicles, aircraft, etc., and supplements the relatively small number of live participants who are on the training range.

The TCC enhances the constructive and live-data feeds with intelligence data (imagery, communications, electronic, measurement and signatures, and/or human intelligence [IMINT, COMINT, ELINT, MASINT, and/or HUMINT, respectively]) as shown in Figure 3. The TCC then forwards this enhanced data to TSAs that are embedded in or strapped onto the actual collection and processing systems used by the unit(s) involved. TSAs use the enhanced data to simulate the sensor inputs of their respective intelligence systems. Thus, for example, for a system that relies on radar as its data feed, the TCC would take the constructive and live data, enhance it with IMINT or ELINT as required, and forward it to the TSA which would then use this data to simulate a radar data feed into the operational asset. The result is that system operators see “the fight” portrayed on their actual operational systems.

The contractor team leader, under contract to the Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI), is building the TCC, and each Program Manager (PM) developing an Army intelligence collection or processing system has the task to develop the TSA for that system. Thus far, eight different Army PMs are developing TSAs, three of which will be part of the IEWTPT initial fielding (Initial Operational Capability [IOC]) to the Intelligence Center at Fort Huachuca this year. These PMs are for the:

- ❑ Joint Surveillance Target Attack Radar System (Joint STARS) Common Ground Station (CGS).
- ❑ Tactical Exploitation System (TES) and Division Tactical Exploitation System (DTES).
- ❑ Tactical Unmanned Aerial Vehicle (TUAV).

The Army will field other TSAs with subsequent versions of IEWTPT, including TSAs for the Distributed

Common Ground System-Army (DCGS-A) and the Aerial Common Sensor (ACS).

Today, constructive simulations like Corps Battle Simulation (CBS), Joint Conflict and Tactical Simulation (JCATS), or Tactical Simulation (TACSIM) drive the TCC, and over time, these will migrate to the objective systems Warfighters’ Simulation (WARSIM) 2000 and One Semi-Automated Forces (OneSAF) simulation as part of the Army Constructive Training Federation (ACTF). The TCC can also simultaneously tie to live instrumented training ranges such as in the “maneuver box” at the National Training Center (NTC).

The IEWTPT TCC enhances the live and constructive simulation data with intelligence data to stimulate the TSAs of each of the collection systems, processors, and ground stations used in the training event. System operators are responsible for recognizing information or activity of value as it appears on their actual systems, and reporting it accurately. They may also cross-cue other resources to assist in data collection, such as the CGS operator requesting imagery from a TUAV operator. Analysts then must use the operators’ reports to determine what is occurring and its significance and to present their findings in such a manner that their significance is immediately apparent. Intelligence and/or operational staffs and commanders then must come up with appropriate assessments, directives, and guidance.

One of the most important capabilities of IEWTPT is its ability to assist in the assessment of the users’ performance. While the TCC is receiving live and constructive data feeds and enhancing them for use TSAs, it is also capturing this “ground truth” data into record files. As the operators send reports up the chain for analysis, these reports also go from the TSAs back to the TCC where they are parsed and recorded. Additionally, the TSAs send footprint data back to the TCC, which allows for capture of what the operators are looking at versus the data presented to them. This information coupled with automated event detection of activity, such as vehicles entering and leaving areas of interest, allows for the creation of very high-fidelity after-action reviews (AARs) and performance measurement.

## Modes of Operation

IEWTPT also has great flexibility to adjust training for a wide variety of audiences, ranging from multiple units and their staffs and commanders to teams or individuals. It uses three modes of operation to accomplish this training:

- ❑ **Integrated Mode.** Driven by a constructive simulation and/or a live, instrumented fight, it trains operators, analysts, intelligence and operational staffs, and commanders, or any combination thereof, at one or multiple echelons and at one or multiple locations.
- ❑ **Playback Mode.** Using a recorded segment of a constructive simulation and/or instrumented live fight as ground truth, it stimulates the TSAs to provide focused training for any of the groupings above without the overhead required to run the constructive simulation or to reengage the live players.
- ❑ **Stand-alone Mode.** Operators and/or analysts work with recorded data from a specific TSA driving their operational system.

When tied to a live event, such as a rotation at the NTC, IEWTPT provides the capability to extend the maneuver box to furnish deep, flank, and rear battles or opposing force (OPFOR) elements operating in the seams between Units of Action (UAs), all tied to the instrumented fight in the maneuver box. One can also add multiple players, including the maneuver brigade's parent division and corps, or additional UAs and/or Units of Employment, as appropriate. This provides the potential for far more realistic and expanded, multi-echelon training opportunities that in turn provide far greater return on the Army's training-dollar investment.

## Conclusion

IEWTPT is a capability that is long overdue. Distance learning and embedded training help solve the problem we recognized more than ten years ago, but we will not truly fill the gap until we can field IEWTPT to both Active and Reserve Components of the Army, and provide soldiers with the most realistic training opportunities possible. It is an imperative that the best army in the world provides the most realistic training opportunities for its soldiers. For the Army Intelligence

soldier of all grades and ranks, and the staffs and commanders they support, IEWTPT is that vehicle.



## Endnote

1. A key issue at the heart of transforming joint military training, U.S. Joint Forces Command's Joint Warfighting Center continues to develop and implement the Joint National Training Capability (JNTC). As one of three capabilities identified in the Department of Defense (DOD) training transformation plan, this effort broadens and deeps the reach of joint force training. The other DOD initiatives to transform joint training are the Joint Knowledge Development and Distribution Capability (JKDDC) and the Joint Assessment and Enabling Capability (JAEC). [From [http://www.jwfc.jfcom.mil/about/fact\\_jntc.htm](http://www.jwfc.jfcom.mil/about/fact_jntc.htm)]

*Paul Menoher (Lieutenant General, U.S. Army, Retired) founded his own firm in Fall of 2001 after working more than four years with industry. Before joining industry, he served more than 35 years on active duty. His final position from 1995-1997 was as the Deputy Chief of Staff for Intelligence (DCSINT), DA. Prior to that he commanded the U.S. Army Intelligence and Security Command, USAIC&FH, the U.S. Army Intelligence Agency, and the 501st MI Brigade Korea. He also commanded two battalions and served in Vietnam and Cambodia. He holds a Bachelor of Arts and Science degree in International Relations. The Director of Central Intelligence presented him the National Intelligence Distinguished Service Medal. In addition, he was a 1998 inductee into the Military Intelligence Hall of Fame. Readers may contact LTG(R) Menoher via E-mail at PMenoherAssoc@aol.com.*

*Roger McNicholas is a Business Area Manager and Program Manager (contractor), supervising all programs and products of a simulation systems facility in Florida. This includes development of the IEWTPT, development of training for several packages on the U.S. Army's Future Combat System (FCS), as well as the Simulation Tool Suites ModIOS® and S2Focus™ and the Dismounted Soldier Simulator Virtual Reality product. Before joining his current firm two years ago, he worked 15 years in business development and management positions. He has a Bachelor of Science degree in Computer Engineering. Interested readers may contact Mr. McNicholas via E-mail at Roger.McNicholas@gdds.com and telephonically at (407) 823-7011.*

# The Postgraduate Intelligence Program for Reserves: A Ten-Year Milestone

by Colonel Mark A. Jensen, USAR

Since 1962, the Joint Military Intelligence College (JMIC) and its predecessors, the Defense Intelligence School and the Defense Intelligence College, have provided graduate-level education in strategic intelligence to thousands of students. Dozens of these students have ascended to the highest ranks in the Intelligence Community, to include positions as the Service Intelligence Chiefs or even the Director of the Defense Intelligence Agency, the JMIC's sponsoring organization. Students in the in-residence, full-time program usually complete the coursework for the Postgraduate Intelligence Program (PGIP) and receive a certificate within a year; those who write a thesis also earn an accredited Master of Science of Strategic Intelligence (MSSI) degree. Of course, the main difference between education at JMIC and any other university program on intelligence is the availability and use of classified material. Another big plus for JMIC students is that the tuition is free.

## A Ten-Year Milestone

One of the part-time programs within JMIC that is less well known than the full-time program is the Postgraduate Intelligence Program for Reserves (PGIP-R). This program just reached a significant milestone in 2003, its tenth anniversary. In June 2003, the PGIP-R faculty, students, and alumni celebrated by holding a banquet at Mount Vernon, George Washington's residence just outside Washington, D.C. The banquet "host," the country's first spymaster and commander in chief, "George Washington," greeted those attending.

The college also recognized this milestone by selecting for its annual one-day conference in 2003 the theme of "Transforming Reserve Component Intelligence." The keynote speaker, Dr. John Winkler, is the Deputy Assistant Secretary of Defense for Reserve Affairs. The morning panel focused on "Reserve Component(RC)Intelligence Transformation Needs and Opportunities." The luncheon speaker was Major General Michael Dunleavy, U.S. Army Reserve (USAR), the former commander of Camp X-Ray at

Guantanamo, Cuba. The afternoon panel discussed "RC Intelligence Support to Homeland Defense."

## The Reserve Program and Faculty

PGIP-R has the same academic requirements as the full-time program. Classroom instruction in the two-year program, however, occurs over twenty-three weekends and in two intensive two-week terms. The coursework, taught at the Defense Intelligence Analysis Center (DIAC) at Bolling Air Force Base,



Students in a study group talk with two faculty members (on the left).

Washington D.C., consists of seven core courses plus seven elective courses. Students typically take two courses during a four-month weekend term.

The workload for PGIP-R, an accredited Master's degree program, is no less than for any other accredited graduate program. Each class period typically requires 100 pages of reading and a writing assignment. The primary objective of graduate-level education is to improve the students' ability to think critically and clearly express their thoughts in writing and briefings. Sometimes as many as one quarter of the matriculating students drop out after the first term after they realize the demands of the program.

One of the strengths of PGIP-R is the quality of the faculty, all current or retired Reservists. Almost half have a Doctor of Philosophy (PhD) or Juris Doctor (JD) (law) degree and another third have an MSSI. Furthermore, most of them work in the Intelligence Community in their civilian jobs and can provide perspective on current intelligence issues. Several are

Photograph courtesy of SGM Ron Fitzpatrick.

at the flag-rank Senior Executive Service (SES) or Senior Intelligence Service (SIS) level or have served as Assistant Secretaries in federal departments.

Another feature of PGIP, both in the full-time and Reserve programs, is the distinguished speaker program. Typically, a senior official from the executive or legislative branches or a flag-rank officer addresses all the faculty and students each month in PGIP-R.

## The Students

In 1999, the PGIP-R faculty assumed the responsibility for teaching students attending the new PGIP monthly (PGIP-M) executive format. The PGIP-M students consist of active duty military as well as government civilians from more than 20 other federal organizations, both within and outside the Department of Defense. Examples include the Drug Enforcement Administration, the Central Intelligence Agency (CIA), the Department of State, and the Federal Bureau of Investigation. The intermingling of PGIP-M students with the PGIP-R students is another advantage of the part-time Post-Graduate Intelligence Program. The diversity of student backgrounds adds tremendously to the classroom discussions.

In addition to the benefit of mixing of PGIP-R with PGIP-M students, about 40 percent of the students bring an "outside the beltway" perspective. They travel long distances to come to the college, some from as far away as California, Bosnia-Herzegovina, or Germany. Depending on the Service and organization, they may pay for a student's time in class and/or travel expenses.

Most students attending PGIP-R/M are O-3s and O-4s of all Services and civilian equivalents. However, noncommissioned officers from E-5 to E-9, officers from O-1 to O-6, and warrant officers have attended, as have two flag-rank civilians. Students with intelligence backgrounds certainly have an advantage in the program, but an intelligence background is not mandatory for admittance.

Since 1993 for PGIP-R and 1999 for PGIP-M, about 450 students have enrolled in these two programs. Of those who enrolled, over 250 have received PGIP completion certificates and almost 100 have earned the MSSI degree. The number of students completing PGIP naturally does not include the students who have enrolled in the last two years. This number also does not include students who have mobilized for Operations ENDURING FREEDOM and IRAQI FREEDOM and had

to defer completion of their coursework. The MSSI completion rate is significantly higher than the completion rates for other part-time civilian graduate programs.

## Student Selection

The PGIP-R/M programs begin each year in October. Each Service and organization with allocated quotas has different criteria for selecting students to attend. Generally, the organizations select students early in the calendar year for attendance later that fall. JMIC requires that each student have an accredited Bachelor's degree and a Top Secret (TS) clearance with sensitive compartmented information (SCI) access. These requirements are absolute and JMIC cannot waive them.

Some details about JMIC are available on the Internet at <http://www.dia.mil/Jmic/index.html>. Dr. John Rowland, Colonel, U.S. Air Force Reserve (Retired), the full-time Associate Dean for Part-Time Programs, can provide other details about PGIP-R/M. His unclassified E-mail address is john.rowland@dia.mil and his telephone number is (202) 231-3684 (DSN 428).

## Outlook

Given the current world situation, the need for intelligence professionals will only increase. PGIP-R/M is an outstanding way to "grow" the country's intelligence expertise among Reservists, active-duty military, and government civilians. PGIP-R has succeeded during the past ten years because of the dedication of both the faculty and the students. The college is investing in secure video-teleconferencing equipment and enhancing its ability to bring continuing education to more students than ever before. The next ten years will undoubtedly bring more growth and stature to the PGIP-R/M programs as the country's demands for quality intelligence increase and as alumni demonstrate the benefits of these programs through excellence in the workplace.



*Colonel Mark Jensen, USAR, is the Reserve Director of PGIP-R/M. He has served in the military for 33 years in the U.S. Army National Guard, on active duty, and in the Army Reserve. As a civilian, he works in the CIA Office of the Assistant Director of Central Intelligence for Collection. Readers may contact the author via E-mail at mjensenj@comcast.net and telephonically at (703) 482-0547.*

# CSA's Focus Area 16: Actionable Intelligence

by Lieutenant Colonel Stephen K. Iwicki

In the January-March 2004 column in the *Military Intelligence Professional Bulletin*, we introduced the concept of "Actionable Intelligence" and gave a very broad description of the Army Focus Area process. Since then, we conducted a second review with the Army Chief of Staff (CSA) and began programming and executing our major concepts. We still face some challenges in gaining the necessary resources for this effort. As we execute the restructuring of our Army, it is important to remember that our nation is at war.

The threat we face today and for the extended future requires us to change our intelligence capabilities and business practices dramatically. We are no longer primarily focused on collecting against conventional threats. The new challenges with transnational terrorism, asymmetric warfare, and the increasingly real specter of weapons of mass destruction are the realities of today. Our adversaries are now empowered by the globalizing effects of technology, communications, media, international travel, worldwide computer networks, multinational corporations, commercial intelligence, and international financing. These new threats will engage us asymmetrically since challenging the United States conventionally is not a realistic option for any future adversary.

## Transforming Intelligence Collection and Processing

To defeat this type of threat, we must transform our intelligence collection capabilities, and more importantly, we must improve our processing capabilities to separate relevant information from background clutter. This is a much more difficult task when fighting an asymmetric threat. The challenge becomes determining the identification of people who intend to do us harm, the structure and capabilities of their organizations, and their intentions in time to defeat them. Focus Area (FA) 16 Actionable Intelligence is the catalyst for the majority of the intelligence transformation initiatives within the overarching Army Campaign Plan.

The Army must be dominant across the full spectrum of operations, using deployable, modular force packages in support of a joint task force, in-

Actionable Intelligence provides commanders and soldiers a high level of shared situational understanding, delivered with the speed, accuracy, and timeliness necessary to operate at their highest potential and conduct successful operations.

—Headquarters, Department of the Army G2

cluding the capability to work with coalition, interagency, law enforcement, and non-governmental organizations. Our soldiers are the building blocks for that capability. To achieve that goal, the focus of our Intelligence Transformation is the soldier. All of our initiatives provide improved battlespace capabilities that connect better-trained soldiers to the network and enable them with knowledge from the global intelligence enterprise.

## Enhanced Intelligence Capabilities At Every Level

First and foremost, intelligence transformation is about enhanced intelligence capabilities at every level, starting with the soldier. Given the current situation in Iraq and Afghanistan, our soldiers are immersed in a dynamic operating environment. They are working within the indigenous communities, talking with the inhabitants, seeing and observing more relevant information than all of our combined technical intelligence sensors are collecting. As a result, in order to collect, integrate, and use this information, the Army is implementing the concept of "*Every Soldier is a Sensor*" (ES2). This concept involves two critical aspects:

- Train all soldiers better to observe and report on their environments and intelligence requirements.
- Train leaders on how to maximize reporting and collection by their soldiers in all capacities at all levels.

The U.S. Army Training and Doctrine Command (TRADOC) is implementing this concept through-

out our military education system. ES2 will help in-grain the concept of fighting for knowledge.

## Task Force Modularity

Second, working closely with the concept of "Task Force Modularity," we have significantly improved battlespace capabilities by increasing intelligence collection and analytical capabilities within our new modular Maneuver Units of Action (MUA), and the Units of Employment (UE) echelons. These changes enable our Army to operate better in both the conventional and asymmetric environments. MUA analysis capabilities expand with the addition of an analysis platoon, an integration platoon, and additional analysts within the S2 sections. Additionally, human intelligence (HUMINT) collection teams are organic to the brigade and an S2X was added to the brigade S2 section to provide technical control and synchronize all counterintelligence and HUMINT in the brigade's area of responsibility. The MUA also has one tactical unmanned aerial vehicle (UAV) platoon (Shadow 200), organic signals intelligence teams (Prophet), and other Joint enablers.

Leading the synchronization of these and other initiatives is FA Actionable Intelligence. The main thrust of FA Actionable Intelligence is to provide greater intelligence capabilities today and to institutionalize the capability for Army Intelligence to continue improving within a rapid spiral-development approach.

## Critical Initiatives of FA 16

The six critical initiatives of FA Actionable Intelligence fundamentally change the way the Army thinks about and performs intelligence collection, analysis, production, and dissemination. Our focus is to transform both our analysts and software tools from Industrial Age processes aided by technology, to true Information Age processes that allow us to use advanced software tools to process, analyze, and visualize the vast amounts of information available today.

We need better data tools capable of processing millions of data elements and visually presenting this information to the analyst so that a human can see the relevant information contained in 200,000 messages rather than having to read and analyze each individual message. Some of these advanced

tools, such as STARLIGHT, are in use today and are radically changing the way we do business. The six critical Actionable Intelligence initiatives encompass:

- Tactical overwatch.
- Interim Distributed Common Ground System-Army (DCGS-A).
- Pantheon Project.
- Information Dominance Center (IDC).
- Project Foundry.
- Red-Teaming capability.

**Tactical Overwatch** will formalize a discrete, downward-focused mission task to support designated tactical forces during periods of low situational awareness and high vulnerability, particularly when on the move from fixed intelligence facilities with access to forward area and national collection, shared databases and advanced processing.

**Fielding an Interim Distributed Common Ground System-Army (DCGS-A).** DCGS-A is already a Future Force Program of Record (POR) design scheduled for fiscal year 2008. We have begun accelerating DCGS-A to the field in a spiral-development approach. The Army is fielding interim DCGS-A fixed site capabilities to the theater intelligence brigades and groups and we are expanding this effort down to the maneuver battalion level.

**Pantheon Project.** This project's team of 10-12 elite, world-class individuals from business, academia, and government will rapidly develop and field new capabilities that solve our hardest technical problems, creating technological or procedural solutions for the enhancement of tactical through national intelligence echelons. These solutions will then rapidly spiral forward into the intelligence community and tactical units.

**Information Dominance Center (IDC).** The IDC is a state-of-the-art operational intelligence organization that rapidly leverages national, theater, and tactical reporting to establish threat association and linkages; recognize threshold events, activities patterns, and anomalies; and aid understanding of the significance of information "buried" within large volumes of collected material.

*(Continued on page 55)*

# Doctrine Corner

## USAIC Fields Two New Intelligence Manuals

by Stephen C. Clarke

The U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) is in the final stages of producing a new field manual called **FM 2-22.3, Human**

**Intelligence Collector Operations**, and has recently fielded an approved special text, **ST 2-91.6, Small Unit Support to Intelligence**, dated March 2004. The new FM on human intelligence (HUMINT) is the first for the 97E military occupational specialty (MOS) since its change in designation from Interrogator to HUMINT Collector. Its tentatively scheduled for final approval this Fall.

### FM 2-22.3

FM 2-22.3 will supersede **FM 34-52, Intelligence Interrogation**, which was published in 1992. FM 2-22.3 is currently in Final Draft form and USAIC&FH has placed it on our Army Knowledge Online (AKO) Collaboration web site for review by all Army proponent agencies. You may contact ATZS-FDC-D@hua.army.mil for authorization to access the draft.

The Army is developing FM 2-22.3 in response to a recognized need for a document that contains updated tactics, techniques, and procedures (TTP).

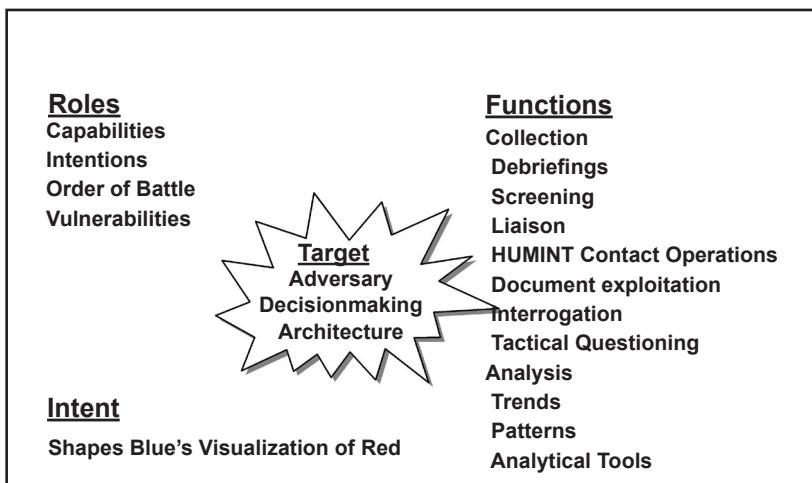


Figure 2. HUMINT Roles and Functions.

FM 2-22.3 also tackles the change from a relatively narrow focus on tactical interrogation to the broader spectrum of HUMINT collection activities. In addition, it addresses the employment of HUMINT collection teams within the framework of changing Army doctrine. (Figure 1 shows the tactical HUMINT organization.) The inclusion of the J2X/G2X element and streamlined command and reporting channels has brought the depiction of command and control (C2) functions up to date.

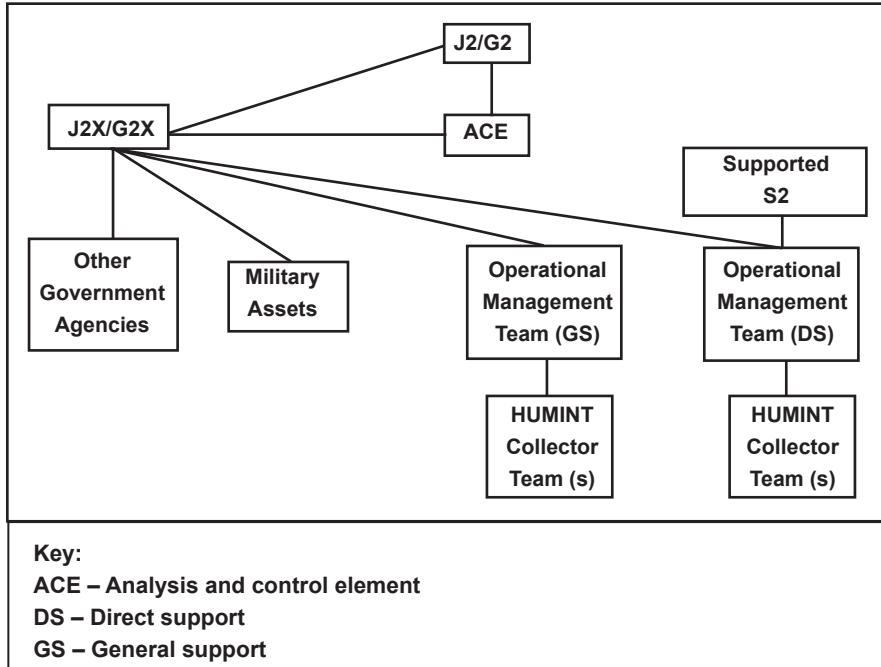


Figure 1. Tactical HUMINT Organization.

Why the changes? In 2003, USAIC&FH approved new operation and organization (O&O) plans for both HUMINT and counterintelligence (CI) operations, which effectively separate the two disciplines. Consequently, FM 2-22.3 describes the deployment of HUMINT collection teams (HCTs), whose military component consists of enlisted 97Es (HUMINT Collector) and 351E (Human Intelligence Collection

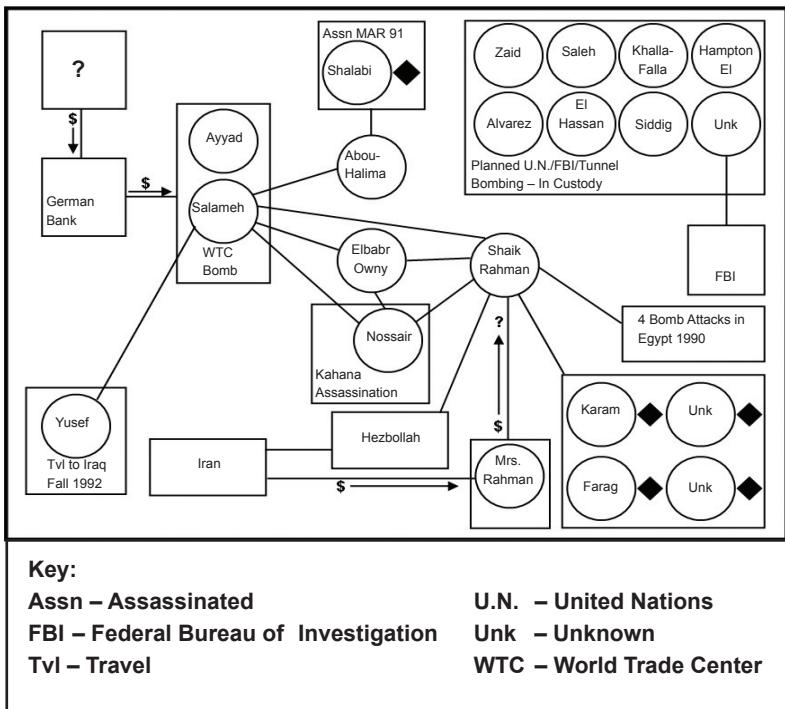


Figure 3. Example of a Link-Analysis Diagram.

Technician) warrant officers. Previously a mixture of CI and HUMINT personnel had deployed as a tactical HUMINT team (THT). This new employment strategy acknowledges the different missions that CI and HUMINT have and aims at employing HUMINT collectors more closely in accordance with their training and capabilities (see Figure 2).

There have been significant advances in technology since we fielded FM 34-52, and FM 2-22.3 brings the subject up to date. The new manual addresses the automation, biometric, and communication technologies that are vital to the success of HUMINT collection in the modern Army. The automation piece explains the hardware and software capabilities required to allow the HUMINT collector to access and interface with distributed databases and digital communications on the battlefield and elsewhere.

“Biometrics” is the study of measurable biological characteristics and the Army currently fields equipment that uses this technology. FM 2-22.3 describes the current capabilities of man-packed equipment to record identifying characteristics, such as fingerprints and unique iris patterns and store them in a database for retrieval by any authorized user of the system. There is also a discussion of biometric equipment to help HUMINT collectors determine the truthfulness of a source.

The new FM also presents automated analysis tools such as time and event charts, association matrices, and link-analysis diagrams that increase predictive analysis capability.

The introduction of FM 2-22.3 brings about other changes. The chapter on Approach Techniques has been expanded and introduces some additional report-building methodologies that support debriefing and elicitation rather than only addressing interrogation in the tactical setting. Other methodologies include expanded questioning techniques for debriefing, and a discussion of various types of HUMINT contacts.

Instruction on analysis for HUMINT collectors had previously been available only in the Warrant Officer Technical Certification Course, but it is now part of the 97E enlisted curriculum. As a result,

FM 2-22.3 devotes an entire chapter to HUMINT analysis. The manual contains detailed descriptions and examples of time and event charts, association matrices, and link-analysis diagrams (see Figure 3), and other analytical tools.

FM 2-22.3 has greatly expanded appendices to include extensive extracts from the **Law of Land Warfare (FM 27-10 dated 18 July 1956 as changed 15 July 1976)** and **Allied Joint Publication (AJP) 2.5, Handling of Captured Personnel, Equipment and Documents**, which contains the complete guide to the international system of allocating interrogation serial numbers. In the past, this document has been difficult to obtain; with increased emphasis on coalition operations, it is a sorely needed asset. FM 2-22.3 includes a guide for S2s as well as a questioning quick reference guide for the trained HUMINT collector, example forms, and a source and information reliability index. The final appendix in the FM contains instructions for document exploitation (DOCEX) and handling.

The HUMINT collectors’ participation in DOCEX has been deemphasized. In the past, HUMINT collectors were assumed to be the proper people to conduct DOCEX due to their language capabilities. Current doctrinal thought acknowledges

that a document exploiter does not need HUMINT training to translate a document, and that the unit can better employ the HUMINT collector in pursuit of the mission he or she was trained to do. FM 2-22.3 not only addresses HUMINT support to DOCEX, but also DOCEX support to HUMINT. This approach to the topic recognizes that DOCEX is an Army-wide responsibility and that HUMINT is one part of it and a consumer of DOCEX information, rather than the major provider.

FM 2-22.3 is the result of hard work and dedication by the Doctrine staff at USAIC&FH to capture the numerous changes in the training and employment of the HUMINT collector. However, the emerging doctrine for the Army Future Force has spread the responsibility to collect intelligence information to every soldier. "Every Soldier is a Sensor" has become the motto and indeed every soldier can provide information that contributes to the commander's situational understanding. To aid this effort, USAIC&FH produced a *Tactical Questioning Guide* that was very well received in the field.

## ST 2-91.6

In March 2004, Major General James A. Marks, Commander, USAIC&FH, approved a special text called **ST 2-91.6, Small Unit Support to Intelligence**, which is an expanded version of the *Tactical Questioning Guide* and supercedes it. ST 2-91.6 is not theater-specific and is designed to help all soldiers collect information through tactical questioning, enemy prisoner of war (EPW) handling, and document and equipment handling

in all operations. The ST stresses adherence to the *Geneva Convention* throughout the text.

Much of the information in ST 2-91.6 is geared toward patrols, personnel working traffic control points (TCPs) or roadblocks, and other situations where soldiers would come in contact with the local population. Once they collect information, they must, of course, report it in order for it to be of value. To close this loop, ST 2-91.6 provides guidelines to S2s for debriefing patrols and others, and it provides sample reporting formats. ST 2-91.6 also provides a TTP for operations with an interpreter and describes the different categories of interpreters and how to work effectively with them.

ST 2-91.6 is not designed to turn soldiers into intelligence collectors. However, it does introduce the basics of tactical questioning and provides some tools for patrols and S2s.

ST 2-91.6 is available on AKO in PDF format. USAIC&FH has also formatted the manual as a generic appendix which would be suitable for inclusion in any field manual that needs to provide a tactical questioning TTP. The appendix is available in Microsoft™ Word format and is available from the author at the E-mail address below.



*Stephen Clarke (Chief Warrant Officer Two, U.S. Army, Retired) is the Project Leader for HUMINT doctrine at the USAIC&FH Doctrine Division. Readers may contact him via E-mail at [stephen.clarke1@us.army.mil](mailto:stephen.clarke1@us.army.mil) and by telephone at (520) 538-1004 or DSN 879-0971.*

## Time for Subscription Renewal?

If you notice a "#" or "\*" in the address block on the back cover or the mailing label, then it is time to renew your subscription. The "#" means you have one more issue coming, the "\*" means that this is your last issue. You can renew either by calling us at (520) 538-1009 or DSN 879-1009 (with a credit card handy) or by sending us the completed subscription form on page 71. If you wish to keep this issue intact, you may make a photocopy of the form and mail or fax it to us.

## Read Any Good Books Lately?

We welcome reviews of books related to intelligence professional development or military history. Please mail or E-mail your book reviews with your phone number, address, the title, author, publisher, price, number of pages, and the publisher's address (listed on the book's copyright page). Please send your reviews to [mipb@hua.army.mil](mailto:mipb@hua.army.mil) or mail them to ATTN: ATZS-FDT-M USAIC & Fort Huachuca, 550 Cibeque St, Fort Huachuca, AZ 85613-7017.

# Letter to the Editor



Foreign language is **not** the most important skill in the Army. However, as long as we persist in fighting with people who speak something other than English, it can certainly come in handy.

Major General James A. Marks, in his "Always Out Front" column in the January-March 2004 issue of the **Military Intelligence Professional Bulletin**, mentions interpreters in passing. There is no mention of language training or of how to work with an interpreter. There is just the ground-level assumption by many that we will always have reliable, proficient, loyal interpreters available. There is the continued assumption that we will be able to perform, "*Careful and quick handling of [enemy prisoners of war] EPWs/detainees and documents ....*" Who will talk to the enemy prisoners of war and detainees? Who will read the documents? From where will the people with these foreign language skills come?

Foreign language capability is not in the same category as the assumed English language capability that is so useful in talking to members of our patrols. It is, however, a very basic enabler.

The solutions advocated by the Intelligence Center are excellent, well thought out and certainly necessary. They assume, however, by failing to mention or stress it, foreign language capability far beyond what is actually available.

Foreign language capability in the Army will not come easily, nor will it appear, magically. It must be continually "poked and prodded" by leaders and practiced by the soldiers.



## Ray Lane Aldrich

Chief Warrant Officer Three (U.S. Army, Retired)  
Warrenton, Virginia

## CSA's Focus Area 16

(Continued from page 51)

**Project Foundry** places a percentage of our tactical intelligence soldiers into ongoing live-environment intelligence operations that provide better technical and regional expertise. Project Foundry will include soldiers from almost every MI military occupational specialty (MOS).

**Red Teaming Capability** will integrate an ability to see ourselves as the enemy sees us in order to holistically assess proposed Blue force operations from an adversary perspective, identify weaknesses, and develop mitigating solutions.

## What Is Next?

The focus of Intelligence Transformation is providing optimized intelligence support to the one who needs the information the most—the soldier. We are effecting this change primarily through the improved changes in our new modular units and

the improved capabilities and processes the intelligence community brings to the fight as a vertical enabler.

In the next issue of **MIPB**, we will discuss how the six critical Actionable Intelligence initiatives are complementary enablers of our tactical forces and nested within our Nation's joint and expeditionary capabilities. The fall issue and this column will provide a detailed explanation of our new modular MI force structure.



*Lieutenant Colonel Steve Iwicki is currently assigned to the Army G2 and serving as the Deputy Director of Task Force Actionable Intelligence (TF-AI). Readers may contact him via E-mail at steve.iwicki@hqda.army.mil and telephonically at (703) 693-6210.*

# Proponent Notes

## Continuing Education and Professional Development

by Lieutenant Colonel Harvey Crockett

The focus of this article is to provide information on the opportunities available to MI professionals to continue their education and professional development during this time of rapid change and war. While the Enlisted and Warrant Education Systems await their turn for major change, the Officer Education System—the first to go through the Army Training and Leader Development review—is moving rapidly forward with change.

We have captured the changes below and we have also provided some additional information on methods to attain civilian degrees and other career enhancing training; then we discuss opportunities for the warrant officers and enlisted soldiers as well. Take a minute to review the information below to inform yourself better on what educational opportunities exist to ensure you always remain out front, relevant, and ready.

### Officer Actions

The point of contact (POC) for officer actions is Ms. Borghardt; readers may contact her via E-mail at [charlotte.borghardt@hua.army.mil](mailto:charlotte.borghardt@hua.army.mil).

### ***Officer Professional Development: Changes to the Officer Education System (OES)***

Within the next few years, we will see major changes in educational training strategies for both Lieutenants and Majors. The Captain-level training had some proposed changes; however, they are on hold. The current Captains Career Course training strategy remains unchanged.

**Basic Officer Leadership Course (BOLC).** This training concept will replace the current Officer Basic course, as we know it. This new approach will expose Lieutenants of all branches to the same common training as well as training together in a common location. BOLC training will be in three phases. Phase I will be the pre-commissioning phase taught at the Reserve Officer Training Corps (ROTC), the U.S. Military Academy (USMA), and Officer Candidate School (OCS). Phase II will be the field leadership training phase with empha-

sis on building confidence and leadership and developing rigor and toughness in junior officers. This phase is currently scheduled to be conducted at four locations (Fort Benning, Georgia; Fort Knox, Kentucky; Fort Bliss, Texas; and Fort Sill, Oklahoma). Phase III will be the actual Branch-specific training phase with officers going to their respective Branch schools; implementation of this training should begin in the fourth quarter of fiscal year 2006 (FY06).

**Majors' Intermediate-Level Education (ILE).** The concept driving the changes to ILE is the need to ensure that **all** Army Majors receive the same quality education. All officers will attend the 12-week common-core phase of this training. The Operations officers will attend the training at Fort Leavenworth, Kansas, while the other officers will attend the common core at a satellite campus. The training at the satellite campuses will be the same curriculum taught at Fort Leavenworth and taught by Fort Leavenworth instructors. Phase II of the ILE experience will be the Advanced Operations and Warfighting Course at Fort Leavenworth for the Operations officers. This phase will be 28 weeks. The Information Operations Career Field (IOCF), Operational Support Career Field (OSCF), and Institutional Support Career Field (ISCF) officers will attend their functional area training. Two pilot courses run in FY03 were at Fort Gordon, Georgia, and Fort Lee, Virginia. Both met with very favorable review. Full implementation should be in the fourth quarter of FY05.

**Career Field Designation (CFD).** The officer should not confuse the CFD process with the Functional Area Designation process, which occurs between the officer's fifth and sixth year of service. The CFD process takes place immediately after the Major selection board for that year group (YG) (in the 10th or 11th year). An officer's personal preference is a heavily weighted factor during this process. However, previous functional area experience and Advanced Civil Schooling also contribute to the CFD board decisions. All officers must select a career

field, even if they wish to remain in the Operations career field.

### **Upcoming Officer Selection Boards**

The Senior Service College selection board meets in April and the Major selection board will meet from mid-April to mid-May. The Career Field Designation Board for YG94 will meet in mid-June.

### **Warrant Officer Actions**

The POC for Warrant Officer actions is Chief Warrant Officer Five Castleton; readers can contact him via E-mail at lon.castleton@hua.army.mil.

### **Professional Development Opportunities**

Civilian education is an important part of a warrant officer's career progression and personal development. The Army goal is that all warrant officers have at least an Associate degree and obtain a Bachelor's degree by the time they reach Chief Warrant Officer Four. Many MI warrant officers have earned Master's degrees. Below are several methods available to allow you to earn your civilian degree.

**Degree-Completion Program (DCP).** This program is for soldiers who have enough credits from an accredited university to earn a degree in 12 months or less. The Human Resources Command (HRC) homepage has all of the information on this program or contact your HRC assignments manager for details. Warrant Officers incur an active duty service obligation for participating in this program.

**Permissive Temporary Duty (TDY) Study.** This program (20 weeks or less) is covered under **AR 621-1, Training of Military Personnel at Civilian Institutions**, 20 August 1999, Chapter 4-1.e, and **AR 600-8-10, Leaves and Passes**, 31 July 2003, Chapter 1 and Section XVI (para 5-31). The Commanding General (CG), HRC, will consider requests for permissive TDY for civilian training exceeding 31 or more days. The civilian schooling must be both sanctioned and approved by CG, HRC, and your commander must provide a recommendation. Participants will incur an active duty service obligation and the TDY must result in the award of a degree.

**Postgraduate Intelligence Program (PGIP) and Master of Science of Strategic Intelligence (MSSI) Degree Program.** Provided by the Joint Military Intelligence College (JMIC) at Bolling Air Force Base, in Washington, D.C., these programs afford you an

advanced degree. This Defense Intelligence Agency-(DIA) sponsored academic institution is now accepting applications for the PGIP and MSSI degree program. All Warrant Officer applicants accepted in the program are expected to finish the MSSI. The MSSI is a year-long program that runs from August through August of each year. The MSSI curriculum emphasizes developing the student's understanding of intelligence at the national level, military strategy, national security policy, and the planning and execution of joint and combined operations. The service obligation incurred is three times the length of schooling. Additional information about the JMIC is at <http://www.dia.mil/Jmic>.

Normally, in order to maximize employment of newly acquired analytical skills, Warrant Officers who graduate with the MSSI degree will have assignments to strategic- or theater-level jobs. Applications must arrive not later than 31 October at the Warrant Officer Division, which will in turn notify officers in writing of their selection or nonselection for the program by 30 January of the following year. (See also the article by COL Jensen in this issue of **MIPB**.)

**White House Fellowship Program.** A great but little known career-enhancing program is the White House Fellowship Program. In this program, selected officers receive an opportunity to serve for one to two years on the one of the White House staffs. Regular Army Warrant Officers with no more than 24 years of active warrant officer service and other than Regular Army warrant officers with no more than 16 years of active federal service may be eligible to apply. Check with your assignments officer at HRC to get complete details about this program.

### **Upcoming WO Boards**

The next WO Promotion Board for CW3/4/5 is scheduled for the period 4-26 May 2004.

### **Enlisted Professional Development Opportunities**

The POC for enlisted actions is Sergeant Major Mitchell; readers may contact him via E-mail at maurice.mitchell@hua.army.mil.

The current operations make it difficult to work on professional development; however, opportunities still exist. Although it is incumbent on the soldier to

*(Continued on page 59)*

# TSM Notes

## *Update on the Joint STARS Common Ground Station (CGS) User's Conference by Colonel Stephen J. Bond*

On 23 and 24 March 2004, the U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM) Office hosted the Joint Surveillance Target Attack Radar System (Joint STARS) Common Ground Station User's (CGS) Conference at Fort Huachuca, Arizona. The conference was an outstanding exchange of recent combat experiences and uses of Joint STARS and the CGS. Attending were 144 soldiers, Marines, airmen, Department of Army civilians, and defense contractors representing more than 40 organizations—many had recently returned from Operations IRAQI FREEDOM (OIF) in Iraq and ENDURING FREEDOM (OEF) in Afghanistan.

The focus of the conference was to share operational tactics, techniques, and procedures (TTPs), discuss system logistics and sustainment concepts, and describe training opportunities for CGS crews. The conference also provided an overview of future initiatives including improvements to the Joint STARS aircraft and CGS systems, and the future vector of the Military Intelligence Corps.

The conference's main feature was presentations by users explaining how they employed CGS to support Army elements (brigades, divisions, corps, and the Land Component Commander), Special Operations Forces, and the Marines, and to cross-level techniques for all units. Among the highlights were CGS Team Leaders from the 103d Military Intelligence (MI) Battalion, 3d Infantry Division (3ID), describing the key role they played on the combat march through Iraq. They stated that during the Division's 350-mile movement from Kuwait to Baghdad, CGS crews consistently provided commanders with timely information that was instrumental to the overall success of the Division's offensive operations.

There were also presentations by the 513th MI Brigade on its support to the Coalition Forces Land Component Command (CFLCC) and the 1st Marine Division. A U.S. Marine Corps (USMC) representative gave the conference attendees insights into the

Marines' use of the CGS during ground combat and stabilization operations. A Team Leader from the 101st Airborne Division (Air Assault) shared the experiences gained from CGS operations during both OIF and OEF. The Conference included additional presentations by the 104th MI Battalion, 4ID; the 102d MI Battalion, 2ID, in Korea; a III Corps Artillery team that was attached to a Special Operations unit; and the 319th MI Battalion, 525th MI Brigade, at Fort Bragg, North Carolina.

The after-action comment provided by Staff Sergeant Adrian Flores from the 513th MI Brigade perhaps best reflected the significant impact that CGS crews made in Iraq—

*"No other collection asset provided the wide-area all-weather coverage of the battlespace that the [Joint] STARS did with the [moving target indicator] MTI radar. The CGS allowed us to interact in real time with the collection platform and to focus on our critical requirements and process the collection data into usable and actionable intelligence products. The soldiers who operated the system proved equally as critical in processing, interpreting, and translating operational requirements to the collection platform. Because they were close to the point of decision, these CGS operators shared the sense of urgency and "can-do" attitude. They worked aggressively to find ways to answer questions instead of deflect them. When other platforms failed or were unavailable, the CGS-JSTARS combination ensured that we were not blind on the battlefield."*

The Army Group Deputy Commander at the Joint STARS Wing, Robbins Air Force Base (AFB), Georgia, provided insight into ongoing operations, lessons learned, and improvements to the Joint STARS aircraft. The Joint Program Office at Hanscom AFB, Massachusetts, provided a dynamic briefing on current and future Joint and U.S. Air Force moving target indicator (MTI) and synthetic aperture radar (SAR) initiatives. The Product

Manager for CGS spoke about the life-cycle logistics support transition plan to Tobyhanna Army Depot, U.S. Army Communications-Electronics Command (CECOM), and a Product Support Integrator. He later described the Service-Based Architecture software initiative and provided a system interoperability demonstration. Finally, the TSM Office gave an overview on the Distributed Common Ground System-Army (DCGS-A) and an update on MTI and SAR programs throughout the Department of Defense.

Another important portion of the Conference was the excellent sharing and cross-leveling of ideas and recommendations during work group sessions focused on seven specific topic areas. The concerns captured in these meetings will enable us to address and resolve issues to improve CGS use and support.

Overall, congratulations on a great job by all presenters, and a special "job well done" for the CGS crews deployed to OIF and OEF—they truly made a difference through effective employment of their

systems. A conference compact disk (CD) with all the presentations was provided to conference attendees and is available to those units that were unable to participate. If units would like a copy for official use, please contact Lieutenant Colonel John Della-Giustina, Deputy TSM for Current Systems and Operations, or Mr. Bryan Wukits, Assistant TSM for CGS and DCGS-A via E-mail at [wukitsb@hua.army.mil](mailto:wukitsb@hua.army.mil) or by calling (520) 533-7862/6201 or DSN 821-7862/6201.



*Colonel Steve Bond is the U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM) for Distributed Common Ground System-Army, Joint STARS, and Common Ground Station. Colonel Bond departs the TSM in July and Colonel James Harper will be his replacement. Readers can contact Colonel Harper at [james.harper@us.army.mil](mailto:james.harper@us.army.mil) and telephonically at (520) 533-3605/2480 or DSN 821-3605/2480. The Deputy TSM is Chris Friend. Readers can reach him at [friendc@hua.army.mil](mailto:friendc@hua.army.mil) and telephonically at (520) 533-8937 or DSN 821-8937.*

---

## Proponent Notes

(Continued from page 57)

maximize his or her time and seek out these opportunities, commanders and other leaders should continue to remind soldiers of opportunities, and, consistent with unit mission requirements, allow time for soldiers to continue to develop. The time invested in the soldier's development will continue to yield a better-qualified soldier and noncommissioned officer (NCO).

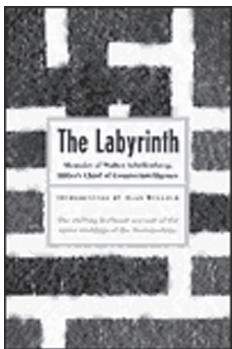
**NCO Education System (NCOES).** Changes have occurred in the NCOES to improve requirements for promotions and attendance. The changes affect entrance requirements in the area of the Army physical fitness test (APFT) for those NCOs returning from one of the ongoing operations. Leaders and NCOs should speak to the unit Schools NCO, check the Noncommissioned Officer Academy (NCOA) website (<http://usaic.hua.army.mil/NCOAcademy/index.htm>), or call (520) 533-4234 or DSN 821-4234 for updated information.

**Joint Military Intelligence College.** Excellent opportunities exist for the enlisted soldier to improve his or her college education as well as knowledge of the U.S. intelligence programs. In addition to the programs listed under Warrant Officer Professional Development—which apply to enlisted soldiers as well—the Undergraduate Intelligence Program (UGIP) and the Bachelor of Science in Intelligence (BSI) offer opportunities based on the soldier's current level of civilian education. Visit the JMIC webpage at <http://www.dia.mil/Jmic/academics.html> and speak to the career manager at HRC for application procedures.



*Lieutenant Colonel Harvey L. Crockett is the Director, Office of the Chief, Military Intelligence (MI). Readers may contact him via E-mail at [harvey.crockett@hua.army.mil](mailto:harvey.crockett@hua.army.mil). Robert C. White, Jr., is the Deputy OCMI; you can reach him via E-mail at [bob.whitejr@us.army.mil](mailto:bob.whitejr@us.army.mil).*

# Professional Reader



(New York: Da Capo Press, 2000) Paperback  
456 pages, \$18.00, ISBN  
0306809273

## *The Labyrinth: Memories of Walter Schellenberg, Hitler's Chief of Counterintelligence by Walter Schellenberg*

Walter Schellenberg, the Counterintelligence Chief for Adolf Hitler during World War II, wrote his memoirs titled "The Labyrinth" recounting the counterintelligence (CI) operations of Germany during the height of the war. [He received one of the lightest sentences of any WWII war criminal, six years in prison. The mitigating factor in this light sentence was his attempts to help concentration camp prisoners in the latter part of the war.]

In his memoirs, Mr. Schellenberg recounts some of the most interesting aspects of the German CI paradigm and the constant battles he waged with his superiors. While many of his tasks were odd by any standard, he also was in charge of one of the most advanced CI and counterespionage (CE) agencies of the time. In fact, in many ways, Schellenberg managed to blend many disparate intelligence disciplines and entities into a workable format. He recounts in his memoirs many of the failures of the Third Reich to recognize the importance of CI and CE and to integrate CI and CE into the operational planning process. One can deductively link the failures of the internal policies in regards to CI to the inability of Germany to effect real stability operations in the Eastern Theater, and consequently win the war.

Mr. Schellenberg believed that the resistance to a "Secret Service" in Germany was at the very least plausibly related to the lack of a Secret Service tradition in Germany like England had.<sup>1</sup> He thought that there was no understanding of effectively implementing intelligence into the planning and operational processes. Furthermore, he lamented the fact that the intelligence services of Germany were—

"Overlapping bureaus and agencies, which resulted in duplication, waste, inefficacy, and

the inevitable personal and professional jealousies. Finally, there was a drastic shortage of specially trained personnel."<sup>2</sup>

Mr. Schellenberg noticed these problems when first installed as the department head and he spent most of his career attempting to fix the system that no one wanted fixed. He makes the point that it appeared that Reinhard Heydrich, Chief of the Internal Security Branch (SD) and Schellenberg's immediate supervisor, constantly attempted to play "divide and conquer" among the different departments in order to maintain political control of them.<sup>3</sup> Thus, according to Schellenberg, the mission got lost in the politics of bureaucracy.

Mr. Schellenberg sought to obtain liaison offices with various departments with which he had to do business. He had not always had the ability to go to other ministerial heads without prior permission and the ability to liaise with other departments improved efficacy.<sup>4</sup> What the reviewer finds most interesting is that the conventional wisdom about Nazi Germany is that the government was a Leviathan and had coordinated information among the various intelligence and investigative divisions. According to Schellenberg, however, this was not the case. It was not due to the phenomena of being averse to investigations and intelligence work per se, it was in fact extreme parochialism. This parochialism would haunt Schellenberg's CI capabilities throughout the war.

He goes on to complain about the lack of security among the upper echelon social circles. "*The amount of highly secret and vitally important information that was so bandied about in these circles was really incredible...*"<sup>5</sup> He specifically blames the scientists, engineers, and senior officers. According to Mr. Schellenberg, these people were the most "loose lipped" among all

of German society. He points to the harm that all the gossip and careless talk among them did to the German war effort. Again, it would seem conventional wisdom about Germany would lead one to believe that each person would be paranoid about being accused of being loose lipped. However, it seems that security among the upper ranks of the Reich was not of interest and, according to the author, did great damage to the war effort.

Perhaps the greatest fault Mr. Schellenberg lays on the German Government was the lack of meaningful support to CI:

*"I told him...It was not enough for the personnel officers to say that they had assigned to me so many hundred men. Numbers in themselves meant little in the face of training masses of foreign nationals, linguists, and specialists, and the deficiencies in technical equipment were just as serious."*<sup>6</sup>

It seems Mr. Schellenberg faced an age-old intelligence problem, the disconnect between the "Real Army" and the "Real Intelligence World." Schellenberg spends much time throughout his memoirs speaking of the inability of the Regular Army staff officers to understand the operations of a CI organization. Throughout the history of Nazi counterintelligence, the German Regular Army staff officers tried to apply Regular Army principals to CI and political intelligence.

*"...how difficult it was for the military leaders who were responsible for planning to make a correct assessment of the information submitted to them. Consequently, if the material did not fit their basic concepts, they simply ignored it."*<sup>7</sup>

This, according to Mr. Schellenberg, led to both the misapplication of CI personnel and assets, and the degradation of the CI mission.

It is apparent that Nazi Germany hampered the CI mission not because of an inability to conduct the mission but due to a the lack of understanding and extreme parochialism on the part of the German command authority. It is interesting that many of Schellenberg's complaints are at the very least analogous to those of U.S. CI professionals about

the U.S. Army command's support to U.S. Army counterintelligence.

*"...[the] Army management's apparent inability to answer simple questions about counter-intelligence force structure, on-the-job training, and counterintelligence investigations is troubling."*<sup>8</sup>

This is in no way intended to draw a moral equivalence between Nazi Germany and the United States; however, it does illustrate a historic point for intelligence in general. When Mr. Schellenberg compares German and British intelligence, he points out the differences between the very capable British intelligence service and the stymied German intelligence services.<sup>9</sup> His conclusion is that the failures of German intelligence are not due to a lack of ability but rather to a lack of historical integration of intelligence into the command structure. If U.S. Army CI does have similar problems to Schellenberg's CI service, it seems *prima facie* that the issue is not the capabilities of U.S. Army CI but a lack of understanding and integration at the Army command level.

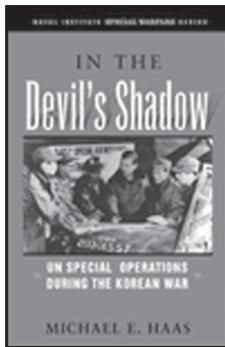
#### **Endnotes**

1. Schellenberg, Walter, **The Labyrinth: Memories of Walter Schellenberg, Hitler's Chief of Counterintelligence** (New York: Da Capo, 2000), page 209.
2. Ibid., page 209.
3. Ibid., page 13.
4. Ibid., pages 211, 361-362.
5. Ibid., page 183.
6. Ibid., page 262.
7. Ibid., page 191
8. Department of Defense. *Report of the Advisory Board on the Investigative Capability of the Department of Defense* (Washington, D.C.: GPO, 1994), page 76.
9. The British intelligence services are some of the oldest and are widely renowned as the best in the world. To wit, the British Government assisted the United States in forming both the Central Intelligence Agency and U.S. Special Forces.



---

**Sergeant James L. Mader**  
Fort Riley, Kansas



(Annapolis, MD: Naval Institute Press, March 2000), 243 pages, \$29.95, ISBN: 1557503443

## In the Devil's Shadow, UN Special Operations During the Korean War, by Michael E. Haas (Colonel, U.S. Army and U.S. Air Force, Retired)

**C**olonel Michael Hass retired from the U.S. Air Force (USAF) after he began his career as a private in the Army Infantry serving in airborne, ranger, Special Forces, and psychological operations units. He was an assault helicopter pilot in Vietnam; during the Vietnam War, he completed 968 combat flying hours and earned the Distinguished Flying Cross. He has also commanded the Pararescue Squadron and completed Pentagon tours with both the USAF staff and the Joint Chiefs of Staff.

The author will influence you in rededicating yourself to your job and being appreciative of the people who brought the U.S. Special Operations Command into existence. The book contains references to Eighth U.S. Army (EUSA) staff members that will hold your attention, and it discusses the fallacies of putting operational elements under staff officers with little or no modified table of organization and equipment (MTOE) or logistics support. The reader will immediately grasp that they have accomplished major improvements and made great strides in operational doctrine.

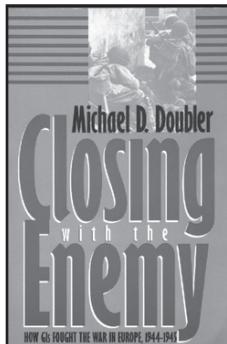
The book commences with the story of easily the best Counterintelligence Corps agent on active duty at the beginning of the Korean War: Donald Nicholas, who began the war as an Air Force master sergeant and ended it as a senior member of USAF positive intelligence operations in Korea with the rank of Major. Although he only had formal education through the 6th grade, Mr. Nicholas was a friend of Republic of Korea President Syngman Rhee and had sources in both North and South Korea. This facilitated his providing some of the best intelligence for his superiors. He was one of the few who, rather than rotating home after a one-year tour, remained in country for the entire Korean War. Before the commencement of hostilities, he had "repeatedly

warned Far East Command (General [Douglas] MacArthur's headquarters) in Tokyo of the impending North Korean attack." However, he sent his warnings in vain, for as the Fifth Air Force Commander later observed, "*Nicholas's reports were suppressed and disregarded.*" His last report actually predicted the "*surprise attack that subsequently stunned a totally unprepared Truman administration*" seventy-two hours in advance of its occurrence. Not so surprisingly, it was Mr. Nicholas's terse report from Seoul on the morning of 25 June 1950 that gave MacArthur's headquarters its first official notification of the North Korean invasion.

The author discusses both the intelligence and the partisan insertion operations and problems. He points out that both operations used the same techniques; however, the doctrinal lines were not clear on operational coordination, actual location of partisan operations, and the relationships between the G2 and G3. He also brings to light the organizational bickering between the new Central Intelligence Agency (CIA), the Army, and General MacArthur's headquarters. It was during this time that the Air Force and the Navy ran operations for their own purposes with little deconfliction of operations with any of the other operational elements. The Air Force ran intelligence and partisan networks that included running a small boat force that raced into North Korean waters to retrieve downed pilots. The CIA and others employed the same assets to work partisan and intelligence agent insertions. The Navy use of underwater demolition teams in partisan support was the first form of special operations missions for Navy swimmers.

This book should be required reading for all serving on the EUSA staff, especially the members of the G2 and G3 sections. The historical examples of problems that occurred during the Korean War would be of great motivational val-

ue for personnel working in the current staff sections. Most importantly, the book shows what a few strong-willed patriots can do to make the situation work at the lower levels regardless of the bureaucratic problems of higher command.



(Lawrence, Kansas: University Press of Kansas, 1994), 354 pages, \$21, ISBN 0-7006-0744-7

**A**re innovation and adaptation best driven top down or bottom up? Just two-and-a-half years after the attack on Pearl Harbor, the U.S. Army landed at Normandy. Over the next eleven months, the relentless offensive combat operations conducted against the German Army carried the U.S. Army into Central Germany and ultimate victory. Given the scale and ferocity of the operations and considering that Germany still had a first-rate army, the European Theater of Operations (ETO) during 1944-1945 proved the U.S. Army's sternest test.

How the U.S. Army fared in the ETO against its German opponent is a source of continuing debate among soldiers and historians. Michael Doubler's excellent book, **Closing With the Enemy: How the GIs Fought the War in Europe, 1944-1945**, is a significant and positive addition to this debate.

This well-written book relies extensively on original sources in its discussion of how the U.S. Army adapted in the ETO. Mr. Doubler argues that the U.S. Army that landed at Normandy was a well-prepared force with sound doctrine, thorough training, and adequate equipment. Its great strength, however, was the institutional willingness to constructively modify tactics and policies to fit the circumstances. The diverse operational environments of the ETO forced the Army to master the challenges posed by its different campaigns: the struggle in the hedgerows, the pursuit across France, battling into urban centers, cracking the West Wall fortifications, slugging through the forests, and conducting opposed river crossings. Except for the defensive phase of the Ardennes battle, the U.S. Army generally remained on the offensive.

---

**James R. Lint**  
Seoul, Korea

---

## *Closing With the Enemy: How the GIs Fought the War in Europe, 1944-1945* by Michael Doubler

The author argues against interpretations that the U.S. Army achieved victory only through application of sheer brute strength while employing little tactical flair. The Army, restricted to a 90-division force dispersed between Europe and the Pacific, did not enjoy a substantial manpower advantage over the Germans.

The author contends that, unlike its totalitarian German counterparts, where innovation was from top down to the troops via the General Staff solution, the U.S. Army drove innovation from the bottom up. Mr. Doubler believes that U.S. soldiers, imbued with the notions of free speech from their democratic society, showed initiative to adapt and devise solutions to problems, not waiting for superiors to provide them. Given the continual tempo of operations, there was little time to devise and disseminate General Staff solutions to units engaged in combat operations.

The book recounts again and again the many instances when soldiers and local commanders devised tactical solutions to seemingly intractable problems. Given the varied campaigns the U.S. Army fought in its drive across Europe, the initiative to devise local solutions was critical for sustaining the Army's offensives and creating an effective combined-arms team. Mr. Doubler's contribution runs counter to the somewhat damning interpretation of muddled U.S. Army performance in the ETO as put forth by Russell Weigley's **Eisenhower's Lieutenants** and Martin van Creveld's **Fighting Power**. While the U.S. Army in the ETO was certainly not a perfect instrument, the U.S. soldiers' ability to adapt, as the author points out, was its key to success.

---

**Sergeant First Class Peter Clemens, USAR**  
Stafford, Virginia

# MI Corps Hall of Fame



## 2004 Military Intelligence Corps Hall of Fame Inductees

The 17th annual Military Intelligence Corps Hall of Fame (HOF) ceremony will be held on 25 June 2004. During the ceremony, the Corps will induct six new members: Command Sergeant Major (Retired) John C. Butler, Command Sergeant Major (Retired) Robert T. Hall, Lieutenant General (Retired) Claudia J. Kennedy, Lieutenant General (Retired) Robert W. Noonan, Jr., Major (Retired) Kenneth L. Robinson, and Command Sergeant Major (Retired) Debra E. Smith.

### **Command Sergeant Major John C. Butler (U.S. Army, Retired)**

Command Sergeant Major John Butler began his military career as an Infantry soldier in 1969. After basic training and advanced individual training (AIT), his first assignment was with Company D, 1/8th Cavalry, 1st Infantry Division (Airmobile) in South Vietnam. Before coming to Military Intelligence (MI), he spent his first fifteen years serving in Infantry Branch assignments. During this time he served in numerous leadership positions, to include assignments with 1/8th Infantry in South Vietnam, 3/8th Cavalry in West Germany, 1/31st Infantry in South Korea, the United Nations Command Support Group—Joint Security Area (UNCSCG-JSA) in South Korea, and as a Drill Sergeant at Fort Jackson, South Carolina. In 1984, CSM Butler was selected to serve as a Senior Intelligence Sergeant with the 3d Brigade, 7th Infantry Division (Light). In preparation for the Brigade's certification during Exercise Celtic Cross

IV, he was singularly responsible for writing the intelligence portion of the 3d Brigade operations plan (OPLAN). During the actual exercise, he supervised the Intelligence Section and ensured the prompt, accurate flow of intelligence information throughout the command.

By 1986, CSM Butler had decided to make a career change to Military Intelligence. He completed the Intelligence Analyst Course and subsequently moved to S2 duties. His common-sense approach to his new intelligence duties earned immediate recognition; during a Gallant Knight command post exercise, the Commander, XVIII Airborne Corps, singled him out for his outstanding contribution.

CSM Butler's next assignment was as First Sergeant of B Company, 10th MI Battalion, 7th Infantry Division (Light). In this role, he provided exceptional leadership, mentoring, and training for all the soldiers of his unit. After his service as First Sergeant, he moved on to become the G2 Sergeant Major, 5th Infantry Division, Fort Polk, Louisiana, in 1990. During Operation DESERT SHIELD, he created an in-depth training program for all G2 soldiers in anticipation of a deployment to Southwest Asia, raising unit readiness to its highest level while continuing to provide quality intelligence support to 5th Infantry Division (Mechanized) (5ID [M]).

In 1992, he became Command Sergeant Major of the 302d MI Battalion, 205th MI Brigade, in Germany. During his time as the Battalion CSM, his battalion was cited as the best intelligence organization of its type during a V Corps Battle Command Training Program (BCTP) exercise. He was personally responsible for the successful relocation of the battalion from Frankfurt to split locations at Wiesbaden and Heidelberg. The battalion continued to provide full intelligence support during this move.

In 1996, CSM Butler moved on to become the CSM for the 15th MI Battalion (Aerial Exploitation

Battalion [AEB]), 504th MI Brigade, at Fort Hood, Texas. His final assignment was as the Brigade CSM for the 504th MI Brigade. Here again, his continued support of training and leadership development through mentoring resulted in an exceptional command climate within the Brigade.

CSM Butler's dedication to duty and outstanding contributions over a long and illustrious career have had a lasting and significant impact on all the soldiers and commands where he served. His was a positive influence on the lives, careers, and families of all those with whom he served. A true mentor and soldier's soldier, CSM Butler retired in 1999.

### **Command Sergeant Major Robert T. Hall (U.S. Army, Retired)**

Command Sergeant Major Robert Hall entered the Army in 1970. After basic training and AIT, he served as a Manual Morse Intercept Operator with the 7th Radio Research Field Station in Thailand. Upon his return to the United States in 1972, he was assigned to Vint Hill Farms Station, Virginia; when Vint Hill closed in 1974, he was transferred to San Antonio, Texas. A year later, he attended the Cryptologist Course for Supervisors at Fort Meade, Maryland. That course led to his assignment at Fort Devens, Massachusetts, as a Morse Code Instructor. It was during his assignment at Fort Devens that his strength as a trainer, mentor, and leader began to evolve. Recruited for the 402d Army Security Agency (ASA) Detachment Special Operations (Airborne), 10th Special Forces Group (SFG) Airborne in May 1976, he performed duties as a Special Operations Team Intelligence Collector/Radio Operator and as a Team Sergeant.

In 1981, CSM Hall was assigned to the 328th ASA Company, 502d ASA Battalion, in Augsburg, West Germany, where he served as Service Platoon Sergeant, Operations Platoon Sergeant, Field First Sergeant, Training Noncommissioned Officer (NCO), and NCO In Charge (NCOIC) of the Processing, Control, and Analysis Section. He returned to Fort Bragg in 1984



where he was assigned as Operations Sergeant of the 519th MI Battalion, 525th MI Brigade (Airborne). CSM Hall was then reassigned to the G2, 1st Special Operations Command (SOC) as the Signal Intelligence/Electronic Warfare NCOIC. In September 1985, he assumed duties as the First Sergeant, A Company, 8th Psychological Operations (PSYOP) Battalion, 4th PSYOP Group.

CSM Hall graduated from the Sergeants Major Academy in 1989 and again returned to Fort Bragg to be the Command Sergeant Major of the 9th PSYOP Battalion. In May 1990, he returned to Germany to be the Command Sergeant Major of the 511th MI Battalion (Tactical Exploitation), 207th MI Brigade, in Ludwigsburg, Germany. During his time with this unit, he deployed to participate in Operations DESERT SHIELD and DESERT STORM. Upon returning to Germany, he took part in the deactivation of the 511th MI Battalion.

Returning to the states once again, CSM Hall became the Command Sergeant Major of the U.S. Army Intelligence School, Fort Devens, Massachusetts, and the 112th MI Brigade from September 1992 until its deactivation in 1993. Upon deactivation of the 112th, he moved on to become the Command Sergeant Major of the U.S. Army Intelligence Center and Fort Huachuca. From January 1995 until June 1996, he served as the Command Sergeant Major of the U.S. Army Sergeants Major Academy, at Fort Bliss, Texas.

CSM Hall's final assignment was as the CSM of the Third U.S. Army and U.S. Army Forces Central Command (ARCENT), Fort McPherson, Georgia, from June 1996 to his retirement on 21 January 2000.

### **Lieutenant General Claudia J. Kennedy (U.S. Army, Retired)**

Lieutenant General Claudia Kennedy is the first and only woman to achieve the rank of three-star general in the United States Army, taking her from the Women's Army Corps in the late 1960s to the position of Department of the Army (DA) Deputy Chief of Staff for Intelligence from 1997 through 2000 in which she oversaw policies and operations affecting 45,000 people stationed worldwide.

Following in her father's footsteps, Lieutenant General Kennedy joined the Army in 1968 and received a direct commission in June 1969. She began her career as the Administrative Officer, G1, for the Army Garrison at Fort Devens, Massachusetts. Her next assignment was as a Recruiting Officer for the Women's



Army Corps in New Hampshire. She then commanded the Staff and Faculty Company of the U.S. Women's Army Corps Center and School at Fort McClellan in 1973.

Her next assignment was as the Electronic Warfare Staff Officer for the U.S. ASA Field Station Korea.

In July 1977, she returned to the United States and worked with the U.S. Army Intelligence and Security Command (INSCOM) at the National Security Agency as a Cryptologist Staff Officer. Next stationed at the Army Field Station Augsburg in Germany, she was the Assistant Operations Officer. Returning to state-side once again in 1984, she was assigned as a Staff Officer for the DA Directorate of Training, Deputy Chief of Staff for Operations and Plans in Washington, D.C.

In 1986, LTG Kennedy assumed command of the 3d Operations Battalion, U.S. Army Field Station Augsburg. She later commanded the San Antonio Recruiting Battalion until July 1990. After attending the U.S. Army War College, she commanded the 703d MI Brigade, in Kunia, Hawaii. In all of these assignments, LTG Kennedy made immediate and significant improvements in the units' competence, cohesion, and overall readiness by maintaining emphasis on honing critical intelligence skills. Attention to detail in planning and execution were the hallmark of her leadership throughout her career.

In 1993, as Brigadier General Kennedy, she served as the Director of Intelligence G2 at U.S. Forces Command. Next she served as the Deputy Commander, U.S. Army Intelligence Center and School at Fort Huachuca, Arizona. She was responsible for human intelligence (HUMINT), counterintelligence (CI), and signals intelligence (SIGINT) doctrine, development of intelligence architectures, and oversight of all intelligence acquisitions. From 1995 until 1997, then Major General Kennedy served as the Assistant Deputy Chief of Staff for Intelligence, DA, Washington, D.C. In this role, she recognized the ever-growing importance of tactical CI and HUMINT in

providing critical intelligence support to the warfighter and reorganized the Human Intelligence Division into a full-fledged Army Staff directorate.

From 1997 until her retirement in June 2000, LTG Kennedy served as the Deputy Chief of Staff for Intelligence (DCSINT), DA, in Washington, D.C. As the DCSINT, she ensured that Army Intelligence both supported the warfighter and met the Army's responsibilities in executing the National Military Strategy. She worked hard to ensure the full integration and synchronization of all of the Army's intelligence requirements, resource processes, and priorities with the priorities of the war fighting Combatant Commanders. Her further contributions included the development of winning strategies to articulate Army priorities to key officials with the Office of the Secretary of Defense (OSD), the Intelligence Community, and on Capitol Hill. She retired in June 2000.

Since completing her Army career, Claudia Kennedy has chaired First Star, a nonprofit corporation and published her book, **Generally Speaking**, in September 2001. She is a trustee of Rhodes College and associated with commercial and nonprofit organizations as well as with the International Spy Museum. She has appeared as a military consultant for NBC and CNN and as a guest on several television programs. Claudia Kennedy has been widely recognized for her leadership and lifetime achievements.

### **Lieutenant General Robert W. Noonan, Jr. (U.S. Army, Retired)**

Lieutenant General Robert Noonan's career spans 35 years and includes a progressively challenging list of assignments available to a commissioned officer in Military Intelligence. Commissioned through the Reserve Officers Training Program in 1968 at the University of Notre Dame, his initial assignment was as an Intelligence and Operations Advisor, IV Corps, in South Vietnam. He then served as a Basic Training Company Commander at Fort Campbell, Kentucky, before assignment as the Brigade S2, 1st Brigade,



3ID, in Schweinfurt, West Germany. LTG Noonan attended the Military Officer Advanced Course, and then served as Company Commander at Fort Devens, Massachusetts, with subsequent assignments as a Plans Officer and Manpower Management Analyst. His next assignment took him to 25ID, at Schofield Barracks, Hawaii, as Division Artillery S2, Company Commander, and Deputy Division G2.

His next duty was assignment as a Tactical Intelligence Officer with the Rapid Deployment Joint Task Force and U.S. Central Command (CENTCOM) before selection as Battalion Commander, 125th MI Battalion, and G2, 25ID, at Schofield Barracks. LTG Noonan then became Deputy Chief and Division Chief, Intelligence and Electronic Warfare/Command and Control Countermeasures, DA Deputy Chief of Staff for Operations. He followed this assignment by serving as Executive Officer to the Army's Deputy Chief of Staff (DCS, G2).

He then assumed command of the 513th MI Brigade, Fort Monmouth, New Jersey. Under his command, more than 1400 soldiers in four battalions transformed into a deployable, trained, and ready force. He provided forward, multidiscipline intelligence support to major Joint exercises and to Joint and Combined operations in Kuwait, Saudi Arabia, and to the United Nations and Joint operations in Somalia. During his command, the four battalions received national recognition as Department of Defense (DOD) Intelligence Collector of the Year and best Army Tactical Signals Intelligence Unit of the Year. Also during this time, LTG Noonan successfully planned, coordinated, and executed the movement of the 513th Brigade Headquarters and three battalions from separate sites on the east coast to Fort Gordon, Georgia.

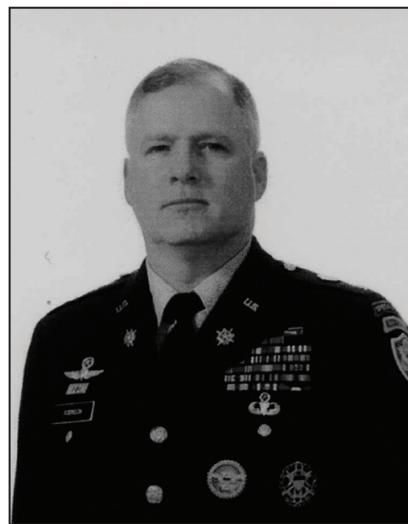
Subsequently selected as Deputy Chief of Staff, Operations, U.S. Army Intelligence and Security Command, he oversaw the refocusing of the command to a force projection Army, the demands of the Unified Commands, and the downsizing and restructuring of INSCOM to meet the Army's and national intelligence future requirements. He sharpened INSCOM's focus on tactical and operational support to warfighters around the world. He was instrumental in the successful deployment of the Predator Unmanned Aerial Vehicle (UAV) to Albania in support of Balkans contingency operations. His vision to translate concepts rapidly into operational capabilities was the singular reason for INSCOM's success in providing fused intelligence support and resources to Joint and Combined operations.

His next assignment was as Director for Intelligence, J2, U.S. Central Command. He ensured Central Command received the best multidisciplined, fused intelligence products and predictive analysis during the execution of Operations SOUTHERN WATCH, DESERT STRIKE, DESERT THUNDER, and maritime intercept operations. His keen insights and in-depth analysis of Iraqi activities earned him an impeccable reputation and the trust of Congress, the State Department, and the Joint Chiefs of Staff. His next assignment was command of the U.S. Army Intelligence and Security Command. His leadership led to the refinement and enhancement of national and tactical SIGINT partnerships that significantly increased operational readiness and provided seamless SIGINT support to operations in Bosnia-Herzegovina and Kosovo.

LTG Noonan's final assignment was as Deputy Chief of Staff, Intelligence (DCS, G2), DA, Washington, D.C. From this post, he was the forerunner for transforming Army intelligence to support future warfighters. His visionary concepts of providing ground forces with accurate, fused, predictable intelligence from space to mud were fully integrated into intelligence policies, programs, and budgets. Following the events of 11 September 2001, was the vanguard in providing analysis; vision; leadership; and support to DOD, national agencies, Combatant Commanders, and Army leaders during the fight against global terrorism and the Iraqi crisis. He contributed immeasurably to the National Security Strategy by his precise and often diplomatic dealings with more than 27 embassies in Washington, D.C. His efforts with military attachés and ambassadors greatly strengthened Secretary of State policy positions. He retired in 2003.

### **Major Kenneth L. Robinson (U.S. Army, Retired)**

Major Kenneth Robinson enlisted in the Army in 1975 and immediately received a nomination to the West Point Preparatory School. He declined his acceptance to the West Point and proceeded to 1st Battalion (Ranger), 75th Infantry. He



continued through his enlistment in several Ranger, Special Forces, and mechanized units.

MAJ Robinson completed his initial enlistment and enrolled in the Army Reserve Officers Training Corps (ROTC) program at Marion Military Institute. He graduated from the Marion Military Institute, earning the prestigious George C. Marshal Leadership Award. Commissioned a Second Lieutenant, he completed his undergraduate education at Auburn University. He applied for active duty and was assigned to the Military Intelligence Branch. While at Fort Huachuca for the Military Intelligence Officer Basic Course, Major Robinson designed, instructed, and led the School's first viable pre-Ranger Training program. This program significantly improved the selection rate of MI officers to attend the U.S. Army Ranger School.

Major Robinson moved on to the XVIII Airborne Corps in December 1985 where he served as the Operations and Plans Officer, Operations Battalion, 525th MI Brigade. Subsequently, in 1986, he oversaw the establishment of the Long-Range Surveillance Company (LRSC) within the 519th MI Battalion. In that same year, Major Robinson was the XVIII Airborne Corps representative at the Worldwide LRSC Conference where he successfully defended the retention of a long-range surveillance capability within the Army MI brigade force structure.

MAJ Robinson assumed command of A Company, 519th MI Battalion, in June 1987. During this command he designed new methods of screening, video surveillance monitoring, and mission critical reporting. An instructional tape, capturing these innovations, was integrated into the doctrinal program of instruction for interrogation at the Intelligence Center and School.

After command, while still a Captain, he was selected to serve as the Operations and Intelligence Officer for a special intelligence mission in support of Joint Task Force 118 in the Middle East. The Task Force's mission was to support operations against forces laying mines and attacking Kuwaiti oil tankers. Major Robinson not only planned missions, he actively participated in combat operations, flying with aircrews and deploying with special boat units on their combat patrols. Upon his return from the Middle East in October 1988, the newly promoted Major Robinson was selected to serve as the Battalion S3 of the 519th MI Battalion.

Then in 1990, Major Robinson was chosen to attend the Defense Intelligence Agency (DIA) Postgraduate Intelligence Program (PGIP), but upon arrival in Washington, D.C., he was diverted to be the Intelligence Requirements Officer to the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. Subsequently, when Iraq invaded Kuwait, Major Robinson was singled out to be the Operations and Intelligence Officer of a special liaison element assembled in support of the Commander in Chief, CENTCOM's command, control, communications, and intelligence efforts.

After the Gulf War, he returned to his duties at the Office of the Secretary of Defense (OSD) where he worked intelligence policy issues closely with the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI) regarding nonofficial cover activities. Upon completion of this assignment, MAJ Robinson returned to and graduated from PGIP. In June 1993, following his graduation, he was again requested to work on the Joint Staff as the Intelligence Policy Officer in the J3 Special Operations Division, Operations Support Branch. In June 1994, he became the Detachment Commander of a DOD special mission unit. This assignment sent him to many countries to include Bosnia, Columbia, and Haiti on sensitive intelligence missions.

After graduating from the U.S. Marine Corps Command and Staff College in 1997, Major Robinson was again assigned to the Office of the Deputy Secretary of Defense where he dealt with a number of intelligence-related issues. His daily duties included interaction with the Directors of both the Central Intelligence Agency (CIA) and DIA on Gulf War issues. He testified and performed liaison with the President's Special Oversight Board for Investigations of the Gulf War. The Secretary of Defense recognized MAJ Robinson for his efforts and awarded him the Defense Superior Service Medal.

Selected for promotion to Lieutenant Colonel in 1998, Major Robinson was soon after diagnosed with an acute medical problem for which he medically retired in 1999. In 2001, MAJ Robinson, now a civilian, accepted a position with the Cable News Network (CNN) as a Senior Terrorism and National Security Analyst.

## **Command Sergeant Major Debra E. Smith (U.S. Army, Retired)**

Command Sergeant Major Debra Smith entered the Army in 1973. She attended basic training at Fort McClellan, Alabama, and Morse Code Operator training at Fort Devens, Massachusetts. Her first assignment was at Field Station Korea in 1975. After her tour in Korea, she returned stateside and was assigned to the 902d Military Intelligence Group, Fort Meade, Maryland. While there, she served as a Morse Operator and attended the Cryptologic Course for Service Supervisors.

In 1978, CSM Smith was assigned to Field Station Augsburg, where she served as a Signals Search and Development Operator and Section Supervisor. Her next assignment returned her to the Intelligence School at Fort Devens, where she served as an Instructor and Platoon Sergeant. She was reassigned to Field Station Berlin in 1983 as a Platoon Sergeant and subsequently as the NCOIC of the NCO Development Course. During her assignment in Berlin, CSM Smith was chosen for the Sergeant Morales Club. She transferred to the 714th MI Battalion in Augsburg, West Germany, in 1985 where she again served as Platoon Sergeant as well as NCOIC, Manual Morse Division.

CSM Smith departed Augsburg in 1986 to attend the Cryptologic Course for Senior Supervisors enroute to an assignment at Fort Huachuca, Arizona, as an Advanced NCO Course (ANCOC) Instructor. In 1987, she moved to Field Station



Panama to the 747th MI Battalion as a First Sergeant. In 1989, she departed Panama and attended the U.S. Army Sergeants Major Academy at Fort Bliss, Texas. Her next assignment was with INSCOM as the Career Management Field 98 (SIGINT) Training Manager.

On 18 July 1991, she was appointed to the rank of Command Sergeant Major, becoming the first female in the Military Intelligence Corps to attain that rank. She initially served as the CSM of the 731st MI Battalion and then with the 733d MI Battalion in Kunia, Hawaii. As the CSM of both of these units, she established a highly regarded Noncommissioned Officer Development Program (NCODP), which served as the model throughout INSCOM. Chosen to be the CSM of the 733d MI Battalion during its activation, her efforts resulted in putting the newest INSCOM battalion on a sound operational footing in record time.

Her next assignment sent her to the 344th MI Battalion at Goodfellow Air Force Base, Texas. Her personal leadership during an unprecedented kidnapping and murder of a soldier within the unit served to focus efforts and provide much needed stability to the unit. She later used this experience to train and teach others on how to deal effectively with "Trauma and Serious Incidents in Units."

In February 1996, she again returned to Fort Huachuca to become the Command Sergeant Major of the 111th MI Brigade. During a period of serious personnel turbulence resulting from downsizing and realigning the forces across the Army, she continued to instill pride in the unit and to build intelligence soldiers second to none.

Her final assignment began in May 1997 as the Command Sergeant Major for the Defense Language Institute Foreign Language Center (DLIFLC) and Presidio of Monterey, California. She continued to emphasize soldierization skills for linguists and was instrumental in bringing drill sergeants to DLIFLC to assist in this vital process. She retired in August 2000.

### **MI Corps Hall of Fame Nominations**

The Office of the Chief of Military Intelligence (OCMI) accepts nominations throughout the year for the MI Hall of Fame (HOF). Commissioned officers, warrant officers, enlisted soldiers, and civilians who have served in a U.S. Army intelligence unit or in an intelligence position with the U.S. Army are eligible for nomination. A nominee must have made a significant contribution to MI that reflects favorably on the MI Corps.

The OCMI provides information on nomination procedures. If you wish to nominate someone, contact OCMI, Futures Directorate, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-MI (HOF), 110 Rhea Avenue, Fort Huachuca, AZ 85613-7080, call commercial (520) 533-1180, DSN 821-1180, or via E-mail at OCMI@hua.army.mil.

# Sly Fox Notes

## ASAS Master Analyst (AIS 1F) Allocations

by Matthew J. Nunn

The original goal of the All-Source Analysis System (ASAS) Master Analyst Program (AMAP) circa 1997, was to place 156 ASAS Master Analysts (additional skill identifier [ASI] 1F) in the field. These allocations basically broke down to three at each division, corps, and echelon above corps (EAC) analysis and control element (ACE), with additional allotments for the U.S. Army Training and Doctrine Command (TRADOC) and various other non-ACE en-

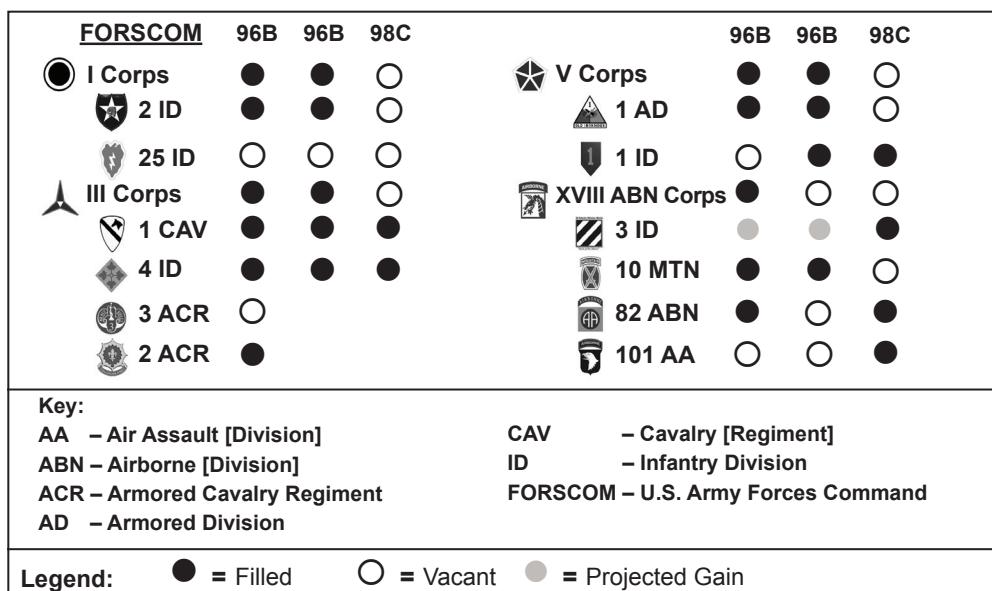


Figure 1. FORSCOM ASAS Master Analyst Distribution.

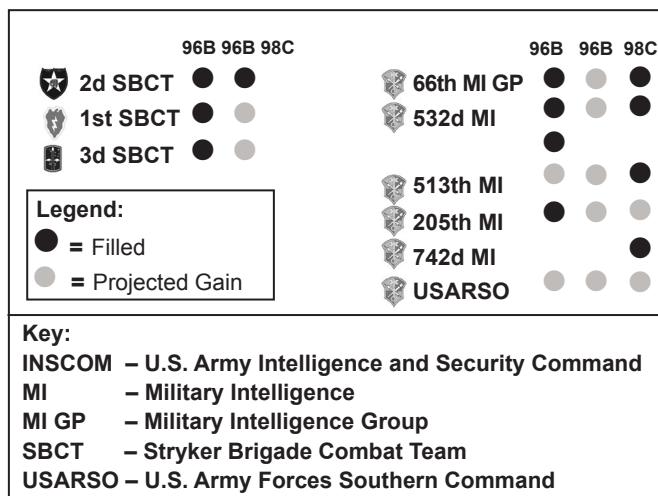


Figure 2. SBCT and INSCOM ASAS Master Analyst Program Distribution.

ties. These numbers also included an approximately 50-percent overage to provide for attrition, rotation in and out of the program for other professional development opportunities, etc.

Figures 1 through 3 illustrate the current distribution of Army ASAS Master Analysts in U.S. Army Forces Command, the Stryker Brigade Combat Teams (SBCT) and U.S. Army Intelligence and Se-

curity Command, and in training units, respectively. The MOS columns in each figure reflect the actual 1F slots at the unit. Most units have authorizations for two 96B (Intelligence Analyst) 1F and one 98C (Signals Intelligence [SIGINT] Analyst) 1F. Columns without any markers indicate that the unit only has one or two specific slots. For example, in Figure 1,

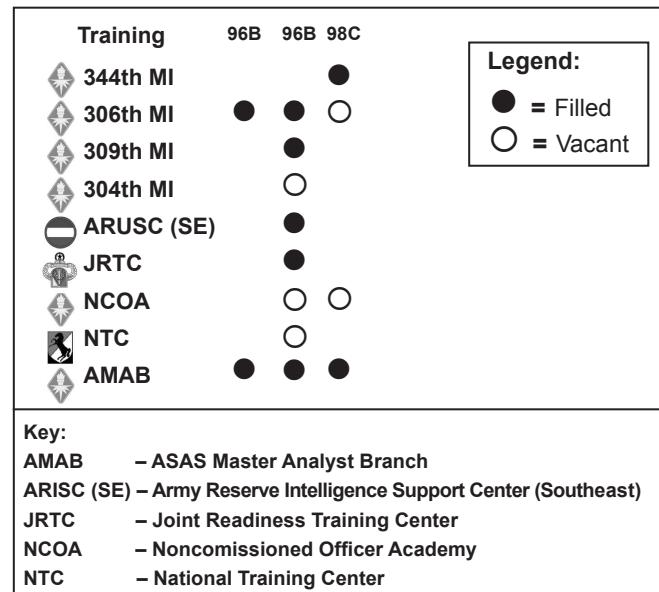


Figure 3. ASAS Master Analyst Program Distribution for Training.

<b>ASAS Master Analyst Course</b>	
AMAC 05-001	12 OCT – 17 DEC 04
AMAC 05-002	07 MAR – 06 JUN 05
<b>ASAS Certification Course</b>	
ACC 05-001	31 JAN – 18 FEB 05
ACC 05-002	16 JUN – 01 AUG 05
ACC 05-003	12 SEP – 30 SEP 05

**Figure 4. AMAC/ACC Schedule for Fiscal Year 2005.**

the 4th Infantry Division has authorization for two 96B 1Fs and one 98C 1F, while the 2d Armored Cavalry Regiment has only one authorized 96B 1F.

Under force modernization, the Master Analyst requirement will potentially increase to 307. This amounts to one at each maneuver Unit of Action (MUA), two at each Military Intelligence company

(approximate total of 144), 42 at other units, and 20 for TRADOC and various other entities plus the 50-percent overage for attrition.

To meet this increased requirement for additional Master Analysts in the field, units need to make the most of the training opportunity offered by the ASAS Master Analyst Course (AMAC). See Figure 4 for upcoming AMAC schedules and ASAS certification courses.



*Matt Nunn is the Course Manager for the ASAS Master Analyst Course (AMAC) and ASAS Certification Course (ACC) for the ASAS Master Analyst Branch. His career has included 13 years as a SIGINT Analyst at multiple echelons and 7 years instructing the AMAC and ACC. He also has 10 years of experience using and teaching various ASAS systems. Readers may contact Mr. Nunn via E-mail at matthew.nunn@us.army.mil and telephonically at (520) 533-1924 or DSN 821-1924. You may also contact the AMAB through their website at URL 150.180.145.79.*



Order Processing  
Code \*6489

# MIPB Subscription

Subscription Order Form





Please send me \_\_\_\_\_ subscription(s) for \_\_\_\_\_ years (no more than 2) for **Military Intelligence Professional Bulletin (MIPB)**. \$21.00 (Domestic, APO, and FPO); \$29.40 (Foreign) per year. You can E-mail us at [sharon.nieto@hua.army.mil](mailto:sharon.nieto@hua.army.mil).

The total cost of my order is \$ \_\_\_\_\_. All prices include regular domestic postage and handling and are subject to change. I understand this charge is not refundable.

**Address**

---

(Company or Personal Name)

---

(Street Address)

---

(Additional Address/Attention Line)

---

(City, State, ZIP Code)

---

(E-mail Address and Telephone Number)  
Please include your E-mail address to confirm Receipt of payment.

**Please choose method of payment:**

Check payable to the **Superintendent of Documents**

GPO Deposit Account No:   

MasterCard  VISA  Discover

Expiration Date \_\_\_\_\_

Authorization Signature.....

**Mail to:**  
ATTN: ATZS-FDT-M, U.S. Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017



# Contact Information and Submissions



***This is your magazine. We need your support in writing and submitting articles for publication.***

## **When writing an article, select a topic relevant to the Military Intelligence community.**

Articles about current operations and exercises; Tactics, Techniques, and Procedures (TTPs); equipment; and training are always welcome as are lessons learned, historical perspectives, problems and solutions, and short "quick tips" on better employment of equipment and personnel. Our goals are to spark discussion and add to the professional knowledge of the MI Corps. 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 a new piece of technology will change the way we operate.

## **When writing for *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 more than a year to publish some articles.
- Please note that submissions become property of ***MIPB*** and may be released to other government agencies or nonprofit organizations for re-publication upon request.
- Be aware that ***MIPB*** is posted on the MI Life-Long Learning Center (MIL3C) (two issues behind the current one) and is available for sale by the Government Printing Office.

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

- A cover letter with your work and home E-mail addresses, work telephone number, and a comment stating your desire to have your article published. We accept electronic or hard copy cover letters.
- Your article in Microsoft 2000 or Word 7.0. Do not use special document templates.
- A Public Affairs release if your installation or agency requires it. Please include that release with your submission.
- A release signed by your local security officer or SSO stating that your article and any accompanying graphics and pictures are unclassified, nonsensitive, and releasable in the public domain. Once we receive

your article, we will send you a sample form to be completed by your security personnel.

- Any pictures, graphics, crests, or logos which are relevant to your topic and enliven the article. We need complete captions (the who, what, where, when, why and how), the photographer's credits, and the author's name on the photos. Please do not embed graphics or images within the text, attach them as separate files. Images should be sent to us in tif or jpg formats. Please note where they should appear in the text.
- 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, E-mail address and phone numbers, with the biography.

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

Submit articles and graphics to [MIPB@hua.army.mil](mailto:MIPB@hua.army.mil). or mail (on disk or CD) to:

ATTN ATZS-FDT-M (Smith)  
U.S. Army Intelligence Center and Fort Huachuca  
550 Cibeque Street  
Bldg 61730, Room 105  
Fort Huachuca AZ 85613-7017

If you have any questions, please E-mail us at [MIPB@hua.army.mil](mailto:MIPB@hua.army.mil) or call us at (520) 538-0956/DSN 879-0956. Our fax number is (520) 538-1007.



## **Military Intelligence Professional Bulletin**

Upcoming Themes and Deadlines for Article Submission

Issue	Theme	Deadline
Jul-Sep 04	Joint and Expeditionary Capabilities Within the Intelligence Community	5 Aug 04
Oct-Dec 04	MI and Modularity	5 Sept 04