



MI PB

Military Intelligence Professional Bulletin

October-December

2003

PB 34-03-4



Intelligence
Lessons and
Observations



From the Editor

"Whom shall he teach knowledge? and whom shall he make to understand doctrine? ... for precept must be upon precept, ... line upon line... here a little, and there a little."

-*Isaiah 28:9-10 (KJV)*

Even in ancient times, a solid foundation of doctrine has been a non-negotiable prerequisite for success. Army Intelligence doctrine changes as appropriate and as required. The primary impetus towards positive change begins with the observations and lessons learned that impact real-world implementation of tactics, techniques, and procedures.

Doctrine was never intended to be so abstract that an advanced degree in physics is required to comprehend it; instead, doctrine is supposed to build, with theory and reality supporting one another. The theoretical underpinning provides the basic material that is adapted to the particular venue; the real-world applications, in turn, sometimes change our methodologies.

Technology and advanced capabilities significantly influence the type and nature of data needed and desired by decision makers. Innovative and adaptive field expedient methods can become doctrinal solutions.

For all these reasons, doctrine is always evolving and adapting.

For all these reasons, we need to hear from you, in the field, how you conduct business—what are your successes? Failures? And what can or should be done to fix these matters?

In this issue, Doctrine Corner specifically lays out the questions and base-line queries for which we are actively seeking answers. Elsewhere, we lay out some of the specific observations thus far collected, and outline how these observations may impact current Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF).

We invite you to consider the questions in light of your own experiences, and to submit your responses to the Lessons Learned team. We would also like to share your knowledge with the rest of our readership—so write us an article, or even a Letter to the Editor. This is YOUR magazine—and as such, the thought-pieces presented are likely to provoke some of you to write. We welcome your letters and, as time and space permit, will publish as appropriate.

This is a period of tremendous Operational Tempo for the entire Army, and particularly for the Intelligence Community. Despite these demands, you have shared your knowledge and experience with the rest of the readership. We extend our sincere thanks to all who contributed their time and effort to the creation of this issue of MIPB.



A handwritten signature in black ink.

CW3 Del E. Stewart
Managing Editor

MILITARY INTELLIGENCE

PB 34-03-4

Volume 29 Number 4

October-December 2003



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

Chief Warrant Officer Three

Del E. Stewart

Editor

Elizabeth A. McGovern

Associate Editor

JoNell M. Elkins

Design Director

Specialist Ernesto A. Bolaños

Associate 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 changes of address and subscriptions, see page 28.

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 80.

Check us out on the Internet
<http://mipb.futures.army.mil>

FEATURES

- 5 **Lessons Learned: Six Things Every “2” Must Do—Fundamental Lessons from OIF**
by MG James A. Marks and LTC (P) Steve Peterson
- 15 **Lessons Learned: Task Force Sentinel Freedom OEF/OIF**
by COL Michael J. Gearty
- 17 **Open-Source Information: The Wild Card of the Modern Battlefield**
by John W. Davis (MAJ, U.S. Army, Retired)
- 20 **Deception – Magic!**
by John W. Davis (MAJ, U.S. Army, Retired)
- 23 **Language Choices**
by Ray Lane Aldrich
- 25 **Interpreters in Intelligence Operations**
by COL John S. Rovegno, Linda Hajdari, and Drita Perezic
- 29 **ASAS Contributions to Operation Iraqi Freedom**
by Michael J. Gaynor (CW3, U.S. Army, Retired)
- 31 **Software Engineering Center’s Support to CENTCOM 3Military Intelligence3Military Intelligence** by Don Adamson
- 32 **Lessons Learned: A Ground Surveillance System Platoon in Afghanistan**
by 1LT Jacqueline L. Dominguez
- 36 **Al-Qaeda Wave Attack Assessment**
by Ben N. Venzke
- 38 **Lessons Learned: Army National Guard G2X in Bosnia**
by MAJ Larry Lee
- 43 **CI and HUMINT Operations in Support of Operation Enduring Freedom**
by MAJ Ron Stallings and SFC Michael Foley
- 47 **Transforming Counterintelligence and Human Intelligence**
by CW3 Larry Norris
- 56 **Al-Qaeda Threat to Oil Industry and U.S. Allies**
by Ben N. Venzke and Aimee Ibrahim
- 59 **Commentary: Don’t Let Terrorists Spread Fear**
by John W. Davis (MAJ, U.S. Army, Retired)

DEPARTMENTS

2	Vantage Point	71	Sly Fox
3	CSM Forum	73	TSM Notes
60	Doctrine Corner	75	MI Heritage
66	Proponent Notes	77	Professional Reader
68	Distance Learning		

By order of the Secretary of the Army:

Official:

JOEL B. HUDSON

Administrative Assistant to the
Secretary of the Army

0328002

PETER J. SCHOOOMAKER

General, United States Army
Chief of Staff

Always Out Front

by Major General James A. Marks
Commander, U.S. Army Intelligence Center and Fort
Huachuca



During Operation Iraqi Freedom (OIF) and after some significant thought since my return to Fort Huachuca, a number of lessons learned themes became apparent to me. One of these themes is that with intelligence operations there is no "time out." We, as intelligence professionals, are always engaged. We are either postured for success because of hard training, thorough planning, meticulous preparation and aggressive execution, or we are postured for failure. We are no longer at a crawl, walk, run pace. In our current operational environment we must maintain intelligence readiness to support operations on no notice. Our Army is running; we must stay ahead!

This statement underscores the importance of our profession. Intelligence drives or fails to drive operations (to include decision making, operational execution, and targeting). If intelligence fails to drive operations we fail but, more significantly, soldiers' lives are at risk.

There are four specific aspects of this theme that I believe are important:

- Change our units and organizations, throughout the Army and Department of Defense (DOD), so that they are able to fight off-the-ramp within 96 hours.
- Get more modular.
- Significantly change our garrison and training activities so that we truly train as we fight.
- Help the Army develop mature, assured communications and battle command-on-the-move capabilities.



96 Hours

We cannot afford to wait for the future force tactical units (units of action) that are deployable anywhere in the world in 96 hours. The transition to this paradigm must occur now. The ripple effect of this change touches many different aspects of intelligence to include doctrine, training, force structure, organizational missions, intelligence reach, and building analytical collaboration. However, these are all manageable issues that we must tackle now. This change is non-negotiable, and we must start the process now.

Modularity

We need to relook many of our tables of organization and equipment (TOEs) and tables of distribution and allowances (TDAs) in light of the requirements to support deployable forces with modular intelligence teams within 96 hours, to provide intelligence support "24/7," and based on the complexities of the operational environment. New and improved intelligence systems are great, but technology means nothing without highly trained soldiers and civilians. In the near future we will scrub all of our TOEs and TDAs hard and make sure we have the right soldiers in the right positions in rapidly deployable modules. This must be available at all echelons.

Train As We Fight

MI must critically reevaluate itself "[*by*] changing our mindsets from depending on an 'intelligence buildup' to performing intelligence readiness checks on a daily basis. This change will allow us to meet the requirements for strategic responsiveness

(*Always Out Front continued on page 4*)

CSM Forum

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



In last month's article I asked you the leadership to try and find the time to think about next year's Command Sergeants Major/Sergeants Major (CSM/SGM) Worldwide Conference, to bring to the table those lessons learned from your formations involved with the global war on terrorism (GWOT). We are currently planning for the conference and solicit your input for panel subjects for breakout discussion, briefings, and speaking presentations for "our conference." What we the Sergeants Major all bring to the table will do nothing but train our Military Intelligence (MI) Warriors for success. Again, if there are any briefings, issues, or speaking presentations you would like for next year's conference, please email me at lawrence.haubrich@hua.army.mil or csm@hua.army.mil. Our conference's success is solely based on what "we," the Senior Noncommissioned Officers (NCOs) of our MI Corps, want to accomplish. Also, I need for all of our MI Sergeants Major to ensure I have their email address so I can continue to keep you updated on MI and Army issues and correspondence from the Sergeant Major of the Army and his office.

I need the MI leadership's help in making sure our soldiers are attending their respective Noncommissioned Officer Education System (NCOES) Course (that is, Primary Leadership Development Course [PLDC], Basic Noncommissioned Officer Course [BNCOC], and Advanced Noncommissioned Officer Course [ANCOC]). Currently Armywide we are at a two-year plus backlog in our schools. U.S. Training and Doctrine Command (TRADOC) is looking at the possibilities of developing and executing a fifteen-day program of instruction (POI) for PLDC. We at our NCO Academy are developing what we



will be calling a mobilization POI to fill the void of the backlog with our BNCOC and ANCOC classes. I need the leadership's help in assuring our soldiers show up for their respective NCOES classes. "NO SHOWS" are unacceptable unless there is a justifiable reason. We had six no shows at the last ANCOC, and some of the justifications I heard were totally unacceptable. I must remind the leadership conditional promotions are only for one year. Within that year the soldier has to attend NCOES; if not, they revert to their previous rank held. Exceptions to this policy have to be justified and are not approved automatically. Let's take care of our MI Warriors and get our sol-

diers to their respective NCOES schools. Taking care of our soldiers is NCO business. We make it happen.

Also, TRADOC is looking at piloting a Sergeant/E5 Drill Sergeant Program. I think this is another great program where the NCO can do nothing but excel. One of the issues addressed in this program was the STAR military occupational specialties (MOSSs) across the Army and the ability to fill those Drill Sergeant positions with SGT/E5's. We all know we have a fairly large inventory when it comes to "STAR MOSSs" in the Military Intelligence Corps. Again, I ask the leadership of MI to canvass their formations and to send those deserving soldiers who meet the "army standard" before the promotion board. Promoting those deserving soldiers will do nothing but strengthen our Corps in the Current Force and lay the foundation for the success of our MI Warriors of the Future Force. Our MI Warriors are the best and the brightest soldiers in our Army. Let's grow and groom them for success. This is why Military Intelligence is "ALWAYS OUT FRONT."

(CSM Forum continued on page 4)

(Always Out Front continued from page 2)

through our preparation in garrison. Intelligence operations must become the norm in all intelligence units.” – COL Charles Atkins

At the operational and strategic levels our intelligence teams usually staff their intelligence “go to war” systems every day. In these organizations we live by the ethos of “every soldier, every team, every day.” However, that is not the case especially at the lower tactical levels. At this echelon we still build teams as we deploy and, in some cases, as we cross the lines of departure. In order to fight off-the-ramp in 96 hours, we must break this model. The Army model for intelligence at all echelons while in garrison needs to mirror how, in my experience, our sister service, the Navy, operates every day. The Navy covers down on their “go to war” intelligence systems on board ship every day, whether they are in port or at sea. They train and fight with the same tools in the same configurations. We need to grow the number of headquarters that have already adopted this model and also continue to improve the realism of our intelligence training events and simulations.

Assured Communications and Battle Command-On-The-Move

We have already taken some early steps with this task by recommending a new Army strategy for expanded space-based communications as a result of lessons learned from OIF. A solid battle command-on-the-move capability is a part of the recommendation. OIF proved that if we are to conduct dominant maneuver through the depth of the battlefield as we did, assured communications are essential. We can no longer be satisfied with “Intel refueling stops.” We must realize in our lifetime effective and user-friendly battle command-on-the-move. Again, this change is nonnegotiable.

Together, we the collective body of the Army Intelligence Community and the larger DOD Intelligence Community must attack these issues head-on and find the right solutions. With the continuing global war on terrorism, intelligence is critical, and with intelligence operations there are no time outs. Now, we all need to move out sharply, play our part in shaping our future, and make sure we stand up and say

I GOT IT!

(CSM Forum continued from page 3)

As your MI Corps CSM, what I value more than anything is visiting your units and talking with our great MI Warriors in your formations. When talking with our MI Warriors, the feedback I get on what we at the U.S. Army Intelligence Center can do to ensure we are training the MI Warrior to be successful is irreplaceable. I learn so much from our great MI Warriors, and it is all of you in your formations which make me a better informed MI Corps CSM—smarter and successful in my job—so I thank you all for making my job easier.

At Fort Hood, I visited the 504th MI Bde, 15th MI Bn (AE), 303D MI Bn (Ops), and the 321st MI Corps Spt Bn (USAR), III Corps G2, and the TES-Main. This great MI Brigade is fully engaged with their soldiers deploying worldwide in support of GWOT. I also visited the 312th MI Bn, 1st Cav Div, which was going through some intense unmanned aerial vehicle (UAV) training and preparing for their future deployment early next year in support of GWOT. While in the great state of Texas I also went to Camp Bullis, where I visited the South West Army Reserve Intelligence Support Center (SW ARISC), the

470th MI Group, and elements of the 321st MI Corps Spt Bn (USAR). Rest assured, the MI Warriors at Camp Bullis too are engaged daily with GWOT. I also had the opportunity to visit our great MI career and assignment managers at MI Branch at Department of the Army Personnel Command. The soldiers and civilians at our MI Branch truly have their hands full in managing our warriors; they not only take care of the soldiers but also the families. I would ask you all whenever you are in the D.C. area to stop by and thank those soldiers and civilians at MI Branch for what they do. I have always said, our MI Community is a “Military Intelligence of One,” supporting the Army of One theme. We are the Active Component (AC), Reserve Components (RC), U.S. Army National Guard (ARNG), Department of Defense civilian, contractor, and retiree—a *Military Intelligence of One!*

Thank you all for what you do for our MI Corps and our Army and for teaching and making me a smarter and more effective MI Corps CSM. As always, let’s take care of each other and our families. You train hard, you die hard; you train easy, you die easy. Peace needs protection.

ALWAYS OUT FRONT!

Lessons Learned:

by MG James A. Marks, Commander, U.S. Army Intelligence Center and Fort Huachuca and LTC (P) Steve Peterson

During OIF MG Marks was deployed as the C2, CFLCC. LTC (P) Steve Peterson, Student National Defense University, was also deployed as the Chief Planner, C2, CFLCC, during OIF. This article and slides are adapted from the Intelligence Officer's Battlebook prepared for Military Intelligence leaders.¹

In March 2003, Coalition Forces under the leadership of the United States invaded Iraq to remove a tyrant. With slightly more than two divisions, we invaded a country the size of France with a population of approximately 26 million and entered into conflict with an Army of 23 divisions and approximately 450,000 regular and irregular forces. As coalition troops crossed the line of departure no one knew the degree to which Iraqi forces would fight, whether weapons of mass destruction would be used, and whether Saddam Hussein would order the destruction of dams to flood the approaches to Baghdad or the oil fields to hamper coalition operations.

We did know how Iraqi forces were arrayed, where they were likely to defend, whether they were moving, and what they were doing as the war approached. We knew water levels and rates of flow, locations of thousands of survivability and fighting positions, the status of heavy equipment transporters, preparations for defense or destruction of the oil fields, and thousands of other facts.

But intelligence is more than facts and figures. The Intelligence Battlefield Operating System (BOS) is—

- An adaptive network of properly trained, equipped, and deployed intelligence organizations manned by some of the finest soldiers and civilians in our nation.
- A complex system that operates worldwide, from mud-to-space in real time, in support of an operation, to include the ability to leverage theater and national capabilities.
- Cooperation and division of labor internally, higher, lower, adjacent, and across components and the coalition.
- Systems designed for collecting information, processing data, analyzing and refining intelligence and influencing decision making.

The job of the intelligence officer is to make it all work in concert to meet the commander's needs. The following principles are fundamental to a "2" at any echelon from battalion to Coalition Forces Land Component Command (CFLCC). It is a Herculean task, but the "2" can succeed by doing *six things*:

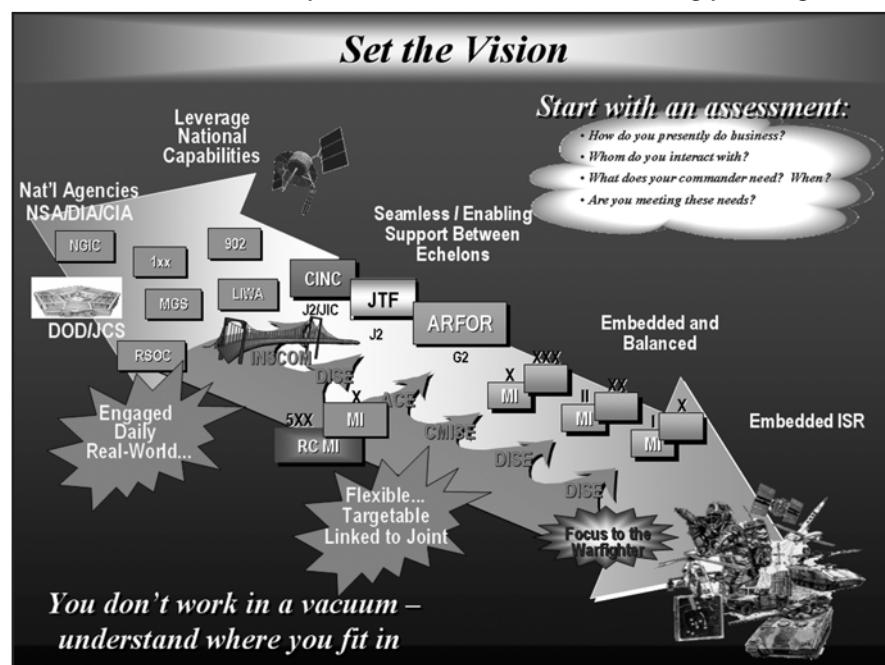
- Set the Vision.
- Build the Architecture.
- Build the Team.
- Build Analytic Collaboration.
- Fight Intelligence, Surveillance, and Reconnaissance (ISR).
- Influence Decision Making.

Six Things Every "2" Must Do—Fundamental Lessons From OIF

All six areas are closely interrelated, and the lines among them are blurred, but they provide a useful construct for conducting an effective intelligence operation. These *six things* were not pulled out of thin air; they were derived from a careful study of the evolution of the CFLCC C2 in preparation for and during execution of Operation IRAQI FREEDOM (OIF).

SET THE VISION

Doing the right things and getting them done right requires a vision—an objective for which to strive. Unless you have a vision and are driving your organiza-



tion forward, you will be falling behind. “Maintaining the status quo” should be thought of as “dead in the water.” As the “2” you must drive the organization forward by setting the standard for the staff—and for that, you need vision!

Start With an Assessment

To set the vision for your organization, you must first understand where you are starting. You must make an assessment and establish a thorough understanding of the baseline—your organization, personnel, systems, training, support, and where you fit in the context of the larger formation.

During OIF, after I was assigned as the CFLCC C2, I immediately set out to assess the existing organization and determine what was needed. I spent a month visiting organizations, consulting experts, and determining what resources we would need to leverage. We studied the enemy, our theater, and the units that would compose CFLCC. Then I set a clear vision and we worked to drive the organization to meet that vision.

Look at your structure and how you are organized:

- What are the functions performed by each part of your organization?
- How are you manned?
- Do your personnel have the skills to accomplish the mission?
- What systems are you using, both internally and to communicate externally?

Examine how you presently operate:

- What does your commander and staff need and when do they need it? Are you presently meeting your commander’s and staff’s needs?
- What do you get from and provide to subordinate, higher, and adjacent units?
- Lay out how you operate—identify the inputs you receive and the outputs you produce. What processes do you use to convert your inputs to outputs?
- What is the battle rhythm of your headquarters, your section, and of the intelligence organizations with which you interact?
- What would improve the quality of the support you are providing?
- Where does your unit fit in the context of the larger formation and in the intelligence effort as a whole?

Understand Where You Fit ...

You Do Not Work in a Vacuum

Successful intelligence operations influence decisions. Intelligence operations are essentially characterized by collection of intelligence, accurate reporting on that intelli-

gence, and access to national databases and analytic centers that contribute to the intelligence—i.e., collection, analysis, processing, and dissemination. As a “2” you will not work in a vacuum; you must leverage every possible resource. There is more to this task than you might think. Today, intelligence in support of tactical commanders depends on worldwide operations in real time (across services, joint, coalition—tactical to strategic).

During OIF, small unit actions drew directly upon national level intelligence delivered to commanders on the ground in real time. SIGINT operations involving national assets and entities on three continents were used to provide real time force protection and targeting data directly to tactical commanders. Similarly, IMINT products processed far from the battlefield were used to direct targeting, even to cross-cue and verify unmanned aerial vehicle (UAV) video to direct close-air-support (CAS) operations in real time.

Develop a List and Diagram

Begin to lay out where you fit. You are going to capture your place in the staff, the formation, your higher, lower, adjacent organizations, and other entities to which you will reach for data, products, or processing. Give yourself sufficient room because you are going to end up with a larger network of interactions than you first think. Write down your unit, its higher, the higher above that—go step-by-step all the way up to the national level (do this even if you are a battalion “2”) and do not leave out any echelon of command. Write down the echelons below you—go all the way down to individual soldier (do this even if you are at the combatant command level). Be specific and seek out those who can help you get it right.

You will rely on the collection and reporting that you diagram through all of these echelons, and the intelligence you produce is of relevance at these echelons as well. The modern environment blurs the strategic, operational, and tactical doctrinal framework. Success depends on seamless information exchange.

During OIF, the CFLCC Joint Analysis and Control Element (JACE) often leveraged NGIC extensively. The NGIC LNO understood the scheme of maneuver and priorities for that day. Together the JACE chief and NGIC LNO would focus NGIC’s exploitation of imagery to meet specific needs. At certain points in the battle, national imagery was exploited by NGIC and passed to the JACE within 30 minutes—a remarkable example of timely information exchange.

Identify the intelligence organizations and intelligence collectors associated with each entity and echelon. Do not forget that every element on the battlefield (combat, combat support, combat service support) is also a collector, processor, and communicator of information. Be

sure you include other services, coalition entities, and national agencies that will be operating in the battle space. If there are nongovernment organizations (NGOs), other international organizations, or press operating in the battle space, understand that they may be sources of information and intelligence that you can leverage as well. Understand who owns them, who controls them, who tasks them, and how and what they collect is processed, exploited, and disseminated.

Talk to other staff elements and find out what information and reporting systems they rely on for situational awareness (for example, artillery counter-battery radars, air defense missile and aircraft early warning, maneuver element scouts, aviation reconnaissance, service support convoy debriefings, etc).

During OIF, elements in the JACE had direct access to missile warning data feeds through a carefully designed architecture. As a result, they would receive missile launch warning even slightly before the rest of the CFLCC staff and could immediately begin working the cross-cueing of collection for counter-surface-to-surface missile (SSM) suppression and targeting.

Start to understand how all of these entities report and communicate. Diagram their connectivity in simple terms—just draw lines showing who talks to whom under existing structures. You will have many question marks and holes as you put together this diagram. When you run into an unknown, continue to press on and try to fill in the gaps.

Then determine which of these entities has information that is of use to you and your commander. Who in this diagram will have information relevant to you—not only in terms of the level of detail but also in terms of the timeliness with which it can be accessed? Who can provide you collection, processing, and analytic products that are not feasible for you to produce? Do not get hung up on how—that comes later.

Now seek to understand what networks they are tied into. Work to understand how entities will communicate higher, lower, adjacent, and through intelligence reach to support outside the theater. Develop a close working relationship with the communications officer. You will need to understand general battlefield communications structures and architectures as well as the intelligence specific communications structure. Some entities bring their own communications (for example, satellite communications, high frequency, etc.) independent of that unit's networks.

During OIF, National Security Agency (NSA) teams deployed with SATCOM capabilities in order to leverage national processing in real time. NIMA deployed its own communications packages to provide bandwidth necessary to pass imagery in a timely manner. These teams brought capabilities to the Corps, the Marine Expeditionary Force (MEF) and, in some cases, to the Division level.

Finally, you need to take a close look at your requirements again (what the commander, staff, and you need). You have to understand what outputs you must provide and to whom. For each output, which will you produce and which will you get from others? As you set your vision, objectives, and the baseline for your tactics, techniques, and procedures (TTPs), keep in mind three considerations: relevance, timeliness, and tailored products for the decision makers.

BUILD THE ARCHITECTURE

Think of an architecture as simply the set of interconnected physical systems by which you receive or pass information or data from one entity to another for a specified purpose. In thinking about an architecture you will need to think about inputs, processors, communications, and outputs. More specifically you will need to think about hardware, software, communications, circuits, communications security (COMSEC) materials, network classification, technicians, funding, database access, liaison officers (LNOs), training, and TTPs.

Use the list and diagram that you developed as a part of the vision and add details, to include specific questions and answers, about what your requirements are, what you have in place now, with whom do you interact (send and receive data, information, and intelligence), and what communications are in place.

During OIF, CFLCC had a highly capable, skilled, and talented systems architect. The commander made it very clear that having a vision to drive the architecture is the most critical aspect of building an effective architecture.

The Devil Is in the Details

Now you are ready to start working through the specific details of moving data and building the architecture. None of this will happen unless you pay close attention to putting the architecture in place to accomplish it. Do not assume that this is something that will happen on your behalf—it will not, and the parts that do will not work the way you require. If you are thinking, “I will leave that to the Army, the contractors, and the systems experts to provide,” you will fail. Although you will rely on experts to work through the details, you must define the functions the architecture will perform and ensure it will get you what you need when you need it.

Build the Architecture

Science (Technology) and
Art (What's it doing for me?)

- What do you need?
- Who has it? "Pull"
- How do I get it?

- What do you have?
- Who needs it? "Push"
- How do I get it to them?

"If you aren't talking, you're just camping."
- 3rd Infantry Division AAR

Depending on what echelon you are at, your architecture might be relatively simple (for example, at battalion level) or it might be very complex. Every situation is different. You will never master all the technical aspects of every architecture and do not need to. However, you do need to know how to think through the development of an architecture and the types of questions to ask to ensure that your architecture meets your requirements. Whether you are a battalion S2 or a combatant command J2, there are basic things you will need to know. Some of the things you will have to know include—

- ❑ Where you will operate from and where you will be moving.
- ❑ What you want to receive and send (from and to where, whom, and if they will be moving).
- ❑ What communications and COMSEC will be required.
- ❑ What power and facilities will be required.
- ❑ What operator training will be required.
- ❑ What maintenance and system or data administration will be required.
- ❑ What approvals and permissions will be required.
- ❑ Interoperability of data, communications, hardware, and software.
- ❑ How the architecture will need to grow over time.
- ❑ What alternative methods and means of communications are available.

Work With Others

The answers to the previous set of questions plus many others will help you define the architecture. By doing your homework and setting a clear vision you can get

During OIF, CFLCC used a system called command and control personal computer (C2PC) to display the common operating picture at all echelons. Bandwidth limitations made it difficult to pull map data across the network. To overcome that limitation, systems loaded the map data locally and then only had to send and receive overlay files and across the network. This dramatically reduced the demand on limited bandwidth.

the decision maker's and other staff's consensus, approval, and resourcing to build your architecture. Some tips to succeed include:

- ❑ Make use of experts to work through the technical aspects of the architecture.

- ❑ "Sell" your objective architecture and understand how to build it incrementally.
- ❑ Look for other people's money first. Contingency operations come with money.
- ❑ Prioritize those pieces that can demonstrate tangible results and use those results to gain further buy-in.
- ❑ Realize that there are often opportunities to make gains with little investment. First look for opportunities where procedural or policy changes will yield improvements.
- ❑ Look for ways to leverage existing architectures in different ways. When bandwidth limitations do not let you pass imagery in real time, load it to local storage devices in advance and only pass overlays during operations.
- ❑ Prepare to make use of the unfunded requirements process and do not hesitate to work internal budget processes to compete for resources.

Drive the Architecture to Meet Your Functional Requirements

If you need live, full motion video, you will have to put the systems, communications, hardware, and software in place to get it.

During OIF, we decided early on that we wanted to distribute Hunter video across the theater. To do so required the development of an architecture that could make use of the Global Broadcast System (GBS). This required CFLCC to bring GBS stations into theater for units that did not normally have them. It also required engineering of display architectures.

You will have to do the same if you want specific capabilities for unit reporting, terrain data, geospatial products, measurement and signature intelligence (MASINT), signals intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT), open-source information, technical data, etc., as a part of the architecture.

During OIF, national systems that processed intelligence in the United States, Europe, and other locations across the globe were used to provide immediate force protection warning and targeting information to soldiers and marines in contact. This was possible because the architecture foresaw the need for immediate communications with NSA that were not available through "organic" communications. This was identified to the command, and the CFLCC C2 advocated a request to provide the Corps and the MEF with Critical Source Lites with analysis teams. This task required the right hardware, software, communications, circuits, COMSEC, technicians, funding, database access, LNOs, and TTPs.

In today's world, intelligence is mud-to-space. It is complex and technical. Do not be afraid to ask questions and admit what you do not know. You will need to leverage experts—do not let them baffle you with "techno-speak." Sometimes they do not know as much as they want you to think. Remember also that sometimes you do know more than you think. Only by asking questions of many different people will you learn whom you can rely on. Remember, no one will give you the architecture you need unless you define it and put personnel to work building it. Having the right architecture is critical to your success as a "2." Pay attention to the architecture development early and ensure it will deliver what you need.

While the right architecture is important, it alone will not deliver success. Intelligence depends upon analysis. And there is no better analytical engine than the human mind. Remember, intelligence is about predicting human behavior, and it takes "men in the loop" to do that effectively. Your ability to put together the right team is critical to your success as a "2."

BUILD THE TEAM

As the "2" you must build a team that spans echelons and organizations. Building the team involves understanding who else you must work with within the unit—higher, lower, adjacent, and across the intelligence community—through effective intelligence reach opera-

tions. It is a matter of knowing capabilities, training the necessary collective skills, establishing effective relationships, developing mutual battle rhythms and TTPs, and leveraging the right architectures and collaboration tools.

Individuals

Teams rely on skilled individuals. You must ensure your soldiers are equipped with the right skills to perform the required tasks. They need to be competent in their military occupational specialty (MOS) and/or area of expertise. You must ensure they receive the training and certifications necessary to be expert in their individual specialty skills. As you develop battle drills, production requirements, standing operating procedures (SOPs), and TTPs you must train your soldiers within each area. Since they will leverage a variety of tools, you must train them on their use. They must understand the hardware, software, communications, and databases—how to use them and how to troubleshoot them.

During OIF, the JACE recognized how critical specialized systems training was and leveraged all-source analysis system (ASAS) training teams prior to deployment and again in theater. They also ensured software and hardware experts were embedded in the staff.

Intelligence soldiers also must be highly proficient at briefing, writing, and other communications skills. Intelligence is worthless if it does not influence decision making. Therefore, leaders must train every intelligence soldier in how to communicate clearly and effectively. Miscommunication leads to incorrect analysis, incorrect conclusions, and incorrect decisions. Even if a sol-

Build the Team

➤ Intelligence is a team sport – played on many different fields simultaneously

➤ You must build a team that spans echelons and organizations – across the battlefield, the theater, and the globe

dier is not a briefer, we must train him or her to be precise and succinct to facilitate collaboration with other members of the intelligence and greater warfighting team.

During OIF, the JACE ensured that its six weeks of vignette training incorporated the requirement that the junior analysts briefed the products they developed to the senior leadership.

Sections

Section training is the next level essential to team building. No individual works alone. You must give attention to building the “digital squad.”

During OIF, this was another area of emphasis during the JACE’s vignette training. Each section had to develop a functional diagram to show where it fit in the context of the larger intelligence effort. They had to understand their products, the products of the other sections, and the ways in which they interacted. Thus, when the war began, there was no misunderstanding of roles or dependencies and the JACE functioned quite effectively as a single entity.

Across Sections

Just as you must have the right skill sets within a section, you must have the right distribution of skills across sections. Do you have a battle captain that knows how it all fits? Can your senior analysts correctly inform and leverage the collection effort? Do your collection managers understand their role? Training is obviously a critical part of team building. You must train as you fight and practice as a team; only in this way will you build synergy. However, building the team goes beyond matters of training alone.

Teamwork across sections also includes organizational structure, the physical configuration of work areas, and collaboration with external agencies and with other parts of the staff. Structure yourself to facilitate teamwork.

During OIF, CFLCC paid close attention to physical structure as an important aspect of team building. It rearranged its organization to improve interactions and built facilities that would allow optimal interaction and synergy between sections. When the JACE was hampered working in tents, CFLCC designed and built an open-floor structure that would allow the sections to improve fusion, mutual situational awareness, and cooperation. We embedded intelligence elements within the different operations and planning elements to ensure optimal teamwork with the rest of the CFLCC staff. Additionally, we relocated some systems to ensure they were properly used and realigned the HUMINT Analysis and Requirements Cell under the JACE when we needed to improve crosstalk.

You cannot work effectively as a team unless you know your counterparts, have practiced with them, and understand the positions they hold. You must understand the organizations in which they work, their role in those organizations, and how they interact with your organization.

During OIF, the CFLCC went to great lengths to do this. They had face-to-face coordination meetings with U.S. Central Command (CENTCOM), major subordinate commands (MSCs), and personnel from all participating intelligence agencies during the months leading up to the war. Additionally, they had training exercises and rehearsals. Finally, they began the MSC video teleconferencing (VTC) in November to develop and practice TTPs in the December and February exercises. Analysts used chat and information workstation (IWS) sessions (on-line collaboration tools) and VTCs to coordinate their efforts. TTPs for web posting were put in place throughout all units and agencies. By the time hostilities began, the CFLCC intelligence team extended literally around the globe.

Battle Rhythm

Battle rhythm is another important aspect of building an effective team. You must understand your command’s battle rhythm and how it fits with the battle rhythms of higher, lower, and adjacent commands as well as within the larger intelligence community. You must work to nest your battle rhythms within these other battle rhythms so you are providing effective and timely inputs to decision making.

C2 Battle Rhythm					
Time	Zulu	Local	Event	When	Where
0100	0400		CENTCOM JJC/JOC UPDATE VTC	Daily	CC SCIF
0200	0500		HUDDLE	Daily	WAR RM
0230	0530		CSC/C2 MAP HUDDLE	Daily	WAR RM
0300	0600		C2 VTC to MSCs	Daily	CC SCIF
0430	0730		COMBAT ASSESSMENT BOARD	Daily	DOCC
0430	0730		SOF/OGA	Daily	C3 OFF
0600	0900		CO INTEL UPDATE	Daily	CC SCIF
0630	0930		PLANNING GROUP MEETING	Daily	OPG RM
0700	1000		DAILY EFFECTS BOARD	Daily	DOCC
0800	1100		BATTLE UPDATE ASSESSMENT	Daily	CMD CTR
0900	1200		IO BOARD VTC	Daily	JACE VTC
1000	1300		FUOPS SSE MEETING	Daily	JACE TENT
1030	1330		COMPONENT COMMANDERS BOARD VTC	Daily	CC SCIF
1130	1430		HUDDLE	4-5 x/wk	JACE
1145	1445		I2 OPS/PLANS VTC	T, TH	JACE VTC
1200	1500		EFFECTS WORKING GROUP	Daily	DOCC
1230	1530		C35 FUOPS Brief to CG	As needed	OPT Conf
1330	1630		JOINT COLLECTION MGMT BOARD VTC	Daily	JACE VTC
1400	1700		OPNL PROTECTION WORKING GROUP	Daily	PMO
1515	1815		CENTCOM TARGETING COORD BOARD VTC	Daily	CC SCIF
1515	1815		OIL VTC	TH	JACE VTC
1700	2000		COMPONENT INTEL VTC	Daily	JACE VTC
1800	2100		BAGHDAD UPDATE VTC	FRI	JACE VTC
1945	2245		WMD VTC	Daily	JACE VTC
2000	2300		BATTLE UPDATE ASSESSMENT	Daily	CMD CTR

Bold Text = CFLCC Battle Rhythm Event

Italic Text = C2 Internal Event

Normal Text = Events with CFLCC, CC, or MSC staff

Liaisons

The effective use of embedded liaisons is an important aspect of teamwork with national intelligence organizations through intelligence reach. The most effective intelligence reach operations have a “front end” collocated with the supported organization. This liaison must be more than a passive representative in order to be effective. The liaison must—

During OIF, we were successful at using battle rhythms to work as a team across the unit; the timing of the daily CFLCC MSC VTC synchronized the intelligence picture with V Corps and I MEF. The VTC was held at 0600 local. This was after the 0400 analyst-to-analyst VTC with CENTCOM and before the intelligence update to the Commanding General at 0800. It gave the opportunity for the C2 and the G2s to discuss the intelligence picture, gain a common understanding of planned operations, and discuss the intent for collection before their first decision-making sessions within their respective staffs. Thus, the Intelligence BOS spoke with one voice each day.

- Understand their parent organization thoroughly to include capabilities and how to leverage them.
- Come equipped with the right database accesses and have the right communications.
- Must be proactive and involved in all aspects of the plan.
- Aggressively advocate for applying their parent organization's capabilities to the fight; they must not wait to be tasked.
- Look for opportunities to contribute. However, even the best liaison forward can succeed only if his parent organization provides a responsive point of entry at the home station.

Optimally, the parent organization will have a dedicated support element whose battle rhythms will be 24/7 and matched to the forward element's needs. When both of these conditions are met (a responsive representative forward and a tailored support element at the parent organization), team work is optimized.

During OIF, the CFLCC was fortunate to have many liaison elements and supporting organizations that functioned in this way. The best example was NGIC. NGIC's liaison was superb. He was involved in every aspect of CFLCC intelligence operation. This liaison developed superb methods of coordination with the JACE, understood NGIC's capabilities, and understood how to leverage NGIC. The other critical part of NGIC's superb support came from the NGIC commander's willingness to reorganize to provide optimal support. NGIC matched its battle rhythms to CFLCC's needs.

BUILD ANALYTIC COLLABORATION

Effective analytic collaboration must leverage complementary capabilities. This requires more than an architecture that enables communication and the use of collaborative tools. It requires careful mutual planning, division of labor, defined responsibilities, and procedures for adapting to changing circumstances as they develop.



Build Analytical Collaboration

- Leverage complementary capabilities
- Avoid duplication of effort
- Requires:
 - Mutual planning
 - Division of labor
 - Defined responsibilities
 - Procedures for adapting to change




Assign the right tasks to the right unit.

Prior coordination and thorough planning is the key to effective analytic collaboration that avoids duplication of effort, ensures maximum coverage, and provides for optimal analysis. You must assign the right tasks to the right entities. This cannot be done in isolation; you have to work to secure agreement from team partners on their responsibilities, timeliness requirements, procedures, and under what circumstances arrangements will be changed. Division of labor works best when responsibilities match organizational interests. Similarly, assign responsibilities to organizations that have the most direct access to the information for which they are responsible. Make units responsible for analysis and reporting in (and often beyond) their areas of operation and for collection reporting for assets they command and control. Do not assign responsibilities to organizations that do not have the capability or the architecture to respond quickly enough to meet your needs.

It is very important to develop procedures for dividing responsibilities to avoid duplication of effort. If three organizations all receive the same data feeds, you do not want all three to focus their effort on the same exploitation problem. For example, you do not need National Imagery and Mapping Agency (NIMA), National Ground Intelligence Center (NGIC), and your Tactical Exploitation System (TES) all exploiting the same piece of imagery while other imagery goes unexploited.

During OIF, this was not always accomplished well. There were actual instances in which three organizations worked on analyzing the same piece of imagery simultaneously while other images went unexploited. To make the problem worse, in at least one instance all three organizations gave different reports based on the same piece of imagery. Fortunately, this was the exception and not the rule and in most cases CFLCC had effective collaboration procedures in place.

You must also plan how you will shift effort as the battle develops.

During OIF, CENTCOM took responsibility for the Republican Guard; Europe Command (EUCOM) Joint Analysis Center (JAC) had responsibility for the corps in the Northern Reporting Area; and CFLCC had the III and IV Corps. CFLCC further gave responsibility for the first echelon divisions to V Corps and I MEF. Operations proceeded very quickly and outpaced a shift in analytic responsibility. CFLCC's interest turned to the Republican Guard prior to responsibility for tracking it passed to them.

The above scenario emphasizes that it is important to plan in advance what the intelligence handover lines will be in managing the analytic distribution of responsibility.

FIGHT ISR

I use “Fight ISR” here specifically instead of “manage collection” (or the new encompassing doctrinal task of intelligence synchronization) to emphasize that the proper application of ISR assets is a combat multiplier when treated like a weapons system—one that we must focus at the point of decision, and dynamically retask as the situation changes. Fighting ISR also includes the intelligence equivalent to the operational paradigm of “fight the enemy not the plan.” This mindset includes using well-developed procedures and carefully planned flexibility for dynamic retasking in support of emerging targets, cross-cueing, and for post-strike battle damage assessment (BDA). Processing, exploitation, and cross-staff combat assessment procedures must be developed and practiced in advance if they are to be effective.

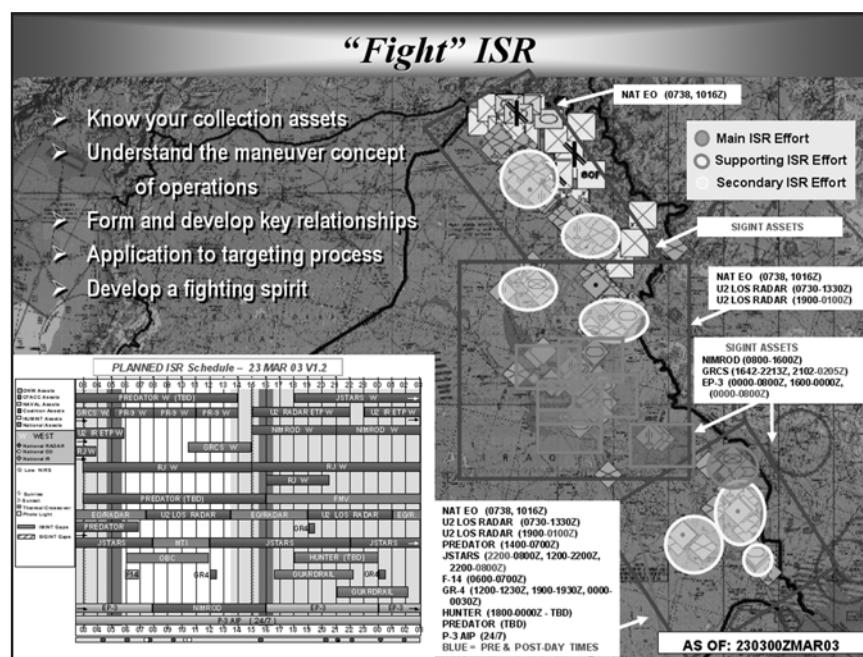
Of all of the tasks a “2” must undertake, fighting ISR is perhaps the most challenging. It requires detailed specialized knowledge and training and the ability to effectively use a variety of complex visualization and collection management tools. Most importantly, it requires a collection manager (at some echelons the “2” is the collection manager) that—

- ❑ Shows a fighting spirit.
 - ❑ Thoroughly understands war-fighting, targeting, and ground maneuver.
 - ❑ Aggressively competes for resources and does not take no for an answer without a fight.

- Verifies every collection detail during planning and follows up during execution.

Several conditions must be met for the “2” and collection manager to “fight ISR” effectively. The “2” and collection manager must thoroughly understand—

- ❑ Every aspect of the collection assets operating in theater, to include capabilities and limitations (those they control and those controlled by others).
 - ❑ Tasking, processing, exploitation, and dissemination for each collector, along with how they are employed.
 - ❑ How collectors communicate and how they can be retasked dynamically.
 - ❑ Effective cross-cueing and the leadtimes for retasking.
 - ❑ Targeting and the processes by which target decks are loaded, sensor packages are selected, and assets are allocated.
 - ❑ The collection planning process and the battle rhythms associated with the air tasking order (ATO) and the execution of planned collection.
 - ❑ The physics of the battlefield and the staging and employment of assets.
 - How long will it take an asset to get to the target area?
 - How quickly and how far can it travel if dynamically retasked? What threat conditions will limit its employment?
 - What are the ranges and durations of its missions? What factors may constrain its operation (temperature, elevation, etc)?



The development of a detailed plan enables the collection manager to be an effective advocate for the allocation of collection resources he does not control. It also helps him cover gaps using other assets when he is not successful in securing support from higher echelons. Collaboration higher, lower, adjacent, and across components is also essential; there must be synergy between the application of collection assets. Duplication of effort must be avoided and procedures for handing over collection responsibilities across boundaries must be well understood, coordinated, and practiced.

While fighting ISR the “2” and collection manager must—

- ❑ Use systems that show in real time where the collector is and what it is looking at and they must have the ability to communicate with those who control the platforms.
- ❑ Use established procedures for getting immediate processing and exploitation.
- ❑ Understand the maneuver concept of operations, the commander’s priority intelligence requirements (PIRs), and enemy capabilities and doctrine.
 - Actively participate in the planning process and they must communicate effectively with the commander to ensure his priorities are being met.
 - Use well-developed relationships with collection managers, analysts, and asset managers at higher, lower, and adjacent, and remain in close contact with those who control the tasking and employment of the collection platforms.

INFLUENCE DECISION MAKING

A “2” can get everything right if he sets the vision, builds the architecture, builds the team, builds analytic collaboration, and fights ISR and still fail if he does not influence decision making. “Perfect intelli-

gence” is useless if the commander does not receive it, does not understand it, or does not believe it. Your success depends on your credibility with the commander. Credibility is the critical prerequisite to influencing decisions and the key to being an effective “2.” Here is how you build credibility:

- ❑ Know what commanders, staff, and soldiers at all echelons need for the fight and give it to them. You must know both your business and the business of warfighters; you cannot be an effective intelligence officer unless you understand what warfighting is all about.
- ❑ Adapt your products to the needs of the commander. You must master the visual portrayal of information to communicate quickly, clearly, and succinctly and put the information and intelligence in forms your commander best understands.
- ❑ Be competent, confident, and communicate clearly.
- ❑ Know the business of intelligence inside out. You must know intelligence capabilities and how to leverage the greater intelligence community.

Relevance, timeliness, and tailoring products to the decision maker—these are the critical elements to remember in producing intelligence. To influence decision making, you must be in the thick of it. You must be an integral part of developing the plan. In fact, you must shape the commander’s interest and not merely respond to it.

Intelligence must drive operations, but it will not automatically happen. It depends on you. Set the vision, build the architecture, build the team, build collaboration, fight ISR, and, above all influence decision making. If you do, you will set the standard for the staff and serve your commander well.



During OIF, the CFLCC C2’s role in influencing the decision to attack early to seize the oil fields to prevent their destruction is a superb case study of how a “2” can effectively influence decision making. It started with an assessment persuasively stated to the C5. After convincing the C5 that we would best achieve tactical surprise by a ground attack before air operations, we put the case before the Commanding General who discussed it with the CENTCOM Commander (all well before operations began). The C2 equipped the MEF with intelligence products tailored to their requirements, which prepared them to attack quickly and effectively. At the point of decision, effective intelligence analysis and collection equipped the “2” with a proper read of the indicators that the Iraqis were preparing to destroy the oil fields. Effectively presenting that case to the Commanding General and CENTCOM led to the decision to attack early. That decision was well inside the Iraqi’s decision cycle, and the results were superb. Intelligence drove operations.

Endnote

1. Readers can obtain a copy online at AKO Knowledge Coordination Center "After Actions Reviews" folder under "Intel Officer Handbook and OIF Lessons Learned" subfolder.

MG James A. Marks, a native of New York was commissioned 4 June, 1975, into Military Intelligence upon graduation from the United States Military Academy. During his 26 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, KY; Aide de Camp, Commander in Chief, U.S. Pacific Command, Camp Smith, HI; S3, 319th Military Intelligence Battalion (Airborne), 525th Military Intelligence Brigade, XVIII (Airborne) Corps, Fort Bragg, NC; Executive Officer, 313th Military Intelligence Battalion (Airborne), 82d Airborne, Fort Bragg, NC; Commander, 107th Military Intelligence Battalion, 7th Infantry Division (Light), Fort Ord, CA; G2, 6th Infantry Division (Light), Fort Wainwright, AK; Special Assistant to the Chief of Staff of the Army; Com-

mander, 504th Military Intelligence Brigade, Fort Hood, TX; Deputy Chief of Staff, Intelligence, Headquarters, US Army, Europe and Seventh Army, Heidelberg, GE; 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; deployed as C2, Coalition Forces Land Component Command; resumed Command of United States Army Intelligence Center and Fort Huachuca. He is an Honor Graduate of the U.S. 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.

Influence Decision Making

- **There is no “perfect” intelligence**
- **Put your fingerprints on your intelligence**
- **Take ownership – no “information fondling”**



*Intelligence is useless if the commander doesn't receive it,
doesn't understand it, or doesn't believe it.*

Lessons Learned: Task Force Sentinel Freedom OEF/OIF

by Colonel Michael J. Gearty

In this time of war, the U.S. Army Intelligence Center (USAIC) is living up to the Military Intelligence Corps motto "Always Out Front" in more ways than one. Not only has the Center of Excellence continued its proud traditional missions within the U.S. Army Training and Doctrine Command (TRADOC) construct of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities—DOTMLPF—we have literally stepped up to the plate in the Global War on Terrorism (GWOT) and are directly engaged with commanders, staffs, and soldiers in the field. And it should come as no surprise that USAIC has been in the fight long before the bullets, SCUDs, and Patriots started to fly in mid-March 2003 during Operation Iraqi Freedom (OIF).

As early as November and December 2002, as part of the road to war, key subject matter expert (SME) "tiger teams" deployed to Camp Doha, Kuwait, from Fort Huachuca, Arizona, to begin to assess operational postures of systems, equipment, architecture, and training, to name but a few key areas. But even before that, select groups of intelligence professionals representing the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH) deployed to various units and areas throughout Afghanistan to identify critical intelligence requirements and shortcomings in the very earliest days of the GWOT. From the outset, it was clear that "Task Force Sentinel Freedom" was fully engaged and committed for the duration of the conflict. But it is not enough, because commanders can never get too much actionable intelligence. We have a long, long way to go.

Today, in both Afghanistan and Iraq, in OEF/OIF, intelligence is the en-

gine that drives operations. Battalion, Brigade, Division, and Coalition Joint Task Force (CJTF)-level Commanders are listening to their "2" and planning and executing operations based on the "2's" read of the situation. At least one division commander recently told his S2s and G2, "I am going to be tougher on you than anyone else in this entire organization." Rightfully so. Intelligence must be laser focused in order to drive operations and simultaneously protect the force.

Several examples of intelligence successfully driving maneuver highlight the point, not the least of which is the violent, fatal, and deliberate U.S. Forces' housecall on Uday and Qusay. This was based on a Human Intelligence (HUMINT) tipper received less than 24 hours prior to execution. Both OEF and OIF theaters have undeniably grown into HUMINT-intensive battlefield environments. The demand for "oven-fresh" actionable intelligence is understandably sky-high from commanders who have either enjoyed first-hand operational success with HUMINT, know a fellow commander who has, or purely and simply must have specific, timely, and accurate intelligence on who and where the enemy is and what he is planning next in order to take the fight to him first. But even given the current operational environments lending themselves to stability operations and support operations, it is not only HUMINT making a difference in finding the bad guys but also Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Measurement and Signature Intelligence (MASINT), and even Open-Source Intelligence (OSINT) contributing to an all source intelligence effort.

That's where we come in—again—we being Task Force Sentinel Free-

dom OEF/OIF. From 9-11 in 2001 through today, we have brought the very best that the world's premier intelligence center and school has to bear against some incredibly challenging technological, culturally dynamic, and humanly complex intelligence requirements. In short, some very tough nuts to crack. For example, we are taking some very important lessons learned from successful interrogation techniques used on al-Qaeda and Ba'athist Regime Death Squad "hard cores" at Guantanamo Bay, Cuba, right back to Afghanistan and Iraq. Task Force Sentinel Freedom OEF/OIF Mobile Training Teams (MTTs) are currently in theater instructing CJTF-180 and CJTF-7 "HUMINTers" on these lessons learned and more very specific skill sets to glean key pieces of information hidden somewhere inside the 20 or so centimeters between detainees' ears.

Approach techniques, cultural savvy, and psychological understanding of the mindset of an enemy prisoner of war (EPW) are but a few of the key and critical skills our SMEs are getting across to our guys downrange asking the tough questions. And since it is infantry and armor soldiers who are out in the streets and neighborhoods of places like Bagram, Baghdad, Mosul, Kandahar, and Tikrit dealing with people and situations everyday, we're executing on-the-job tactical questioning skills training with our maneuver brothers-in-arms and learning a great deal from each other in the process. The same holds true for our combat support and combat service support soldiers beating the bush day in and day out.

The All-Source Analysis System New Equipment Training Team (ASAS NETT) MTT recently returned from a two-month training and fix-it

trip to Kuwait and Iraq. The expertise in systems hardware and software, networking, and architecture these noncommissioned officers (NCOs)—ASAS Master Analyst Course graduates—bring to the table is phenomenal and exactly the type of hands-on “fix-it now” skills soldiers and leaders in theater are looking for. Another ASAS NETT MTT is currently in Germany preparing 1st Infantry Division soldiers and units for upcoming operations in OIF2.

These MTTs are but three examples of ongoing efforts in support of U.S. and coalition forces in theater time now. Call this Phase I. Phase II will include additional MTTs over the next few (three to six) months designed to provide more solutions—read FIX IT—vice “assess” it—to existing problems with existing forces in theater. Phase III will comprise MTTs and efforts primarily in support of units and soldiers who are projected to go downrange to either Iraq or Afghanistan in upcoming and successive rotations. In addition to 1st Infantry Division mentioned above, Task Force Sentinel Freedom OEF/OIF is fully engaged with III Corps and 1st Cavalry Division in the critical synchronization of training, equipment, and architecture in preparation for OIF2. 25th Infantry Division will receive the same levels of energy and dedicated professionalism from Task Force Sentinel Freedom OEF/OIF as Tropic Lightning units and soldiers get ready for OEF-A.

Task Force Sentinel Freedom has built a number of relevant and focused blocks of instruction to meet current and emerging theater warfighter requirements. The 2X course is designed to fill big gaps in much needed areas of knowledge on how to analyze Counterintelligence (CI) and HUMINT, understand what you know and what you don’t know, and how to manage assets and information to reduce the difference between the

two. We believe this 2X course, with applications from Battalion through CJTF, is long overdue throughout the community, and will be a valuable toolset in any operational environment. As with most other courses in support of OEF/OIF, the 2X course will include an MTT and residence version for maximum flexibility to deploying or deployed units and soldiers. Similarly, Task Force Sentinel Freedom is developing tailored MTT instruction in CI to Force Protection Source Operations (CFSO), Advanced Interrogation Skills, and All Source Analysis Skills.

Again, it has not been all about just CI/HUMINT. The TRADOC Systems Manager (TSM) and Program Manager (PM) Prophet have partnered with National Security Agency (NSA) in order to rapidly enhance SIGINT collection capabilities in response to a changing communications target. In a unique venture, the Prophet team and the Army Cryptologic Office (ACO) have delivered the Prophet Hammer system to every division and armored cavalry regiment (ACR) in Iraq, providing increased collection capabilities and Very Small Aperture Terminal (VSAT) communications reach to the Gordon Regional Security Operations Center (GRSOC) as well as NSA. An intrepid crew from the ACO delivered the system and trained soldiers in Iraq, and the Prophet Hammer system is already proving its worth in the urban fight. The Prophet Hammer is a successful example of the Technical Insertion Concept—providing theater-specific collection capability to the tactical unit. The Prophet Hammer is ideally suited for the Phase IV mission in Iraq, and is providing commanders with much-needed force protection information and enemy intent. In fact at the recent Infantry Conference, warfighters singled out Prophet Hammer and Technical Insertion as key enablers and a success story.

And speaking of success stories—Hunter Unmanned Aerial Vehicle

(UAV) has been an absolutely phenomenal workhorse throughout the course of OIF combat operations, so much in demand that units have literally flown the engines off them and have TSM-UAV hopping to keep up with high usage operational tempos. Two of the three corps units deployed supporting OIF totaling over 450 sorties and 2,200 flight hours. Overall, the Hunters performed very well during the war, successfully locating artillery, tank, and rocket-launcher targets during their extended-range intelligence, surveillance, and reconnaissance missions. They assisted in cross-service cueing for the Marine Corps and Air Force to destroy high-value targets. And Shadow UAV is quickly establishing itself as a highly reliable, flexible, short-duration platform. Designed primarily to provide brigade commanders flexibility with surveillance and reconnaissance, two Shadow systems are supporting OIF totaling over 450 sorties and 1,900 flight hours to date. Like Hunter, they were able to locate Iraqi weaponized trucks, tanks, armored personnel carriers, and para-military personnel; and conducted force protection, route reconnaissance, and security support prior to raid missions. Finally, the Hunter/Viper Strike (Armed UAV) has successfully passed its tests and, if fielded to the theater, promises to be every bit as lethal, if not more so, than its Air Force counterpart, Armed Predator.

The wealth of lessons learned in the GWOT and the rich level of experiences throughout the Intelligence Community demand that we sit up and pay attention. Task Force Sentinel Freedom OEF/OIF has and will continue to incorporate the Center for Army Lessons Learned findings as a baseline for returning to the DOTMLPF construct. Key to Task Force Sentinel Freedom’s commitment to unit,

(Continued on page 70)

Open-Source Information: The Wild Card of the Modern Battlefield

by John W. Davis
(Major, U.S. Army, Retired)

(Article updated: From ARMY Magazine, July 1997. Copyright 1997, by the Association of the U.S. Army and reproduced by permission.)

Imagine the horror of death by friendly fire. See the faces of a mother and father at the moment they are told their son or daughter was killed by American fire. Today, far more than bullets can cause this horrific scene. This is a new age, and there are new threats.

Information warfare is the latest theme to capture the imagination of the U.S. Army. The Objective Force, the technological army with the narrow soldier base, depends on the rapid and accurate flow of information to fuel its highly technical killing power. To protect its classified information, this army can depend on traditional security elements. This new army, however, also generates a massive amount of unclassified material that is overlooked by traditional security measures. Could this material reveal the secrets the Army hopes to protect? In the information revolution, "open-source" information is the wild card of the modern battlefield. It is a form of friendly fire. The Army must protect this vulnerability through operations security.

Information—its access, use, analysis and control—is clearly a military matter. Classified information is protected by an array of security measures that are well known and practiced. But what about the literally millions of bits of unclassified personnel, logistical, operational, and supply documents that the Objective Force is generating? What can this information reveal and who

will watch over it? What will protect this information that spews out over unsecured faxes, E-mail messages, and telephone networks?

The General is skillful in attack whose opponent does not know what to defend, and he is skillful in defense whose opponent does not know what to attack.

—Sun Tzu 400-321 B.C.

In the furor over recent revelations of Chinese espionage, who has asked how much they gathered from totally legal, totally open-sources? What country will risk a major espionage recruitment when the same materials could be collected from an uncontrolled, open military website? Was it not Mao Tse Tung himself who counseled that, "The commander applies all possible and necessary methods of reconnaissance, and ponders on the information gathered, eliminating the false and retaining the true, proceeding from one to the other, from the outside to the inside..."? Does this not suggest collecting the unclassified until one can interpolate the secret?

The Army must face this modern problem. Can the flow of information necessary to conduct operations hurt the Service? What if the unclassified material is so voluminous, so comprehensive that it reveals the essential secrets the Army is otherwise so careful to protect?

At the beginning of World War II, some 300 British engineers died because they could not defuse the new electrical bombs dropped by the Germans over England. It took trial and error and the chance discovery of intact electrical bombs on a downed German aircraft before the technology was defeated.

Eight years earlier, in 1932, the technology for such bombs had been entered into the public records of the British patent office, yet none of the engineers knew about this open-source of information.

Three hundred men died while the answer they sought gathered dust in an unlikely place. Those who build the bombs that killed these men had found the information first and laid claim to it legally and openly. Had they known this, it would have been easy to convince the British people of the value of open-source awareness.

A shop-worn story of yesteryear? Are hired workers on North Atlantic Treaty Organization (NATO) compounds in the Balkans pacing off mortar ranges, as did the Vietnamese before them? Was it not the Belgian resistance fighter who said that people who experience occupation know the adversary better than he knows himself?

An earlier example involves the Maxim gun. When asked in 1884 why Western nations had colonized almost the entire known world, the English writer Hilaire Belloc said that it was not because of their advanced civilization, greater universities, or cultural advances.

No, he quipped, "Whatever happens, we have got, the Maxim gun, and they have not!" Of course, the technology for this early machine gun and other technological information was routinely shared and sold in open contracts between "civilized" countries. In World War I this exchange of information resulted in the slaughter of an entire generation; by then all nations had access to the Maxim gun.

These stories show how open-source, openly available information works. What is routinely, even inadvertently given away today could kill someone tomorrow. Information that is not tracked could later surprise the Army on the battlefield. These stories about open-source information end in bloodshed. Is it inappropriate to say that the victims died from friendly fire?

Information is the lifeblood of the high-technology Objective Force. An array of information will deploy with the Objective Force wherever it goes, whoever the adversary is. Unlike most of the adversaries of the United States, whose technological developments are not shared openly, much of the information about the Objective Force's development is available to the entire world. For example, the Associated Press reported on a Pentagon armaments display showing soldiers with heat-sensitive night-vision sight, lightweight body armor, and computer backpacks. They reported concepts about laser warplanes, seagoing missiles, and more. Today there are many armaments magazines, defense sites on the Internet, and newspapers reporting the business of warfare. These open-sources of information are cheap, readily accessible, and accurate.

Through the eyes of a Western analyst, the publications are what they seem: military trade journals that cover market share, sales opportunities, competitive and joint ventures, and national acquisition goals. They are straightforward.

Graphs and computer-generated art enhance the stories and illustrate the concepts. In the photographs used, sleek missiles fly, spotless armored vehicles roll, and wholesome, clean soldiers pose with the latest weaponry in pleasant pastures. There is no blood.

Consider now the reader of this same information from poorer, less industrialized, embargoed, or other-

wise ostracized nations. Consider also the people of para-nations, the ethnic clans, narcotics traffickers, and terrorists. They see the same information in terms of life-or-death choices. They cannot afford technical research or development, and they cannot "comparison shop." They know they must choose wisely the first time because there may not be a second choice. For them, the only collection method may be what they can learn from open publications. The more sophisticated groups can build on information from open-sources and confirm their conclusions with traditional collection methods. Their interest is far from abstract.

Several truisms must be accepted in this new world of half-wars against nontraditional adversaries. Poorer nations want to survive. In order to do so they are offered the Hobson's choice of spending what wealth they have on arms or relying on a guardian nation to arm their people. They are not interested in future sales, in market share or in the bottom line. If they do not choose correctly from the arms necessary to protect themselves, they will cease to exist, or worse, be enslaved. Obviously, they see the world from a dramatically different perspective.

The West views military technology as a chess game. One player creates this, the opponent creates that to counter it, and so on. In this rational game of give and take, no one dies and the game goes on. Some call this the arms race, but nobody dies in a race. Such a sterile view of the industry misses the point.

Analysts of arms markets from non-Western countries or para-nations see the armaments industry differently and arguably more clearly than Western nations do. They, like the United States, will determine their needs and do all within their power and budget to acquire those necessities. Unlike the United States, they see their existence as often nasty,

brutish, and short. They often feel they must confront the killer at the door, rather than the economic competitor in the pinstriped suit. It is not surprising that poorer countries decided to buy machine guns as soon as they could afford them, once they saw what happened to those who did not.

The callousness of the Western businessman who commented about a recent technology theft, "Who cares, we'll just build a counter-measure," would be incomprehensible to his counterparts in a poorer country who bet their very existence on successfully using proven technology in the near term.

Those of poorer countries have a vested interest in what is available on the arms market today, and in knowing how their potential adversary will fight. What if their potential adversary is the United States?

These poorer countries want to know, simply put, how to beat the United States in battle. To be able to surprise the U.S. military, they will try to learn more about it than the military knows about itself. They do not have the wherewithal to conduct massive technical research, so they will take any shortcut. All open-sources will be exploited. Why spend the money on research and development if the final product is going to be for sale or is explained on the Internet? Why test weapons if the answers nations seek are printed in publications that cost only a few dollars each? Comparison tests will be done by those governments that see weaponry more as a commodity to be marketed than as a means of killing people.

Western powers think of long-term strategies while poorer nations wonder how to stop the immediate threat. They know they are dead if they make the wrong choices, so they research information thoroughly. If they can piece together information about the true intentions of an adversary from what they can collect

on the open-source market, they will do so. It may be the only source they have. These are the types of adversaries the U.S. military will confront tomorrow.

These differing perceptions of the world—one by rich nations, the other by poor—must be better understood. A poor man does not care about higher technology tomorrow if his weapon will surprise his enemy today. To achieve this he may act in a way contrary to what the West considers being in his best, rational interest. Westerners must see the world with new eyes—their potential adversary's eyes. History offers many examples.

In the 1920s, for instance, a beaten Germany, penned in by the Treaty of Versailles, entered joint ventures with Bofors Corp. of neutral Sweden. The Germans had studied the published armament policies of other European nations and had observed the soldiers occupying their country. They had studied what would win on a future battlefield, then set out to get it any way they could.

Before World War II, Germany illegally trained its army on the land of its arch-rival, the Soviet Union. Despite open reports of Germany's illicit training, other nations were too complacent to challenge this threat. The West was thinking about long-term, rational arms races. Germany was thinking about a blitzkrieg.

In a later example, the United States was shocked when it was revealed that the Vietnamese communists had routinely spliced into U.S. telephone lines. Open communications were compromised. These were simple farmers who should not have had the capability, the United States complained. The nation did not see the world through its adversary's eyes.

Today, are the Afghani or Iraqi government troops trained by us going to rest assured that the West will protect them? Did the Serbs or Mus-

lims rely on the United States or NATO to take action against a vengeful adversary, or did they take their own measures? Does anyone doubt, however, that all soldiers and irregulars that deal with the U.S., be they on our side or against us, are devouring every statement and operational move we make in our many deployments?

Every open document, every routine, every movement, every communication made by the U.S. military's soldiers is subject to collection or observation. Seemingly innocent communications could confirm or deny the fears of the many groups involved in Afghanistan or Iraq, not to mention Kosovo or Bosnia or Liberia. How many American soldiers realize that a TDY order, supply form, repeated practice, or logistical document could betray the military's true intentions?

Westerners may see no great loss when technology is compromised because they may never see the battlefield result of their work. They may think abstractly of their product as a funded program, not as something that kills someone. Their counterparts in another, less powerful country would face imprisonment or execution if they compromised hard-gathered information.

Westerners must "publish or perish." They have a "right to know" and a free and inquisitive press. Non-Western counterparts do not. The arms race fuels the West's ever-expanding market and the information-rich marketing ethic that advertises it. The military must create policies that protect all of its information—even the unclassified—because, in this new world, information that kills soldiers is a commodity available for sale.

Operations security, a process of securing this unclassified information, whatever its form, can protect the Objective Force. The security process is simple. Each element of the Army must ask itself, "What is it

that I must protect, or else I'll fail in my mission?" The answer is that critical information must be protected, as Sun Tzu noticed so long ago. Not everything that can compromise a mission is classified.

Next, the collection threat to this critical information must be studied. Soldiers must consider who wants what they have. Here, the intelligence community can provide assistance. The collection capability could be a highly sophisticated process or a hacker who can read the Army's E-mail. In weighing the threat to the critical information, the answer to the next question, "Is the Army vulnerable?" may be surprising. Even units with 100 percent traditional security of their classified information have been compromised by a hemorrhage of unclassified data. Unit leaders did not tell their soldiers what was critical to protect, and soldiers did not control bar talk, telephone talk, or what went out over the wire, much less what went into the trash. After the risks are weighed, such as collection capabilities and reaction times, countermeasures must be decided on.

The Army must communicate to accomplish any mission, but it has to remain aware of the unseen listener. Soldiers must know what an adversary can do. To survive, other countries will read everything the Army writes and listen to any conversation they can. The Army has to see itself as others see it.

Once they learned that the Viet Cong had made tiny mines from discarded C-ration cans, soldiers stopped leaving cans uncontrolled. Now, the Army should do no less with its open-source information.



John W. Davis is a retired U.S. Army Major. He teaches the threat portions of the Department of the U.S. Army's Operations Security course at the Space and Missile Defense Command, Huntsville, AL. Readers may contact the author via E-mail at john.davis@smdc.mil and by telephone at (256) 955-1727 or DSN 645-1727.



Deception - Magic!

By John W. Davis
(Major, U.S. Army, Retired)

German bombers rumble relentlessly across the night sky of North Africa following a radio beam directed from German-occupied Libya toward the British port of Alexandria, Egypt. The flight commander notes an anomaly. The beam directs him forward, but he can see the lights of Alexandria to his left. The beam is known to be correct, but below him are city lights. Not only can he see the few inevitable lights in violation of blackout, he can easily see ships' lights in the harbor. He turns toward the lights and bombs... nothing.

In Africa during World War II, German bombers were led astray by an English deception plan that included mimicking Alexandria harbor. Creating the illusion of the actual city, lit by false house and ship lights, British officer Jasper Maskelyne, a professional magician, deceived the deadly German bombers into dropping their bombs 8 miles from Alexandria.

Deception on the battlefield is a force multiplier whose target is the adversary's mind as much as his technology. Deception can be countered by understanding the rules that govern suggestion or, better said, magic.

Successful deception events are occurring worldwide. Despite being monitored by sophisticated surveillance techniques and technology, India exploded a nuclear device under the world's nose. In Kosovo, the Serbs used fake tanks to drain away allied air sorties. Artillery that the Vietnamese "did not have" at Dien Bien Phu appeared as if by magic after having been secretly delivered

from the Korean peninsula. In each case, the adversary was well and truly deceived.

Appearance, Belief, Enticement

The great Chinese military philosopher Sun Tzu wrote:

All war is deception. Hence, when able to attack, we must seem unable.... When we are near, we must make the enemy believe that we are far way. [We must] hold out baits to entice the enemy.¹

Almost every U.S. Army officer has read Sun Tzu's words. Yet, the U.S. military is little prepared for deception operations, which comprise a significant component of information operations. Why?

U.S. analysts tend to misinterpret Sun Tzu's text. Americans are a pragmatic, formulaic, and technology-trusting people. Sun Tzu uses verbs that refer to the mind, emphasizing appearance, belief, and enticement. How something seems or appears, what is believed, and enticement are activities discerned by the mind, not by technology. Deception in war deceives first the mind, then the eye. Few U.S. military analysts would dispute this, but fewer still offer assessments as if they believe it.

Basic military intelligence apparatus is sensory. We use platforms to see and hear the enemy. We base assessments on what is perceived as cold, rational fact. Appearance, belief, and enticement are mental, not sensory words. The U.S. military interprets enemy activities based on what can be seen, heard, and touched.

When a weaker country confronts a great power, the weaker knows it must employ deception to prevail. The U.S. Army's lack of ability in recognizing deception makes it not only vulnerable but also weaker because deception is a force multiplier.

The Principles of Magic

The principles of magic, which all of us—especially children—enjoy, include the following:

- Disappearance.
- Appearance.
- Transposition of objects.
- Physical change in an object.
- Apparent defiance of natural law.
- Invisible sources of motion.
- Mental phenomena.

These principles also govern deception. We all know the adage that the



hand is quicker than the eye. The magician seems to deceive the eye, but this is not true. The hand is not quicker than the eye. The magician actually beguiles the eye. In war, an opponent tries to beguile his adversary's perception. What appears factual might actually be an artful creation with which to convince

the adversary that it is real. Properly understood, these principles can be used to assess the battlefield, to assess intelligence reports, and to defeat deception attempts.

Deceiving the Mind

Before the enemy employs deception, he must analyze the situation, because to defeat his enemy, he must first understand how the enemy thinks. He can then orchestrate the adversary's responses. He will work to understand the enemy better than the enemy understands himself, then he will deceive the enemy's brain, not his eye.

The Germans Versus the Soviets—I

Soviet dictator Joseph Stalin despised and feared English Prime Minister Winston Churchill more than he did German dictator Adolf Hitler. Indeed, we know that in 1941 Stalin believed that reports of an imminent German attack were part of a brilliant British disinformation campaign, not a brilliant German deception operation. Even when undeniable Wehrmacht military buildups were observed and reported by communist spies, Stalin dismissed the reports because the Germans had orchestrated an illusion that played to Stalin's fears of the British. The Germans suggested that the buildups were simply to pressure the Soviets for concessions in an upcoming parlay, making Stalin believe the buildups were in no way a prelude to war. In fact, when a German diplomat stated that war was imminent, Stalin believed and asserted that the nefarious disinformation had reached the ambassadorial level. The Germans had only to convince Stalin of their benign intent until they were ready to launch the great assault of Operation Barbarossa.

The Germans Versus the Soviets—II

In World War II, during the battle of Stalingrad, massed Soviet gunfire suppressed German artillery batteries one by one. Even when the Germans were out of sight, crater analysis served Red Army intelligence sufficiently well to blast the enemy gunners. Except for one battery, the German guns were silenced. This unseen battery fired away, despite massive counter-battery fire. Soviet analysts plotted and targeted every meter of ground near where the guns could possibly be. Yet the Germans kept firing and killing Russians by the score. The mystery was only solved after the Germans surrendered. The wily battery commander had hammered his guns into the frozen Vistula River. Thus, he appeared to be defying natural law. The facts did not change; the enemy's brain had been tricked.

ies one by one. Even when the Germans were out of sight, crater analysis served Red Army intelligence sufficiently well to blast the enemy gunners. Except for one battery, the German guns were silenced. This unseen battery fired away, despite massive counter-battery fire. Soviet analysts plotted and targeted every meter of ground near where the guns could possibly be. Yet the Germans kept firing and killing Russians by the score. The mystery was only solved after the Germans surrendered. The wily battery commander had hammered his guns into the frozen Vistula River. Thus, he appeared to be defying natural law. The facts did not change; the enemy's brain had been tricked.

The Germans Versus the British

Nordpol was the code name of a German deception operation practiced against England early in World War II. British-trained agents were dropped into Holland from secret night flights. Each agent had a radio with which to contact London to vouch for his safe arrival and subsequent actions. Despite the fact that when reports began to come in they did not include confirmation codes, the British never suspected that the operation was compromised. Only when one of the imprisoned British agents escaped was the truth revealed.

Desire to believe something is true can cause the denial of confirmatory observations. In this case it was often believed that the agents were too tired or too mentally drained to identify themselves properly. The allies ascribed reasons to each and every inaccurate message. The Germans gave just enough true information to offset any total reassessment by the English agents. Thus, a subtle form of disappearance was used.

The absence of confirmatory codes was explained away by simply allowing the British to fill in the

reason themselves. After all, were not valid, if relatively insignificant, messages coming from the agents on the ground? German counterintelligence personnel knew that a deception must fool the prevailing adversarial interpretive mind. They understood that when bureaucracies vouch for something, they are virtually impervious to change thereafter. When the first captured British-trained agent's confirmation was believed by his English handlers, the Germans concluded the others would also. The Germans knew that the most difficult path for any analyst was to try to counter received opinion, particularly in the intelligence field. If the high command said all was well, who were the analysts to argue?

The Arabs Versus the United States

The Arab world regularly denounces the U.S. media's stereotypical portrayal of them as Middle Eastern terrorists. Osama bin Laden exploited this belief when instead of attacking embassies in the Middle East his followers blew up two U.S. embassies in Africa, where the attack was a total surprise. The sudden appearance of Arab terrorists in benign backwater countries far from disputed areas was something the United States had never suspected or planned for.

The Russians Versus the Chechens

During the recent Chechen rebellion against Russia, the Russians trapped Chechen rebels in Grozny. The rebels offered the Russians hundreds of thousands of dollars to allow Chechen fighters to escape safely through a minefield that surrounded the beleaguered city.

The Chechens knew Russian corruption well. In fact, they had bought many weapons and much ammunition from the Russians for money and hashish. Why not pay to survive to be able to fight another day?

The money was passed, the path through the minefield was cleared, and the day of escape approached. At dawn, the Chechens entered the minefield. To their shock, the Russians, using registered artillery fire, began firing on the Chechens, forcing them to run in panic into areas where the mines had not been cleared. A Russian general commented later that what surprised him was that the Chechens believed the Russians at all.

Chechen perception of what was true about individual mercenary practices was not true about the Russians' relentless will as a group. Russian individual corruption could not be extrapolated to the entire army. We can learn from this that we can be deceived by our own preconceptions when falsely applied to known facts.

What the Mind Believes

Many people still debate whether British and American double agents Kim Philby and Alger Hiss were actually guilty of spying for the enemy. They were of a certain social class, so many people consider the possibility that they could have been traitors inconceivable. If all members of a leading social class are loyal, how can they betray their country? The trick was observable, but the mind did not want to *believe*. Even when Hiss appeared in the Venona decrypts, his supporters refused to believe he was guilty. If Philby and Hiss were guilty, a veritable "natural law" was compromised.

During World War II in North Africa before the attack at El Alamein, the British were confronted with the problem of how to hide thousands of barrels of gasoline. The solution was to line the barrels up side-by-side, snug against the edge of abandoned

trenches that had been dug months earlier. The German analyst, having viewed the same trenches in dozens of aerial photos, would not notice that the trench shadow was just a little wider than before. What *appeared* to be truck parks with lazy campfires nearby confirmed for the analyst the absence of danger. Yet, when the British attacked, it was with well-fueled tanks that had been hidden under fiberboard truck covers. The attack turned the tide in the Sahara in favor of the British. Transposition of objects helped defeat German aerial observers because although they observed the field of battle, they never really saw it.

During World War I, when the Arabs revolted against the Turks, British military liaison T.E. Lawrence and Arabian tribesmen appeared to be mired in a torpid, sleepy wadi, unable to take a major town or, indeed, to even formulate a plan. Suddenly Lawrence and his compatriots struck as if from nowhere to take the town of Aqaba. The Turks were shocked because they believed that the wide, sandy wastes could not be crossed.

In World War II, U.S. General Douglas MacArthur believed the Chinese army incapable of advance without detection by the United States' superior aerial intelligence systems. Chinese General Mao Zedong's army advanced by night, using the threat of death to keep the men under cover by day. They took U.S. troops by surprise by secretly crossing the Yalu.

Appeared (seemed), believed, enticed—these are abstract words; words of the mind, not of technology. U.S. analysts must be aware of preconceptions. They must ask themselves what they believe to be

true. This is perhaps the hardest question they can ask themselves. Whoever answers this question will best be able to use, or defeat, deception. This insight casts into high relief what Sun Tzu meant when he said, "If you know the enemy and know yourself, you need not fear a hundred battles."²

Exploiting Beliefs

If we know ourselves, we have identified the first target of an adversary's deception. We can then ask how the enemy might try to deceive us. What is he doing to exploit our beliefs? What is he doing to make us believe something? How is he making himself appear? What will he try to entice us into doing? Using these concepts to manipulate us can be powerful force multipliers to a determined enemy.

If we apply counterdeception, which corresponds to an awareness of the principles of suggestion as used in magic, we can begin to interpret an adversary's schemes. The power of suggestion, or magic, has been used for thousands of years. The adage, "we are not deceived; we deceive ourselves," is only true if we allow it to be.

EndNotes

1. Sun Tzu, *The Art of War*, Chapter 1, verses 18-20.

2. Ibid., Chapter 3, verse 18.



Major John W. Davis, U.S. Army Reserve, Retired, is an Intelligence Operations Officer, U.S. Army Space and Missile Command, Huntsville, Alabama. He received a B.A. from Washington University, St. Louis. He has served in various command and staff positions in the continental United States, the Netherlands, Italy, and Germany. Readers may contact the author via E-mail at john.davis@smdc.army.mil and by telephone at (256) 955-1727 or DSN 645-1727.

Have You Moved Recently?

Please notify **MIPB** of your address change. You may send an E-mail to mipb@hua.army.mil with a subject: "Address change." You can also call (520) 538-1009 or DSN 879-1009 or write to U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-FDT-M, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017.

Language Choices

by Ray Lane Aldrich

Afghanistan? Iraq? What do they speak...over there?

The bottom line is, "The commander asks for what he needs." There is no substitute for boots-on-the-ground experience.

That said, there are ways to narrow the field of choices. That's what we at the Army Foreign Language Propriety Office (AFLPO) try to do early enough to appear as if we knew what we were doing when the requests begin to come in. The process has improved significantly since we were hit with the initial question of, "What do they talk in Somalia?" We were at a total loss. Everyone in the office had grown up in the simple bipolar world of the U.S. versus Russia and China.

If you let your attention wander for a moment, the whole world changes around you. We weren't totally asleep; we knew the general solution in Somalia, we just weren't certain what language they spoke.

I'm not positive we're better now. We're certainly a lot less naive and we have developed a system and plan for doing a little advance research. Let me take you through some of the steps and reveal not only the thought processes involved but also some of the actual sources of information, on which we've come to rely.

We have come quite a way since Somalia. While I've personally decided that the whole process is just as well done using the techniques of the Crone who sends the Thirteenth Warrior on his way, there is now a semi-scientific method involved. Don't ask about "The Ethnic Name Test"!

The first thing I usually check is the Central Intelligence Agency (CIA) World Fact Book. It is on-line, comes with a nifty little map, and provides some interesting background information beyond just the languages spoken in a given country. From "the Fact Book" you can get a feel for the religions, the ethnic backgrounds, the education level, and some of the political forces at work on the country. I take the coward's way out on this and print out anything that looks remotely interesting. That way I'm covered, in "the file," when most of the conventional questions are asked.

The second thing I check is the Ethnologue database. It too is on-line. These are the folks that bring you the magic number of "6,800 spoken languages." They are known also for their involvement with the Summer Institute of Languages (SIL). Their primary purpose is "bible" publishing. In the process, they check to see what languages need to have bibles published. The primary result of all of this scholarly investigation, beyond "more than you really want to know about bibles," is a list of the languages spoken in a given area and a general feel for the number of speakers of that language.

Beyond the first two sources, the investigation process gets a little confused and inconsistent. This is one of those areas in which there is no such thing as knowing too much. No other sources of information consistently have the answers that we need. I usually end up checking Country Studies, the old Area Handbooks, now available from the Library of Congress and, if you're lucky, from your local library. A word of caution concerning these Country Studies, however, many of them are dated.

As long as we're looking for information, one of my prime considerations is getting as much as I can without having to stir my seat from in front of the computer. I have my coffee source, my soft drink source, my restroom, my co-workers, and, oh-by-the-way, my boss, all close at hand.

I then turn to my local search engine for either the country involved or the "language du jour." Tourist guides are often quite helpful, bearing in mind that you need to maintain your military perspective.

Another necessary place to look, once you've gathered most of your generic language information, is the AR 611-6 list of Language Identification Codes (LICs) and a quick scan of the other language data contained in the appendixes. You may have to dig for an older copy to find some of the data. Please, also be aware that there are some errors that have been incorporated in the LICs shown in the regulation.

Once you have the LICs for the languages that look like your best candidates for use, you then need to figure out how many linguists the Army has in that particular "flavor." Yet another caution, under the heading of nothing is ever as easy as it should be, there will be some languages in which you are interested that do not have two-digit LICs. Be flexible. The data may not be correct. I don't KNOW why! I have a couple of theories, but they aren't pertinent in this article.

The most memorable case, to me at least, involving incorrect data was back during the Somali Scavenger Hunt. According to the data available, the Army had ten Somali linguists. When we really began to check for the people involved, we

discovered what we actually had were five Samoan linguists whose LIC had been incorrectly entered and five Reserve Component soldiers who were enrolled in the "Simultaneous Membership Program." We actually had no Somali-speaking soldiers. (In case you haven't figured it out, the LIC for Somali is "SM.")

I usually check "ALF" (the Automated Linguist Finder), Ed Christie's linguist database from the Defense Manpower Data Center (DMDC), because I can, it's quick, it's on my desk, and it's consistent. You will probably not be as fortunate. Regardless of what database you check, what you really want to know is if there are any soldiers in the Army with the desired LICs. Now, well before you need the information, is a good time to investigate possible personnel databases.

Once you've determined the likelihood of linguists in a particular language, you're on a divide. Your own specific situation will determine your next course of action. Can you go after individuals? Do you go after individuals? The bottom line in this process, the guiding principle, is that ONLY Personnel can actually "reach out and touch" an individual. The Personnel system is the only system that has access to and really understands the factors that are involved in grabbing a warm body for your particular job.

There are a number of aspects to consider that may be far more important than your desire to set a linguist to work on language stuff. For one thing, we have now begun to talk about individuals, real soldiers. We have gone beyond the academic investigation and moved into an area where there is significant potential to really mess with a soldier's life. The folks in Personnel have access to significant quantities of information concerning that same soldier.

There is nothing that says you can't help Personnel. That help may even include providing them with a list of soldiers that you feel may fill the needs of the requesting commander. When you get down to the personal level, the level where you have an actual name, you can then activate the most scientific tool in our language toolbox. This tool is so secret that I hesitate before I insert it into this open publication. This tool is called "The Ethnic Name Test." I would welcome some other name for this particular tool; I just haven't been able to devise one. If you have a suggestion, please send it to me. "The Ethnic Name Test" is best applied to a list of acknowledged speakers of a given language. You then look at the list and consider that the combination of a 3/3 linguist with a name appropriate for the language/geographical area in-

dicates a strong probability that the soldier should be among your first choices for general language and area knowledge. (I told you it was scientific!)

At this point you are just about finished with anything helpful you can add to the process. By all means, continue to gather information, post maps, post lists of words in the appropriate languages; do anything to increase the available knowledge to enable a valid decision to be made. After the requests begin to come in for linguists in a particular language, walk around, muttering quietly to yourself, "I can't believe they didn't ask for any (Blank language) linguists. I know it's rare, spoken only by 47 tribesmen, but it's pivotal for those environs."



Ray Lane Aldrich has been involved with military aspects of foreign languages through Air Force Enlisted, Army Warrant Officer, and, ultimately, Army Civilian Staff positions. He gathered training in Russian at Indiana and Syracuse Universities, German at the Defense Language Institute, a Bachelor of Arts degree in Russian Area Studies and Russian at the University of California, and graduate focus in the Army Management Staff College. He currently represents the Army Foreign Language Propriety Office for the Deputy Chief of Staff for Intelligence, Washington, D.C., and specializes in military foreign language management. Readers can reach Mr. Aldrich at ray.aldrich.hqda.army.mil and telephonically at (703) 695-1379 or DSN 225-1379.

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 let us hear from you. You can write to us directly at ATTN ATZS-FDT-M, US ARMY INTELLIGENCE CENTER AND FORT HUACHUCA, 550 CIBEQUE STREET, FORT HUACHUCA, AZ 85613-7017, or email us at del.stewart@us.army.mil or mipb@hua.army.mil.

Interpreters in Intelligence Operations

by Colonel John S. Rovegno,
Linda Hajdari, and Drita Perezic

Kosovo operations proved once again our dependence on linguist outsourcing. The military has been unable to predict the location of the next conflict for most of our existence, and therefore have not fielded the quantity of military linguists we need to provide timely, accurate, predictive, relevant intelligence to the commander, thus guaranteeing mission success. When the call comes, we frantically cross-train current linguists into new languages and deploy with the best rudimentary skill sets we can muster. Enter contract interpreters.

They come from all walks of life, and for our current mission, primarily from the Albanian Communities around New York and the Serbian Communities near Chicago. They leave behind civilian employment, school, or retirement; don battle dress uniforms (BDUs) and body armor, and live, eat, and work beside us in the combat zone. They are as heroic as our soldiers and don't ask for praise.

Doctrine provides little insight in performing intelligence operations with civilians possessing limited military training. Experience shows us if we don't immerse them into our operations, we limit our successes and lose out on a significant force multiplier. We must use this experience to develop future doctrine for intelligence collection.

This article chronicles how contract agencies recruit and train civilian interpreters. We then review their military training, assignment to a unit, and assimilation into operations. We show what works and what doesn't and recommend solutions for future operations.

Who Are They?

Interpreters are civilians, hired by contract agencies for the U.S. Government because of their unique language skills. Unlike most military linguists, interpreters speak with native fluency. They learned the language either living in the region or at home in the U.S., because their families have strong ethnic ties to the region.

We classify interpreters into three categories based on security clearance. Category I interpreters are hired

locally, usually possess English as a second language, and do not have a security clearance. Category II and Category III interpreters are all U.S. citizens who generally grew up in a bilingual home in the U.S. Category II interpreters have a Secret Clearance while Category III interpreters possess a Top Secret.

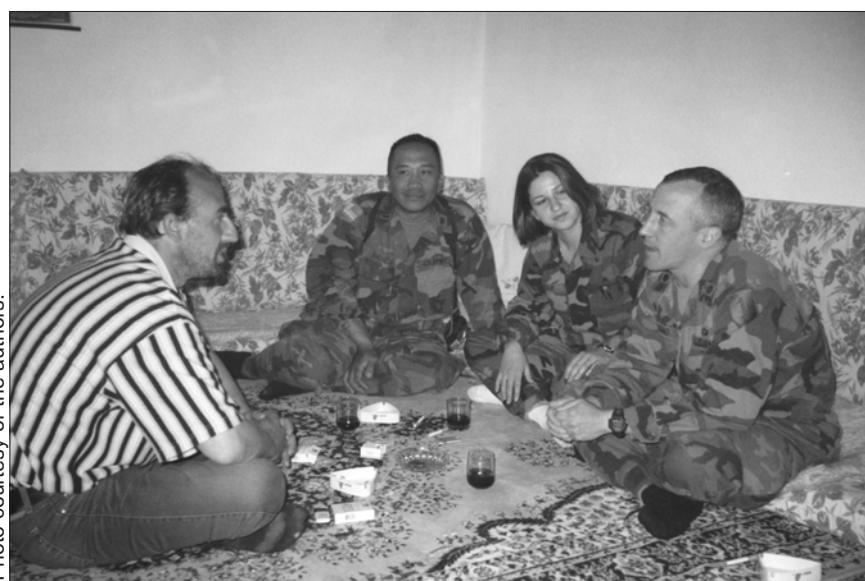
While Category I linguists far outnumber the other categories, they do not work with intelligence units because of security reasons. They do perform a vital role as interpreters for the many patrols and operations working throughout the sector, which do not have as critical of a need for interpreters possessing a clearance. The majority of interpreters working with our unit were Category II, possessing the same Secret Clearance as most of the soldiers on their team. Category III linguists usually work either with high-ranking officers, on teams conducting more sensitive operations, or out of sector conducting sanctuary collection operations.

Recruiting and Initial Training

Contract corporations such as TRW recruit, assess, hire, and train our civilian interpreters. TRW also conducts background checks and initiates initial security clearances. Recruiters begin with acquaintances and network to find more potential interpreters. Their other principal recruiting methods are newspaper ads and word of mouth. The recruiters focus on known concentrations of people having the target language.

Initially, no one knows about the operation, so it is critical that recruiters have as much accurate information about mission, duties, and living conditions as possible. If people do not fully understand what they are getting into, they are very likely to quit or spread negative

Photo courtesy of the authors.



The authors (far right) conducting liaison with an Albanian Mayor (left); assisting is CW3 Ancheta.

DO'S AND DON'TS

- ❑ Remember the interpreter is a facilitator and not part of the conversation.
- ❑ Remain in the first person and request that your interpreter do the same. This takes time to get used to and you might feel rude, but it keeps the conversation between you and your source.
- ❑ Maintain eye contact with your source, not the interpreter. Sometimes body language, facial expressions, and reactions speak more than the actual words, making it crucial that you remember you are speaking to that particular person and not the interpreter.
- ❑ Pace yourself. Limit the number of ideas in one statement. If you try to include too much, the interpreter could forget key points.
- ❑ Allow the interpreter to use a notebook if necessary. This is not to keep a record of what was said but rather to assist in the process by creating a quick reference to ensure nothing is lost in the linguistic exchange. If the notes in the notebook are of a sensitive nature or cause OPSEC concerns, ask that your interpreter give them to you once they are done.
- ❑ Ensure interpreters engage only with the person you are speaking to. Side-bar conversations can sideline communication, prolong meetings, and create diversions.
- ❑ Work out signals ahead of time with your interpreter. If you find yourself in a potential threat situation, work out a signal the interpreter can give to disengage. Many times you will be surprised to know that the person you are talking to does in fact speak English or has a working knowledge of the language.
- ❑ Don't use jokes, maxims, or analogies. They don't have the same effect in another language and often create uncomfortable situations. Ask your interpreter prior to speaking engagements to explain topics or terms that can be problematic. Cultural sensitivity is extremely important, but don't let that override the intent of your message.
- ❑ Don't mix living quarters for Category I interpreters with Category II and Category III.
- ❑ Listen to them, they've seen it all before.

words to their community. On the other hand, when treated well, they are more likely to stay longer and talk positively to their friends.

Early on, the Army identifies a need for interpreters and TRW provides. The "pool" begins large when the mission is fresh. As the Army clarifies and increases qualification requirements, the pool of adventurous qualified people in the U.S. decreases. (Demand remains steady or increases—qualification requirements get tougher and supply dwindles.)

TRW reduces the pool by 50 percent during initial screening (U.S.

Citizenship, Medical, and Security Clearance), then lose about 50 percent of the remaining after language testing.

A successful recruiting program is the biggest key to success. Recruiters must understand what the recruits are getting into so as not to mislead them. The unit must understand what recruiters say and promise, then clarify inconsistencies. All must focus on the mission, determining interpreters' strengths for future assignments, while ensuring training methodologies focus on the target audience and understand these are not military recruits.

The next stop is Fort Benning for military issue, force protection training, proper wear and appearance of uniforms and equipment, and "military culture." This is the most useful training to prepare the interpreters for life in a combat zone and Army life, and is critical in formulating expectations for the future.

Reception and Unit Training

Initial impressions of the unit are critical for the unit and interpreters. Clearly explain missions and roles and show the interpreters how they fit into the big picture. From the beginning, incorporate interpreters into your teams just as you do for other new arrivals.

Other than the standard unit welcome brief, complete with camp rules, ensure you provide your unit Mission Brief, standing operating procedures (SOPs), operations security (OPSEC), and force protection concerns. Since intelligence operations are generally in small teams, every team member is critical to team survival. Everyone must understand their role during immediate action drills and become familiar with the team's weapons and equipment. Interpreters may not carry weapons, but if they are willing, it is in everyone's best interest to ensure they could use the weapons if the need arose.^{1,2}

The situation and mission continuously evolve, and we must ensure interpreters maintain the same situational awareness as their team.

Doctrine

While doctrine says little about using interpreters, what is available is right on the mark. The 97E Soldier Training Publication³ provides some basic guidelines:

- ❑ Maintain eye contact with the source, not the interpreter.
- ❑ Answer questions directly rather than "Tell him that"

- Ensure interpreters are present during report writing to answer questions and clarify details.
- Critique the interpreter's performance.
- Teach interpreters specialized vocabulary.
- Explain the mission.

Remember that the interpreters are the only ones who hear the meetings and recordings first hand. If they are not present during report writing and after-action reviews (AARs), you stand a good chance of missing details that could be the key in answering commander's priority intelligence requirements (PIRs). Additionally, critique the interpreter's performance after each meeting. Explain what you need and expect from them or they won't know what they could be doing to make your job easier. Ensure you teach and clarify military jargon. Some words are as unfamiliar to the interpreters as the local culture is to soldiers. Finally, explain the mission to keep interpreters focused on what is important, rather than on the periphery.

Operations

We use interpreters in intelligence organizations to serve in three primary roles: Interpreters for meetings, translations of recorded voice, and document translations. In each of these roles we must take advantage of interpreters' unique talents and make them part of the collection team. The other option is to simply use their linguistic abilities for rote translations. The former keeps the interpreters motivated while increasing mission effectiveness; the later does little for anyone.

Interpreters don't have a military occupational specialty (MOS), so it is incumbent on the unit to assess skills. After assessing skills and matching those skills to the available positions, permanently assign interpreters to a team. While some consider all interpreters as equals with the belief they are interchangeable and therefore can be maintained in

a pool for use by anyone, you will accomplish the mission better with focus and consistency. In a peaceful environment teams learn how to optimize everyone's talents for maximum results. In hostile situations, teams create immediate action drills that could save each other's lives.

While each role brings with it distinct challenges, all share the basic premise that collectors must understand the mission, situation, commander's intent, and PIR.

Meetings. Meetings comprise the biggest variety of Interpreter Missions and encompass the largest percentage of assigned Interpreters. Operations falling into this category include:

- Field HUMINT.
- Interrogations.
- Local Employee Screenings.
- Counterintelligence Investigations.

The common thread through all four categories is the need for interpreter involvement in all aspects of the mission from Orders Brief through AARs.

Another method that worked well in both focusing the interpreters and improving situational awareness was distribution of Information Operations (IO) Talking Points. The Task Force IO Officer worked with the staff and the commanding general to develop the "approved response" on each key or contentious issue within the area of operations (AO) at that time. The talking points explained the issue and gave bulletized responses explaining the message we wanted to pass to the local population. This ranged from how we would clear

snow from the roads, to how we were handling specific troublemakers in the area. In every meeting, the same issues arose and the interpreters knew in advance what answers to prepare to explain even before the team leader told them.

Overall, personnel involved in field human intelligence (HUMINT) operations maintained the best situational awareness and understanding of the mood of the local populace. The interpreters involved in these operations, while working extreme hours, maintained excellent attitudes and were least likely to request transfers or leave earlier than expected.

Electronic Warfare/Recorded

Voice. Collection of voice transmissions is perhaps the most sensitive mission we give our interpreters. This sensitivity is tied to collection capabilities, so ensure you work with the G2 to obtain the proper approvals before initiating any new collection operations. This type of translation is also unnatural for those not trained in military operations or radio procedures. The fact that they can't ask for clarification of missed points or words further complicates the task.

All of these complicating factors significantly increase the importance of pre-briefs and additional training. Teach the interpreters military and radio jargon and ensure they understand what they are listening for. If you don't explain it, there is a good chance when the key nugget that could answer the CG's PIRs comes over the airwaves, they ignore it as unimportant.

LESSONS LEARNED

- Make interpreters part of the team early and keep them involved.
- Rotate interpreters before they burn out.
- Interpreters provide continuity in operations.
- Interpreters aren't interchangeable.
- Finalize clearances quickly.
- Quickly clarify required interpreter qualifications for the contracting agency.
- Develop assessment mechanism early for various duties.
- First impression is important—conduct organized reception.

Document Translations. There is much to be gained from this boring task so remember to work smart. You will accomplish far more if you acquire and use document translation software, distribute the workload, and prioritize the effort when possible. There are several products on the market so do the analysis and determine what software is right for you. The savings in time and effort are well worth the cost. Spread the work throughout the interpreter force but ensure they know what is important to you, and explain what you want. Don't have them waste time on records that are of no value to anyone, and don't have them translate the document into proper English if a literal translation or simply a gist covering the main points is all you need.

Interpreters will burn out after extended periods in any job, and many units choose to rotate them to vary the routine. One special consideration you must remember concerns interpreters working in interrogation operations. These interpreters become known to the prisoners as part of the unfriendly side of the Peace Force. If you rotate these interpreters to a team trying to build trust and confidence in a sector, you stand a chance of creating the exact opposite effect you are trying to achieve. If they are recognized, the entire team loses credibility.

No matter the type of operation, in this environment you cannot accomplish your mission without interpreters. Integrate them quickly into the team and take advantage of their unique skills and knowledge. If you

are the new team falling in on existing interpreters, listen to them. They have the on-ground experience and have seen the mistakes your predecessors made. They also are the ones who gain the best rapport with your contacts and sources. Use this to your advantage. You will find this out whenever you go to a meeting with a new interpreter. The first question will be, "Where is (interpreter's name)?" Not, "How are you today?"

The Future

We know we cannot produce linguists fast enough for mission requirements, and therefore will use interpreters on all future small-scale contingencies (SSCs). We must develop tactics, techniques, and procedures (TTPs)

(Continued on page 74)



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 misty.simpkin@us.army.mil or ernesto.alonso.bolanos@us.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.

Mail to:

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

Please choose method of payment:

Check payable to the **Superintendent of Documents**

GPO Deposit Account No:

MasterCard VISA Discover



Expiration Date _____

Authorization Signature _____

ASAS Contributions to Operation IRAQI FREEDOM

by Michael J. Gaynor
(CW3, U.S. Army, Retired)

"Thanks for the info." That short phrase from a subordinate command was enough justification for me to bring the All-Source Analysis System (ASAS) to Camp Doha, Kuwait.

A lot has been written about the "added value" of ASAS in a fast moving tactical environment, outside the confines of the "perfect intelligence" produced by exercise message traffic. It has been noted the system is hard to learn, not adaptive to commanders' needs, and requires contractor support to perform optimally. While all of these complaints are true in varying degrees, the bottom line is, does the system perform in wartime? My answer to that is an unqualified YES!

The 297th Military Intelligence Battalion, 513th Military Intelligence Brigade, deployed to Kuwait in support of Operation IRAQI FREEDOM. It was integrated into the Coalition Forces Land Component Command (CFLCC) command and control (C2). An essential part of their intelligence architecture was the ASAS suite of systems (All-Source Enclave [ASE]/Remote Workstation [RWS] Single Source/ASAS Lite). Although there were many challenges—in the 297th we have challenges and not problems—the fact that enemy ground order of battle (OB) intelligence was quickly and efficiently passed from higher to lower and lower to higher echelons proves the system is invaluable to the warfighter.

Initially, debate centered on whether the unit should deploy the ASE into theater; the rationale being the ASE is an echelon above corps (EAC) asset and can (should?) be used as sanctuary op-

erations at home garrison. From home, garrison intelligence would be pushed forward into theater from the ASE to the RWS. Since the RWS has a much smaller footprint and can provide a limited correlation capability, this seemed the logical step to take. The unit would not have the numerous concerns of setting the ASE up in theater (space, power, etc.).

Finally, if the ASE remained at home base, there would be no loss of data from the time of deployment until the time the ASE was established in theater. I was one of the proponents of this theory, believing there was nothing we could do in theater that could not be done from garrison. The Joint Analysis Control Element (JACE) Chief disagreed with my assessment. I realize now leaving the ASAS in garrison would have been a mistake. Although the amount of message traffic would not have changed, the benefits of being deployed in theater far outweighed the drawbacks.

First and foremost was analytical focus. There is simply no comparison in an analyst's perspective when there are no distractions. Although family concerns can weigh on a soldier's mind, for the most part, analysts are totally immersed in their job. Also, being 100 km from your adversary's border will sharpen your analysis on assessments and estimates of enemy strengths and capabilities. Additionally, deployed soldiers will naturally crosstrain into disciplines related to, but not necessarily part of, their mission such as targeting and battlefield damage assessment (BDA).

Lastly, response from the intelligence community was incredible. It is hard to believe the same level of timeliness and support would have occurred from sanctuary operations

in the states. I suppose it is only human nature if someone calls and says they are in Kuwait and needs assistance that the person being called will go the extra step than if the person is calling from stateside.

How did ASAS measure up during wartime operations? There were many times when it was very frustrating dealing with all the idiosyncrasies of the system. The ASAS system is not easy to master and is definitely a perishable skill. This is especially true at the EAC level since the tactics, techniques, and procedures (TTPs) differ from those at Corps and Division.

The added value that ASAS brings to any command is the ability to process large volumes of message traffic quickly. The key to making these messages parseable is that they must adhere to the standard United States Message Traffic Format (USMTF). Here is an example of what we experienced in Operation IRAQI FREEDOM.

"I just cannot understand why this information is not portrayed on ASAS!" My fellow ASAS operators and I cringed each time the JACE Chief uttered this phrase. The routine following this phase was predictable. It always started with a long look at the huge map boards showing Iraqi disposition of forces. Although he knew every position by heart, he would look anyway just in case something had changed. After discerning nothing had changed, he would look at the ASAS-generated picture displaying Iraqi units on the Command and Control Personal Computer (C2PC). Finally, he would look back at the message traffic he held in his hand. Two of the three almost always matched; what didn't match was the assessment of Iraqi

forces in the document he was holding. Unfortunately, the result was also predictable. Next, he would come to me and ask why this report wasn't portrayed on the map. My answer was always the same: "Sir, we never got this report, it's free text." He would mutter something under his breath and talk with the Production Chief to evaluate the information and change the Iraqi dispositions accordingly. He would glance at the ASAS section and wonder again how to better perform ASAS operations at the EAC level.

Although not an everyday occurrence, it happened often enough to make the ASAS analysts wonder what they could do to solve this challenge. The solution seemed simple: since ASAS will accept any USMTF-compliant message, just have the message originator comply with USMTF. The vast majority of messages received were Intelligence Information Reports (IIR) which comply with USMTF standards. Another form of IIR is the Intelligence Periodic Information Report (IPIR); this report is written in free text. The challenge lies in the fact that it is easier and faster for analysts to write a written free-text report (IPIR) than to put the information into a parseable message format (IIR) used primarily by ASAS analysts.

The rest of the intelligence world, along with sister services, prefer the free-text version. A free-text message is easier to read and analysts don't have to search the message for the information they need. Thus, intelligence producers state they are merely responding to the needs and wants of the majority of their customers. So, we have a dilemma. How can the National Agencies satisfy both the need for quick real-time intelligence dissemination and still meet the requirement to provide this same information in a parseable format for ASAS? There are simply not enough assets to do both reports. Additionally, even if additional assets were available, the confusion caused

by duplicate reporting would likely have a negative rather than positive effect.

This challenge became more and more apparent the closer we came to war, and shortly after the war started the percentage of free-text reporting jumped dramatically. Up to 30 to 35 percent of the reporting was coming in free text once hostilities commenced. As always, soldiers complain, get angry, and then adapt. The work-around was to use one ASE node solely dedicated to processing free-text messages. There was a manpower element as well. We dedicated one analyst each shift to ensure we were getting the appropriate traffic, deciding if the message was worth converting into a parseable message, then hand-typing the message into the ASE so it would parse into the database. Although not the ideal solution, it worked. As you may have guessed, time was the most critical element. Fortunately, we had the ability to dedicate a node and the manpower for free-text processing; this luxury does not exist at lower echelons.

Although this solution worked in Operation IRAQI FREEDOM, I suspect if the war had lasted longer we would have run into major difficulties. Additionally, this war consisted of a largely static enemy environment; if the battlefield had been more dynamic the additional time spent processing free-text messages would certainly have delayed timely intelligence dissemination to higher, lower, and adjacent units. The sheer volume of parseable message traffic was enough to keep all of our analysts busy. Adding the processing of free-text messages is not only manpower intensive but also because this position involved deciding which free-text message was worth processing, it had to be manned by a senior analyst.

What needs to happen is a command-driven directive to either convince the National Agencies to

conform to the USMTF standards, or accept that ASAS top-down intelligence information may not contain all intelligence information. Automatic free-text message parsing is not in the foreseeable future. Although a limited ability exists with keyword search programs, again you are at the mercy of the report writer to put in the correct word or phrase.

There are also many things the ASAS system did well during Operation IRAQI FREEDOM. These included data sharing (both top down and bottom up), delegated production, and adaptability. Data sharing from the bottom is a concept not often utilized during exercises. Attempting to incorporate the Marine system into the architecture made the task even more challenging. In the information age in which we now live, the timely passing of intelligence data is critical to commanders in order to effectively and efficiently place their assets. During Operation IRAQI FREEDOM data sharing between echelons using ASAS systems, with few exceptions, worked very well.

In the final analysis it boils down to did the system provide the commander with accurate OB information in a timely manner. On numerous occasions, both higher and lower echelon units stated the intelligence provided by the ASE was invaluable to their mission planning. As the link between the National Agencies and the Corps, the 513th Military Intelligence Brigade is often called upon to "make the call" regarding enemy intentions and capabilities. The ASAS family of systems was an integral part of providing the CFLCC Production Section the capability to do just that.

In closing, to the best of my knowledge this is the first time the ASE had a relevant and active role in combat operations. Although there will always be exceptions, intelligence

(Continued on page 80)

Software Engineering Center's Support to CENTCOM

by Don Adamson

The U.S. Army Communications-Electronics Command (CECOM) Software Engineering Center (SEC) completed the implementation of Modernized Integrated Database (MIDB) Replication of the All Source Analysis System-All Source (ASAS-AS) Conditional Version Release AS3.4.1. This effort provides the capability for ASAS-AS to interoperate with the Global Command and Control System-Integrated Imagery and Intelligence (GCCS-I³).

The Analysis and Control Element (ACE) at echelons above corps (EAC) require a near-real-time (NRT) replication capability to export the tactical enemy ground picture to both theater and national levels. This capability was initially scheduled for completion by June 2003, but was accelerated for fielding by mid-February 2003. The Central Command (CENTCOM) area of responsibility

(AOR) was the first to implement this capability.

To expedite the installation and training of AS3.4.1, experienced ASAS-AS software engineers deployed to Camp Doha, Kuwait, to provide support to the 513th Military Intelligence (MI) Brigade (Bde). The objective was to provide experienced, onsite support with in-depth software knowledge. The installation and training of the AS3.4.1 software and data server (DS) hardware were completed on schedule and within CENTCOM's required two-week period. The onsite engineer worked with ASAS-AS software engineers located at the CECOM SEC Depot at Fort Huachuca, AZ, via the Joint Worldwide Intelligence Communications System (JWICS) to resolve any issues that occurred. This coordination enabled support to be provided expeditiously and effectively.

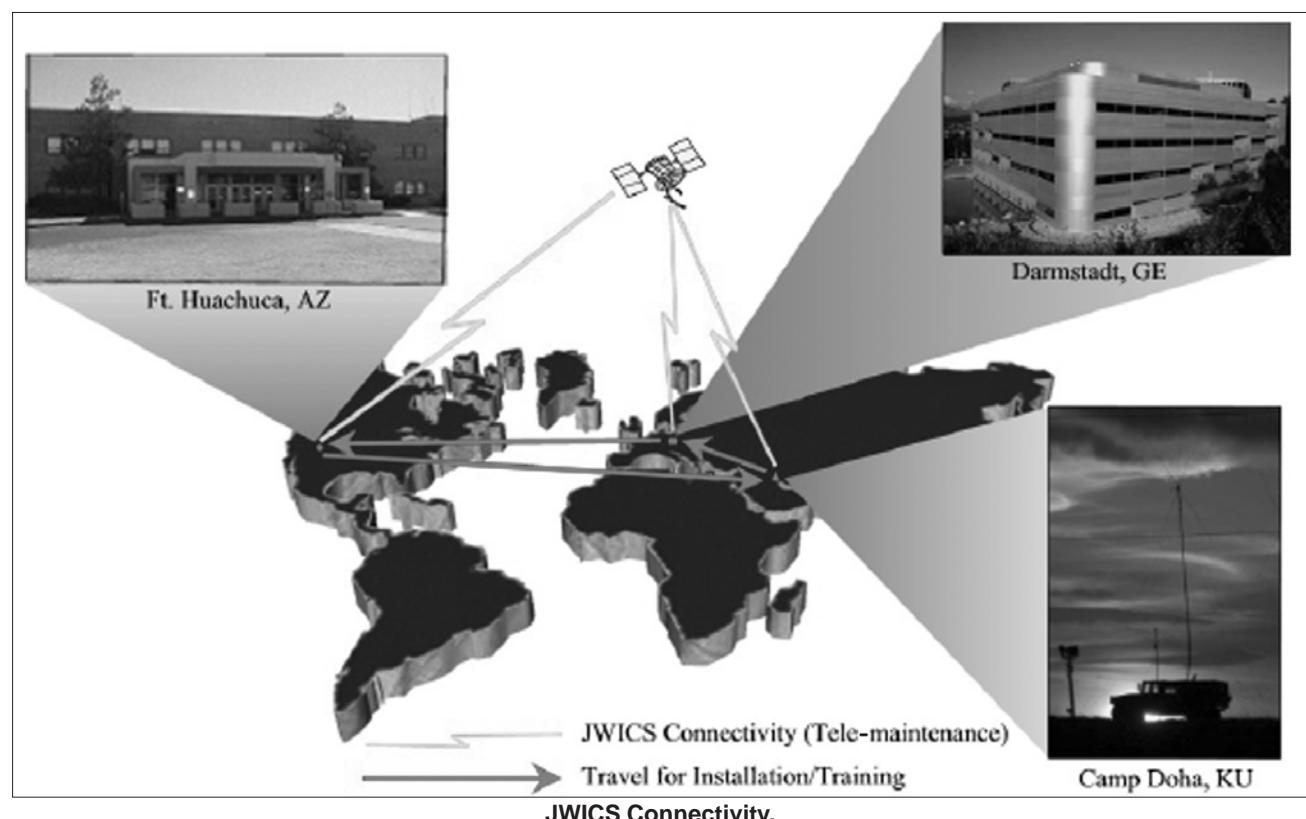
Once installation and training of the AS3.4.1 were completed in

CENTCOM's AOR, the Department of the Army (DA) selected a second site for fielding. At the end of February, the ASAS-AS software engineers were sent to the 66th MI Group (GP) at Darmstadt, GE. Installation of the new software and training were provided for the unit's ASAS-AS analysts, European Regional Software Support Activity (RSSA), and onsite Tactical Automation Support (TAS) Field Support Engineers (FSEs).

At this time, ASAS-AS and DS systems are operational at both sites and ASAS-AS software engineers at Fort Huachuca continue to provide tele-maintenance support as required. This new capability provides a greater view of the battlefield to the warfighter located at the theater level units.



Mr. Don Adamson can be reached via E-mail at Don.Adamson@us.army.mil and by telephone at (520) 538-1849 or DSN 879-1849.



Lessons Learned: A Ground Surveillance System Platoon in Afghanistan

by 1LT Jacqueline L. Dominguez

This article will discuss nine (ten would have been too normal) of our hardest lessons learned while being deployed to Kandahar Airfield (KAF), Afghanistan. Our platoon relationship while deployed was mainly direct support to the infantry battalion responsible for the perimeter defense. Throughout the deployment we worked with six various infantry battalions that included Canadians and Marines. The battalions rotated every three to four weeks; that made liaison and operation a continual battle. It was definitely an experience that will be cherished and remembered by every member of the platoon.

Our first priority was to replace the Marine's ground sensors. We worked hand in hand with them for about seven days prior to taking command and control of the perimeter defense. They had only one string of sensors emplaced to the north in a mountain pass that led to Kandahar City. Problem was many nomadic and village people used the pass to travel back and forth from the city and other villages. Movement in the pass increased as the weather got warmer, and this sensor string proved to be inefficient.

We ended up taking a new approach. We worked with the infantry battalion that secured the perimeter and asked them where the dead spaces were from their fox-holes. There were several areas in the north inside streambeds, areas to the west around the karez system, and south in an orchard (see diagram) that could not be observed. These were also identified as av-

enues of approach and named areas of interest (NAIs) by the brigade and battalion that we quickly volunteered to cover.

Early on, end of January early February, we discovered a regular dismounted reconnaissance of KAF was being conducted with our remotely monitored battlefield sensor system (REMBASS) sensors. They would conceal their movement using the karez system to the west. The karez systems are underground aqua ducts that look like giant anthills, some stand as tall as eight feet high. We had identified these as possible dismounted avenues of approach in mid-January. We emplaced our REMBASS sensors and identified these unwanted intruders every attempt they made to get close to the airfield. After being run off by our quick reaction force (QRF) three times, they eventually stayed away.

In March we had a REMBASS sensor activation in a streambed north, northeast of KAF. There was an Apache in the air that quickly rerouted to this location. The Apache identified a single dismount dressed all in black. Once noticed, the dismounted intruder fled to a nearby Afghani Military Forces (AMF) location.¹ Once QRF ground troops and AMF commanders arrived, there was no one dressed all in black, and they all denied the incident took place. A full search of the observation post (OP) revealed two RPO-A Schnell flamethrowers that their commanders did not authorize them to have. There was definitely something wrong at this OP that was quickly and severely corrected by the AMF commanders. Since then, no one else attempted to penetrate our barrier of protection.

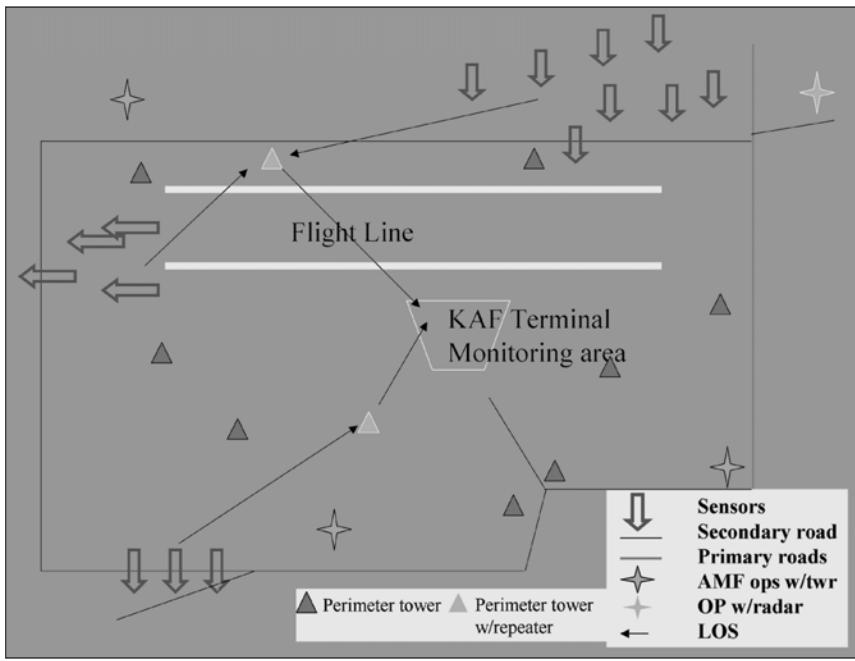
The Ground Surveillance Systems (GSS) platoon (a measurement and signature intelligence [MASINT] collector) has been our extended "feelers" of the KAF perimeter. We can identify any movement coming at us from the north and northeast with our AN/PPS-5B radar. We track our friendly convoys and watch their flanks for any suspicious movement that may be a threat. We are also looking for any dismounts that may emplace along the aircrafts ingress/egress routes. This area (due to its proximity to the ingress/egress routes) is one of the brigade's primary NAIs. It is possible for a high-value target to set up in this area and be able to shoot down an aircraft.

The GSS platoon has ultimately set up a three-kilometer protective ring around the perimeter (in some areas it extends out to six kilometers). With all of the success stories there were also some lessons learned that other GSS operators and leaders might find of particular interest.

Lessons Learned

- 1. Contrary to popular belief GSS Operators (96Rs) are not engineers, even though we seem to find all the mines.**

Due to the vast amount of defensive and reconstructive work that needed to be done on KAF, Afghanistan, engineers were a precious commodity! So as everyone in the Military Intelligence community knows, the last element to get support is Military Intelligence (although it is our job to identify threat prior to its getting to the defensive perimeter). At Fort Campbell, Kentucky, the infantry invited us to some very realistic live environment training on



Kandahar Airfield GSS Operations.

improvised explosive devices and mines. Many of our missions were conducted with only a squad of infantry security, so the training paid off. We knew what to look for and watched every trail carefully. Fortunately, most of the unmarked mines near the airfield are surface laid and were easily visible during our daylight reconnaissance. The mine classes were of great value not only in saving lives but also in intelligence gathering. Our soldiers that had the training could identify the kind of mine or unexploded ordnance for S2 debrief.

Many of the mined areas were marked using rock piles and red painted rocks. You could distinctly tell the rocks were piled into a pyramid. If they were white or no paint, the rocks marked a cleared route as long as you traveled between them. Red painted rocks signified a minefield. Some areas had larger rocks that were painted red on one side signifying a mined area and white on the other signifying the non-mined area.

Other areas immediately around the airfield were not marked. This was because the normal run-of-the-mill civilian population never ventured near

it for about twenty years. In the early 1980's when the Russians occupied KAF they would shoot and ask questions later. The environment created by the al-Qaida and Taliban closely resembled the aforementioned treatment of the civilian populace.

In conclusion to our number 1 lesson learned, I would like to encourage everyone to become smart on

mine awareness. National Ground Intelligence Center has a very good compact disc you can request.² Most of the countries we consider primary threats have an extremely high volume of minefields, and if you plan on spending any time in the military, you will probably find yourself in one of those threat areas.

2. You must beg, borrow, and steal frequencies so your equipment will work.

This is extremely important when working on an airfield. All aviation and the unsecure hand-held radios work on the same frequencies as the sensors and repeaters.

In an attempt to deconflict, we went to the frequency management meeting two weeks after we took command and control of the airfield. Everything was working splendidly for the first month, then some new units started showing up. We began to get a lot of interference on all of our channels so we had to go to the brigade signals shop. The frequency manager left so the brigade signals noncommissioned officer in charge, MSG Collins, took charge and resolved the multiple use of single fre-



GSS Platoon (6th Platoon, D Co 311th MI BN 101st ABN) from left to right:
2LT Dominguez, SGT Forsythe, CPL Balance, SPC Quigg, SPC Brewster,
CPL Cervantes, PFC Emmert, SGT Deter. (Those not shown: SGT Sealy,
CPL Taylor, SPC Johnson, SPC Pike). Taken April 2002 Kandahar.

Photos courtesy of the author.

quencies. Within a week our interference problem was resolved but I am unsure what will happen when the next group of new units begin to flow in.

3. Ensure you learn about all other MASINT equipment, to include coalition, around your area so you are not duplicating effort.

Originally, we had the radar site in the west and a Canadian Coyote was collocated but, not having a good understanding of their capabilities, I thought nothing of it. I eventually asked the Canadian S2 representative about it and he informed me that the Coyotes have the same capability as our radar, plus five kilometers. We then found a new site on the opposite side of the runway and completely off the airfield to avoid duplicating effort.

Additionally, four months into the deployment, a Marine Radar arrived and set up in generally the same direction we had moved to. Nervous we were going to get beaten out on coverage again because of our late-model equipment, we found out that they were looking for aircraft. Their radar was operating in a scan-up-and-out in a complete circle versus our radar's ground level, omnidirectional scan. This was a relief, and we still had a mission!

4. Always anchor your REMBASS sensors no matter how many years of drought the area you are operating in has had.

Afghanistan has had seven years of drought but once we got our sensors in the ground it started to rain. We had anchored the sensors that we put into the streambeds but because it hadn't rained in so long the streambeds were extremely shallow. To anchor the sensors we made a mud mixture around them, allowed the mixture to dry, and that resulted in a cement-like anchor. The amount of rain we received overflowed and deepened the streambeds, sweeping some of our anchored sensors away. We also found that surface-



Crew preparing for a Radar mission at the AMF outpost.

laid mines had shifted. This was particularly important going out to service the sensors.

When going out to service them, while the runoff was still flowing, we sunk an M1114 (an up-armored high mobility multipurpose wheeled vehicle). Like I mentioned before, the intensity of the rains made the streambeds deeper than they had been initially. While attempting to cross an originally four-feet deep streambed, our truck with driver and equipment became submerged into an eight-feet deep stream. Words of wisdom for others: always check the depth of water prior to making a crossing.

5. Explain your systems to the infantry, engineers, and EOD personnel with whom you will be working; it makes your job a lot easier.

Once in country we realized that with the increased risk of improvised explosive devices and mines that our systems, if compromised, may be targeted as. Many of the infantry, engineers, and explosive ordnance disposal (EOD) personnel know what we do, they just don't know how. Plus they haven't seen the equipment and if they have, they have not seen it employed. So we set up some live environment training of our own. We trained fifty infantry personnel, four explosive ordnance disposal

(EOD) technicians, and seven engineers on our equipment purpose and employment. This was in hopes that when on their missions and they came across it, they would not mistake it for a threat device and destroy it. Now five months into the deployment, one month to go, we have had no such incidents.

6. Unfortunately, maps are not always correct and that means the LOS studies created from them are incorrect too.

From the beginning, maps were an ongoing issue in Afghanistan. The last known survey of the area was from the 1980's when we helped the Mujahideen defeat the Russians. Since then, new buildings were constructed and with the way the wind blows around there a sand dune can travel approximately one- to five-kilometers a day. The only way to get accurate line of sight (LOS) is to get out on the terrain. This proved to be a tedious task. All convoys were required to have up-armored lead-and-trail vehicles. Eventually after ten mine incidents in four months all vehicles leaving the KAF perimeter were required to be up-armored. Only the brigade commander could sign off on an exception to policy for light-skinned vehicles to leave the gate. As a result, it required extensive coordination with infantry compa-

nies having tube-launched, optically tracked, wire-guided (TOW) gun trucks, military police, Canadians, and anyone else having a fleet of up-armored vehicles. Eventually things came together with the LOS when the perimeter towers were completed. They were the optimal place to set our sensor repeaters. We set one in the north and one in the south to complete the LOS we needed to monitor. The radar was a little more of a challenge, but it worked out fine on a rooftop of an existing building we occupied with a squad of infantry and some AMF.

7. Do not be forced to turn in batteries prior to deployment; bring them with you at all costs.

The Air Force has many requirements and restrictions that are a real hassle. Batteries were a main concern because they were considered hazardous material. The company decided the paperwork hassle was too great and decided to turn in the batteries to the logistical unit that was deploying with us. We were to get them back in theater but because we have special types of batteries (BA-5598 and BA-5557) for our equipment and a special request for them was not done, they never made it to Afghanistan. We had put off a battery change for fifty-three days. We normally change them every thirty days. (According to doctrine the batteries will last thirty days with one thousand activations per day.) We hadn't gotten more than five activations per day but counting on the batteries to twice the allotted time was pushing it. If at all possible, do the hazardous material paperwork and put more batteries on order immediately arriving in theater to eliminate this problem.

8. Bring all accessory items for your equipment.

Low-and-behold, war is nothing like a three-week rotation at the Joint Readiness or National Training Centers. While preparing for deployment

the platoon was led to believe that they would be in hide sites, remote from any base operations. Completely the opposite was true. We were an intricate part of base perimeter security. We needed our fifty- and one-hundred-feet cables to remote the radars. A couple more repeaters for the sensor systems wouldn't have hurt either. The platoon also conducted company and platoon changes of command. All the technical manuals and a detailed handreceipt of items in the rear would have been of great help. Always be prepared for the worst or unexpected. When deploying to far-off lands for more than three to six weeks, shove a couple of extra sensors, repeaters, monitor cables, technical manuals, and radar CI cables in the storage container. Even if you never use them, you know you have an extra onhand in case you need it.

9. Emplace sensors in rough terrain (train with diversity); that is, hard rocky ground.

Afghanistan terrain is rocky and hard. Although a desert, the surface is not sand. It is a sand-clay mixture that after it has rained, then allowed to dry, becomes almost cement like. We mainly used a post-hole digger and pike to break up the earth prior to digging with an e-tool or shovel. Another issue was the multiple deposits of iron ore in the soil. This made the magnetic sensors difficult to use. It was an excellent environment for the seismic acoustic and infrared passive sensors once you could get them into the ground. Camouflage was another issue. We mainly trained for the green grassy landscape found at beloved Fort Polk, LA. Prior to coming to this area, paint your sensors sand color except for a few. There are areas here that have greenery and the tall grass or shrubs could provide the threat with concealment. Remember to be innovative with your training because things aren't always as they seem.

Conclusion

I would just like to remind soldiers deploying into an environment like Operation ENDURING FREEDOM that it is nothing like the Joint Readiness or National Training Centers rotations. Be prepared for the worst and a variety of experiences. In addition, it is for the long haul—not just three or four weeks. You will be there for at least six months, having to maintain equipment and readiness. I hope this synopsis has familiarized you with some of the things we did and major issues the GSS platoon has run into while serving in Operation ENDURING FREEDOM at Kandahar Airfield, Afghanistan.

First Lieutenant Jacqueline L. Dominguez was deployed in January 2002 to Afghanistan for eight months in support of OEF. She is currently the Rear Detachment Commander (F Co Prov) for 311th MI Bn, Ft Campbell, KY. Her career in the U.S. Army began as a PFC. She attended DLI (Persian Farsi) at Monterey, CA; Cryptological Linguist Tactical Exploitation Equipment Course at Ft Devens, MA; participated in the 1997 Partnership for Peace rotation; and was awarded a 2-year Green to Gold Scholarship to the University of Wisconsin, La Crosse, and received the Superior Cadet Award (1998-1999). She graduated with Honors with a Baccalaureate degree in Psychology in May 2000; graduated in March 2001 from MIOBC at Ft Huachuca, AZ. 1LT Dominguez participated in several Joint Operations in support of Southern Command, Haiti, and JRTC rotations. Previous assignments include 98G AIT at San Angelo AFB, TX; C Company 519th MI Bn, 525 MI Bde, Ft Bragg, NC; TLQ-17/TRQ-32 Squad Leader and Battalion Training NCO; Electronic Warfare Platoon Sergeant for 2d Armored Cavalry Regiment, 502d MI Co, Ft Polk, LA; Assistant 3d Bde, 187th Infantry, 101st Abn Div S2, Ft Campbell, KY. 1LT Dominguez is married with two children. Readers may contact the author via E-mail at jackie.l.dominguez@us.army.mil and by telephone at (931) 798-3505.



Endnote

1. AMF are friendly native militia forces helping us defend the airfield OP.
2. Mine Facts and Landmines and DEMINING, Global Problem, Global Solutions (CD and reference material), Commander, National Ground Intelligence Center, ATTN: Tom Reeder, 220 7th Street, NE, Charlottesville, VA 22902, Fax (804) 980-7699.

Al-Qaeda Wave Attack Assessment

by Ben N. Venzke

*Copyright 2003 IntelCenter/
Tempest Publishing, LLC, All
Rights Reserved—Permission to
redistribute this report in its
complete form, including this
notice, with proper attribution to
IntelCenter ([http://
www.intelcenter.com](http://www.intelcenter.com)) may be
obtained by emailing
info@intelcenter.com. Permission
must be obtained in writing before
redistributing the entire report or
any portion of it.*

ASSESSMENT

Al-Qaeda no longer believes that single, large-scale attacks not employing CBRN (chemical, biological, radiological, nuclear) have enough of an impact for its core series of operations. Consequently, al-Qaeda and its affiliates are actively pursuing a strategy of "wave attacks" designed to hit multiple targets and target classes around the world using a variety of tactics over the course of concentrated 7-9 week periods. The recent attacks in Chechnya, Riyadh and Casablanca point to the beginning of the second such wave of attacks. Additional small and large-scale attacks can be expected around the world during the next 6-8 weeks.

INTRODUCTION

Conventional thinking on al-Qaeda has always led us to believe that the group would typically attempt to execute one major operation per year. Al-Qaeda successfully managed to do so every year since 1998, with the exception of 2000 when its attempts were foiled. While there were times during this period when it can be concluded al-Qaeda would have executed more than one operation if it had been able to, there appears to be no point where the group attempted to conduct a wave of small

and large attacks during a concentrated period.

Security postures and assessments routinely reflect the very real threat posed by sympathizers and individual actors executing attacks in the immediate aftermath of a major al-Qaeda operation. The potential, however, that al-Qaeda would conduct multiple, large-scale operations within days or weeks of each other seemed unlikely.

The events of the fall of 2002 and the spring of 2003 appear to indicate a shift in thinking by al-Qaeda and its affiliates. The period running from 6 October 2002 to 28 November 2002 marked the highest concentrated period ever of successfully executed large and small-scale operations by al-Qaeda and its affiliates. Rather than ride out the "afterglow" period following the Limburg operation, al-Qaeda and its affiliates continued to strike.

The events of the past five days indicate the beginning of a similar trend. No fewer than four significant attacks have been executed in Chechnya, Riyadh, Saudi Arabia and Casablanca, Morocco. Additional small and large-scale attacks can be expected around the world during the next 6-8 weeks.

AL-QAEDA'S THINKING

Al-Qaeda has always sought to execute operations on a scale and in a manner never before seen. This approach, while increasing the difficulty, has put al-Qaeda on the map like no other terrorist group before it. Al-Qaeda feels that this position is of importance to achieving its objectives and continues to evolve its operational thinking in order to maintain this status.

It is al-Qaeda's great attention to operational security, training and the development of an extensive global

network that has allowed it to execute these types of operations around the world. While recognizing its past successes, it is not the type of organization to grow complacent and let itself fall into an operational rut where it simply repeats what worked before. Al-Qaeda continually pushes the envelope on what is possible and evolves its thinking even when succeeding. Threat assessments and security measures cannot simply rely on what al-Qaeda did before.

The "wave attack" concept appears to be a natural evolution of what al-Qaeda feels is necessary to ensure the impact of its strikes.

TARGETS

The targets of the wave of attacks, which occurred in the fall of 2002, spanned the full spectrum from civilian to government to corporate. The overall targeting theme at that time fit with al-Qaeda's focus on striking US allies.

The recent attacks of the past five days were primarily directed at civilian targets with a Western or Jewish connection. There is no reason that additional attacks in the same series will necessarily remain focused on civilian sites. Recent al-Qaeda messaging does strongly point to al-Qaeda's desire to strike targets in Arab countries seen as betraying al-Qaeda and its objectives. The attacks in Saudi Arabia and Morocco bear this out. Future strikes in Arab states are highly likely but attacks could occur anywhere, including in the US and Europe.

TACTICS

Al-Qaeda has already laid out the religious justifications necessary for its use of chemical, biological and nuclear weapons. It has dedicated extensive resources towards the procurement, development and

planning for future use of these weapons, as well as expressed its intent to utilize them. When al-Qaeda feels it is ready to do so, it is highly likely it will. In the meantime, we can expect to see traditional terrorist tactics, such as suicide bombings, vehicular bombings and hijackings, employed in ways never before seen and with great effect for its core series of operations.

During the wave of attacks seen last fall, al-Qaeda did not constrain its operations to only large-scale attacks but rather mixed both. While employing surface-to-air missiles (SAMs), a waterborne improvised explosive device (IED) and other sophisticated operational techniques, the group also made use of simple low-level shootings. If we are currently experiencing another wave of attacks by al-Qaeda and its affiliates, we can expect to see the same blend of both sophisticated and low-level strikes.

FALL 2002

During the eight-week period between 6 October 2002 to 28 November 2002, al-Qaeda and its affiliates executed no fewer than six significant attacks. The strikes spanned six countries and included civilian, military and commercial targets. The longest period between the attacks was 27 days and the shortest was one day. Al-Qaeda made direct claims of responsibility for three of the operations. A listing of the attacks is below.

- ❑ 6 October 2002: Piloted Vehicular Assault—The Limburg (French oil tanker)—Mukalla, Yemen—al-Qaeda claimed responsibility.
- ❑ 8 October 2002: Shooting—US Marines—Failaka, Kuwait—al-Qaeda claimed responsibility.
- ❑ 12 October 2002: Vehicular Bombing—Sari and Paddy's nightclubs—Bali, Indonesia.
- ❑ 24 October 2002: Hostage Taking—Theater—Moscow, Russia.

- ❑ 28 October 2002: Assassination, Shooting—Lawrence Foley (US Executive with USAID)—Amman, Jordan.
- ❑ 28 November 2002: Surface-to-Air Missile (SAM) Attack—Israeli Arkia Flight 582—Mombasa, Kenya.
- ❑ 28 November 2002: Vehicular, Suicide Bombing—Kikambala Paradise Hotel (Israeli-owned)—Mombasa, Kenya.

SPRING 2003

During the four days between 12 May 2003 to 16 May 2003, al-Qaeda and its affiliates conducted four significant operations. The strikes spanned three countries and included civilian, government and commercial targets. The longest period between attacks was one day. A listing of the attacks is below.

- ❑ 12 May 2003: Vehicular, Suicide Bombing—Chechen Nadterechnyy District administration building—Znamenskoye, Chechnya.
- ❑ 13 May 2003: Vehicular, Suicide Bombing—Jedawal Compound—Riyadh, Saudi Arabia—al-Qaeda claimed responsibility.
- ❑ 13 May 2003: Vehicular Bombing—al-Hamra Compound—Riyadh, Saudi Arabia—al-Qaeda claimed responsibility.
- ❑ 13 May 2003: Vehicular, Suicide Bombing—Cordoval Compound—Riyadh, Saudi Arabia—al-Qaeda claimed responsibility.
- ❑ 13 May 2003: Bombing—Saudi Maintenance Company (Siyanco)—Riyadh, Saudi Arabia.
- ❑ 14 May 2003: Assassination, Suicide Bombing—Chechen Administration leader Akhmad Kadyrov—Ilyiskhan-Yurt, Chechnya.
- ❑ 16 May 2003: Suicide Bombing—Restaurant (Israeli ownership)—Casablanca, Morocco.
- ❑ 16 May 2003: Suicide Bombing—Spain House (Spanish social club/restaurant)—Casablanca, Morocco.
- ❑ 16 May 2003: Suicide Bombing/Vehicular Bombing (uncon-

firmed)—Israeli Alliance Circle Club—Casablanca, Morocco.

- ❑ 16 May 2003: Suicide Bombing—Farah Maghreb Hotel—Casablanca, Morocco.
- ❑ 16 May 2003: Suicide Bombing—Jewish Cemetery—Casablanca, Morocco.



Ben Venzke is the founder and CEO of IntelCenter which provides intelligence support to the intelligence, law enforcement, military and security communities. He has been working for the past 14 years to create professional-level intelligence products that place timely, actionable intelligence into the hands of those who need it, whether it is an operator prepping to perform an entry, an analyst sitting at Langley, or a chief of police attempting to assess the threat to his or her city. Mr. Venzke has recently co-authored "The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics & Targets," which has provided readers for the first time in a publicly available format the ability to see what al-Qaeda has said in its own words about targets and tactics. Counterterrorism mission has been his core focus for the past eight years. While running IntelCenter and its sister company Tempest Publishing, Mr. Venzke has managed intelligence products at Jane's Information Group where he worked as an Editor and iDEFENSE where he was the Director of Intelligence Special Projects. He also spent two years as Pinkerton Global Intelligence Service's senior consultant for the Middle East and Africa. He can frequently be seen appearing on CNN, MSNBC, and NBC. Readers may contact Mr. Venzke via E-mail at bvenzke@intelcenter.com.

Reminder: MIPB Mailing Address

Due to a recent reorganization and in accordance with the Official Mail Address Standards, **Military Intelligence Professional Bulletin**'s new address is:

ATTN: ATZS-FDT-M
US Army Intelligence Center
and Fort Huachuca
550 Cibeque Street
Fort Huachuca AZ 85613-7017

Lessons Learned: Army National Guard G2X in Bosnia

by Major Lee Lacy

American author Robert M. Pirsig wrote:

Traditional scientific method has always been at the very best 20-20 hindsight. It's good for seeing where you've been. It's good for testing the truth of what you think you know, but it can't tell you where you ought to go.¹

With the benefit of hindsight much can be written about the G2X experience in Bosnia-Herzegovina since the insertion of North Atlantic Treaty Organization (NATO) peace implementation and stabilization forces in December 1995. The experience of an Army National Guard (ARNG) G2X is worth telling because of the likelihood of similar missions in the future for the Reserve Components (RC). The Stabilization Force (SFOR) peacekeeping operation (PKO) began its transition to the RC with SFOR 9 in 2000². SFOR 9 was a mix of Active Component (AC) and RC soldiers. In 2002, the SFOR mission became primarily an RC operation with SFOR 12. SFOR 13 continued that tradition and is comprised mostly of ARNG and U.S. Army Reserve (USAR) units from 18 different states.

With such a diverse mix, the challenges of mobilization, training, and executing the operation were many. Counterintelligence (CI) and Human

Intelligence (HUMINT) operational assets are not organic to the ARNG division. The G2X staff function exists in only a few AC divisions, and is non-existent in the ARNG. Although the challenges were great, they were not insurmountable. The events surrounding the 35th Infantry Division (Mechanized) activation for SFOR 13 is a good example of the cooperation and partnership of the AC and the RC. Hopefully, others in the RC, destined to follow as peacekeepers, will learn from the SFOR 13 experience.

The G2X is the single focal point for all matters associated with CI and HUMINT in the area of operations (AO); and is the CI and HUMINT advisor to the Senior Intelligence Officer (SIO) Military Intelligence (MI) Task Force Commander and the Commanding General³. The G2X concept evolved from the Army's experiences in Somalia, Haiti, and the Balkans. The need to concentrate CI and HUMINT activities under one staff officer was initiated in order to exercise technical control and to leverage CI and HUMINT assets operating in the AO⁴. SFOR 13 is organized as illustrated in Figure 1.

- ❑ The G2X is a 35E CI field grade officer.
- ❑ The Task Force CI Coordinating Authority (TFCICA) is a 35E company grade officer with respon-

sibility for directing and synchronizing CI activities, as well as deconflicting source operations.

- ❑ A Tactical HUMINT Operations (THOPS) section is organized to provide technical control and oversight of Tactical HUMINT Team (THT) operations on behalf of the G2X. THOPS is led by a 35E company grade officer and is staffed with various enlisted intelligence specialties. THOPS oversees six THTs, comprised of four collectors each, and a four-man security force.
- ❑ THTs are led by 35D tactical intelligence company grade officers and supported by a mix of 97B CI Agents, 97E HUMINT Collectors, and 97L Linguists. Two U.S. national civilian contract Category II linguists augment each team. For ease of operation, each THT is split in two to maximize efforts in their assigned sectors. One team is task organized for CI investigations for the brigade AO. It consists of one 35E company grade officer and two 97B noncommissioned officers (NCOs).
- ❑ The HUMINT Analysis Requirements Cell (HARC) is an entity inside the Task Force Analysis Control Element (ACE) for the purpose of analyzing THT reporting. The HARC, with G2X approval, publishes a HUMINT

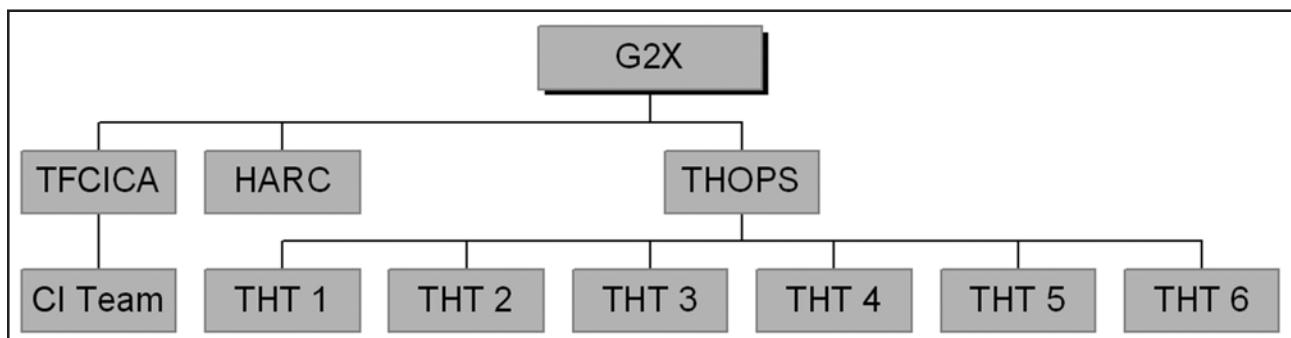


Figure 1. Task Force Eagle G2X Organization for SFOR 13.

Collection Focus based on the Commander's priority intelligence requirements (PIRs). The HARC is led by a 351B CI chief warrant officer and staffed with four enlisted 97B CI agents.

The Deputy G2X at Task Force Eagle is a long-term employed civilian contractor, with CI and/or HUMINT experience. This contractor provides the continuity between units that perform six-month rotations. The Reports NCO is a 96B Intelligence Analyst who handles many of the section's administrative functions. The Reports NCO primarily edits THT reporting prior to releasing to intelligence consumers.⁵

Pre-mobilization activities presented our greatest challenge of the entire mission. Initially, the 142d MI Battalion (Bn) (Linguist), Utah Army National Guard, was alerted for training. A last-minute change in June 2002 resulted in the selection of the 260th MI Bn (Linguist), Florida Army National Guard, instead. The greatest concern was whether the 260th MI Bn could be integrated quickly enough into the training cycle to prepare for the mission. This short suspense, along with commitments to Operation ENDURING FREEDOM, put the 260th MI Bn in a personnel and time crunch. Fortunately, they were able to provide adequate support to the command post exercises (CPXs).

PKO was uncharted territory for both the 35 ID (M) and the 260th MI Bn. The challenge was how to stand up a CI and HUMINT operation in short time, with so few qualified individuals and little resources. Of the 51 personnel from the 260th MI Bn selected for SFOR, only 2 had experience in PKO. We determined the Balkans theater would require specialized skills in the area of CI Force Protection Source Operations (CFSO). The challenge was how to get key personnel funded and scheduled for the six-week course at Fort Huachuca, Arizona.

After mobilization, and as training progressed, we discovered how valuable it was for the TFCICA to attend CFSO training. CFSO training gives the doctrinal background and tactics, techniques, and procedures (TTPs) to conduct overt low-level source operations. Our only regret was the inability to have all THT leaders complete the course. CFSO is worthwhile. We recommend the Army expand the course and consider establishing a mobile training team (MTT) to provide the training materials, support, and oversight for RC units to train CFSO. The MTT is ideal for RC units with limited time and resources. The lack of formal or informal G2X training during our pre-mobilization was a disappointing experience. During the numerous home-station training events leading up to mobilization, not once did we find subject matter experts (SMEs) to teach any of our key leaders, such as the G2X, TFCICA, THOPS Chief, or the HARC Chief. We often found mentors from supporting AC units with some CI and HUMINT knowledge, but we never had the experience of working with an SME until many months down the road.

During the initial train-up period, as we analyzed the required organization, new doctrine, and published standing operating procedures (SOPs), the benefit of an SME with recent Balkans G2X experience to guide us would have paid big rewards in collapsing our learning curve.

Pre-mobilization training included four months of weekend inactive duty training and three CPXs, each lasting one week. During this time the G2X organization operated response cells in the ACE and participated in the training scenarios. Unfortunately, CPX training did not capture the reality of CI and HUMINT operations in the Balkans theater.

Suggested improvements to home station training include adding role players to simulate source operations and CI investigations. The

HUMINT collector source meetings drive source operations in theater, but this type of training was not available until later.⁶ Unfortunately, the HUMINT collectors who provide most of the intelligence in PKO did not begin HUMINT-specific training until a month after mobilization. A field training exercise (FTX) presents a good venue to train CI and HUMINT personnel in scenarios that closely resemble reality in-theater, and should be considered for future mobilizations.

Additional training emphasis should be placed on report writing and editing at all levels. Strong writing skills, as well as CI and HUMINT technical reporting knowledge skills, are essential for success in PKO. We could not identify our weakness in this area until shortly before going into theater.

A success story during the pre-mobilization training was having the HARC embedded in the ACE. The HARC role in analyzing CI and HUMINT reporting enhanced the ability of the ACE to fuse a total common operating picture. We discovered the HARC should be organized so it reports directly to the G2X instead of the ACE Chief. The G2X is the primary recipient of HARC production and analysis. The G2X should drive HARC operations. This was not a big issue for us because of the professional working relationship between the G2X and ACE Chief. Additionally, we found the HARC was limited by the lack of robust HUMINT databases that would add realism to the training. This is an issue common to exercises conducted at the unclassified level.

Lessons Learned From Pre-Mobilization:

- Identify units for mobilization as early as possible and resist making changes.
- Identify key CI and HUMINT leadership early and integrate into all CPXs.

- Include CI and HUMINT SMEs to ensure success—this is crucial in all training.

The next phase of training took us to the Contingency Operations (CONOPS) Course at Grafenwoehr Training Area, Germany, to validate the readiness of all CI and HUMINT personnel to perform the SFOR mission. This was the first time the G2X, HARC, THOPS, THTs, and the CI Team trained together. Regrettably, this training and evaluation came only a few weeks prior to the SFOR Transfer Of Authority (TOA), which left little time for retraining and re-testing.

The training emphasis was tactical HUMINT source operations. The course fell short of training the G2X, HARC, and the CI Team because of this emphasis. A significant benefit of the course was one-on-one training with an SME who had G2X experience at both the Task Force and Corps levels. Future CONOPS courses sponsored by U.S. Army, Europe (USAREUR) will include enhanced G2X and HARC training scenarios relying on the automated CI/HUMINT Management System (CHIMS). USAREUR encouraged feedback on the shortcomings of the CONOPS Course and gave the G2X and TFCICA the opportunity, prior to TOA, to help rewrite the program of instruction. We also learned the CONOPS Course lacked in-depth training for the CI Team. A better alternative is for the TFCICA and the CI Team to spend at least one week with CI SMEs, in lieu of course participation. Furthermore, separate training should be conducted that is both CI and theater mission specific.

The CI Team would have benefited from learning theater-specific Intelligence Memorandum for Record (IMFR) formats, investigative plan development, record keeping, and overall CI report writing in relation to the Sub-Control Office (SCO) Handbook. Overall, the positive attitude among all personnel and their lead-

ership made the CONOPS Course a success. The willingness to learn and accept constructive criticism prepared CI and HUMINT personnel for future challenges.

Lessons Learned From

The CONOPS Course:

- Increased G2X and HARC involvement in the CPX.
- Separate training for the CI Team.

From the CONOPS Course we proceeded directly to the Mission Rehearsal Exercise (MRE)⁷ at the Combat Maneuver Training Center (CMTC), Hohenfels, Germany. The MRE is a mandatory exercise but failed to exercise CI and HUMINT for SFOR operations. The MRE training scenario had no G2X or TFCICA role. THTs were evaluated on soldier skills rarely used after arrival in theater. For example, great emphasis was placed on preventive maintenance checks and services (PMCS) for tactical vehicles. At SFOR, THTs use non-tactical vehicles.⁸ Contractors provide unit level maintenance of all vehicles. Time spent on maintenance checklists and completing forms could have been better used to teach THTs more practical skills, such as defensive driving or advanced surveillance detection.

To make the MRE more successful, training time should be devoted to reinforcing source operational skills, writing skills, integrating CI and HUMINT into the Intelligence Battlefield Operations System (IBOS), and gaining better theater situational awareness.

The CONOPS Course, not the MRE, should validate CI and HUMINT military occupational specialty (MOS) proficiency. This allows collective CI and HUMINT training to take place at the MRE. Additionally, CI and HUMINT personnel should go into theater at least four weeks prior to TOA and begin the difficult process of handing over operations. This permits personnel to better ac-

quaint themselves with the AO, its culture, and understanding the threat. The THTs, THOPS, CI Team, and HARC were able to do this with great success, but the G2X staff did not arrive until 10 days before TOA.

Lesson Learned From

The MRE:

- Build training scenarios and use role players, incorporating the G2X, HARC, and CI Team.
- Evaluate THTs on core skills specific to the theater of operations.
- Permit the CONOPS Course to serve as MRE credit.

The first 90 days after TOA is a time of great excitement, characterized by nervous energy. It presented outstanding opportunities to build on previous training. The relief in place is crucial to success. Every organization has its unique perspective and its own TTPs. The relieving unit must be careful to show respect to current SOPs and to adhere to the command being relieved.

During the transition period, each SFOR 13 THT leader was tasked by the SFOR 13 G2X to conduct a nightly “hotwash” after-action review (AAR) among their teams. The purpose of these AARs was to discuss the day’s events and list three items to sustain and three items to improve. The meetings were mandatory, conducted in private, and included input from the security force. At the end of each week, the cumulative results were gathered and sent by electronic mail to the G2X, who was in Germany. These AARs gave the G2X and the G2 awareness of issues before entering the theater. The relief-in-place went well and finally the mission became ours. As time progressed, we became aware of our shortcomings.

For the first few weeks the THTs struggled with report writing and collection focus. THTs primarily write Force Protection Information Reports (FPIRs)⁹ and Contact Reports in the

Balkans. The ability to accurately convey the results of a HUMINT source meeting, in writing, to higher headquarters is vital to success. This is an area where more practice was needed in order to gain proficiency. The G2X leadership tackled this problem through emphasis on clarity in writing, grammar usage, and sentence structure. The G2X directed the THOPS section to serve as second-line editors and directed personnel changes to ensure our strongest editors reviewed the reports. In addition, during the first monthly G2X Conference, G2X leadership put great emphasis on correcting mistakes related to writing. Team leaders, all company grade officers, were reminded of their personal responsibility as first-line report editors and their role in quality assurance. Within a few weeks of the conference we observed marked improvement in report quality.

To build on this momentum, we requested two HUMINT SMEs from USAREUR G2 to spend two weeks visiting the THTs in the field to assess their needs and provide TTPs. A strong relationship built with the USAREUR G2 proponent office for Balkans CI and HUMINT made the difference when seeking help and advice. Prior to mobilization, and during the CONOPS Course, we worked with USAREUR G2 several times to discuss progress in training, mobilization and other preparations to assume the mission. Upon arrival, the SMEs, both of whom were experienced HUMINT officers in the grade of Chief Warrant Officer 5, spent two days with the G2X staff reviewing areas needing improvement, and mapped out a plan to accomplish their task. In addition, they validated G2X and G2 concerns with the commander and staff. No one THT was singled out, but some teams needed more attention than others. The security force also received an assessment and benefited from the extra attention. The SMEs identified several areas in which the

THTs were doing well. The overall quality of FPIRs showed even more improvement from the early weeks of the mission, due to refined TTPs. The SMEs encouraged the operational flexibility given to the THTs, especially the command decision to lower the collector profile by using NTVs and permitting the wearing of civilian clothing for missions¹⁰.

The CI investigative effort was noted for its success and effectiveness. This compliment was echoed by the Theater SCO. Once again, the ability and willingness of CI and HUMINT personnel to learn and improve was singled out for praise. Consequently, we found new areas for improvement. Our contact reports were revised to more concisely report casual contact information. We built and improved the quality and content of source dossiers, which had been neglected over the years with the turnover of personnel every six months. Additionally, it was emphasized that source handlers should develop a skeptical view of their sources and prepare detailed questioning plans. Based on the feedback from the SMEs, the G2X

and THOPS Chief immediately developed a roadmap to implement the suggested improvements. Spot-checking, along with unannounced visits to THTs, was chosen as the best method to monitor progress. Improvement and quality assurance is a never-ending process and remains high on the agenda for the weekly G2X staff meeting. Regardless of whether a unit conducting tactical HUMINT operations is experienced or not, it is beneficial for SMEs to evaluate the Task Force and give an honest assessment of how operations are conducted.

We discovered soon after TOA the need for a focused HUMINT collection effort. About 30 days into the mission the first set of PIRs were published. We struggled to communicate a concise HUMINT collection emphasis to each THT based upon the PIRs. The HUMINT Collection Plan (HCP) that initially resided on the ACE homepage was unwieldy and mostly ignored. In addition, the ACE Collection Manager published a weekly Collection Emphasis Message (CEM). Both the HCP and CEM were over 30 pages and difficult for



THT source handlers and interpreter, with source screened from casual view, conducting a personal meeting in support of Task Force Eagle.

Photo courtesy of 1LT Osvaldo Cabrera.

THTs to use in focusing their collection efforts. To remedy this situation, we adopted a more relevant HUMINT Collection Focus (HCF) and eliminated the longer and more confusing HCP.

The HCF, produced by the HARC and approved by the G2X, condensed the CEM into HUMINT-specific collection tasks into two-week increments. We borrowed this idea from Joint Task Force 180 and modified it to meet the needs of a PKO environment. It reinforces the Task Force PIR and Intelligence requirements (IRs) and further reduces it into specific intelligence requirements (SIRs). In addition, the HCF lists collection requirements assigned to all THTs, and those requirements meant for specific teams based on the AO.

The THTs found the HCF to be an invaluable tool because it focused on HUMINT only and tailored the collection effort to them. The HCF also allowed the G2X to choose from the CEM those tasks appropriate for HUMINT and to reject those best suited for another HUMINT approach, such as the presence patrol (sensor) or liaison.

Perhaps, our greatest lesson learned involved the proper and timely release of HUMINT data. Often, we felt pressure, mostly from outside the IBOS, to prematurely release HUMINT prior to reports being checked for quality, accuracy, and completeness. We usually prevailed, and the intelligence was processed and analyzed properly prior to its release.

There were times when a THT collected intelligence that met the Task Force criteria for a Spot Report. Our guidelines were: receipt of intelligence warning of imminent danger or receipt of perishable information. We developed a TTP to "fast track" its reporting, processing, and analysis. This enabled the

timely release of intelligence to consumers. This TTP worked well on several occasions and demonstrated a total team effort, to include the ACE.

Lessons Learned The First 90 Days:

- ❑ Stress quality of reporting, not quantity.
- ❑ Use the HCF as a tool to enhance tactical HUMINT collection efforts.
- ❑ Use SMEs from higher headquarters to evaluate THT TTPs and give advice.
- ❑ Resist the pressure to release non-time sensitive HUMINT before it is properly analyzed.

The benefit of 20/20 hindsight inspired this article so others who will follow in the CI and HUMINT roles will learn from our experience. The road traveled to our destination as peacekeepers for SFOR 13 was difficult, but it did not have to be. Many of the issues brought forth can be or will be corrected by the time this article goes to press.

The truth of what we knew as leaders, collectors, investigators, managers, and analysts was validated soon after TOA. We found we were untrained in many aspects to assume the CI and HUMINT mission. Those issues have been addressed and hopefully corrected as follow-on peacekeepers prepare for their missions.

One truth guided us through this entire experience: do not underestimate the will and determination of a professional soldier to learn his duty and execute the mission. The leadership, motivation, professionalism, and high morale among SFOR 13's CI and HUMINT soldiers gave us the momentum to conquer all challenges that came our way.

Endnotes

1. Robert M. Pirsig (b. 1928), U.S. author. Zen and the Art of Motorcycle Maintenance, pt. 3, ch.24 (1974).
2. 49th Armored Division, Texas Army National Guard.
3. U.S. Army, INSCOM Training and Support Detachment, U.S. Army Intelligence Center, 2001. G2X Staff Handbook, Fort Huachuca, AZ.
4. Ibid.
5. This is the organization for SFOR 13 as of December 2002. Staffing requirements may vary based on the needs of the Army and the capabilities of the mobilized unit.
6. 515th MI Bde BOLD KNIGHT and GOLDEN KNIGHT exercises provide model training scenarios.
7. The acronym was changed to MRX in mid-2003.
8. Non-tactical vehicles (NTVs) are similar to civilian vehicles, but with U.S. Army registration.
9. SFOR 13 fielded CHIMS in July 2003, replacing the FPIR with the CI Information Report (CIIR).
10. The G2 delegated civilian clothing approval to the G2X. Civilian clothing was permitted for the convenience of the source and to lower the profile of the source handlers, interpreters, and enhanced security.

Major Lee Lacy is currently serving as the Deputy G2, 35th ID (M), Fort Leavenworth, KS. He served as the G2X for TF Eagle, SFOR 13, in Bosnia-Herzegovina, supporting Operation Joint Forge. His previous assignments include ACE Chief and G2 Chief of Operations in the 35th ID, S3 of the 635th MI Battalion, Missouri ARNG, and served S2 of the 2d Battalion, 635th Armor, Kansas ARNG. He spent four years on active duty, serving as a tank platoon leader, then Assistant Brigade S2, in the 1st ID (M). Major Lacy has a Bachelor of Arts in Political Science from the University of Arkansas, where he received his commission through Army ROTC. He is an Army Command and General Staff College graduate. Readers may reach him via E-mail at lee.lacy@us.army.mil and telephonically at 913-758-5278 or DSN 585-5278.

CI and HUMINT Operations in Support of Operation Enduring Freedom

by MAJ Ron Stallings and SFC Michael Foley

Much has been learned in recent years about the value of active counterintelligence (CI) and human intelligence (HUMINT) as they relate to modern conflict. Some intelligence professionals proclaim that CI and HUMINT have accounted for more than 80 percent of the intelligence collection in places such as Bosnia, Kosovo, and now Afghanistan. The introduction of the integrated 2X concept has proven itself to be a major step in the right direction. This concept incorporates management, control, and coordination measures which synchronize and deconflict CI and HUMINT in all directions throughout the theater of operations.

The "Draft" 2X Handbook continues to serve as the guide for 2X and CI and HUMINT operations in the deployed and tactical environment. Basic rules, roles, and responsibilities have proven to be "spot on." This document, coupled with experiences and lessons learned in Bosnia, Kosovo, and now Afghanistan, continue to produce a more refined concept. It outlines procedures and relationships involving national, strategic, and coalition CI and HUMINT assets. We clearly need to form and train tactical 2X officers and sections at various echelons throughout our military forces. Tactical CI and interrogation operations have vastly improved since the incorporation of the 2X concept.

Vital to the success in the process are the 2X, CI Coordinating Authority (CICA), and the HUMINT Operations Cell (HOC) chief. Led ultimately by the 2X, who serves as the Director of CI and HUMINT activities, these three individuals are charged with coordinating, managing,

deconflicting, and properly reporting—

- CI investigations.
- CI force protection (and HUMINT) source operations.
- Mobile and sporadic team-level operations.
- Interrogations and debriefing results.
- Certain other overt HUMINT operations, as required.
- All covert and/or special compartmented HUMINT operations.

This harmonious relationship fully incorporates the primary HUMINT analysis and requirements management and totally complements intelligence centers, especially the Coalition Joint Intelligence Support Element (C-JISE) in Afghanistan.

The XVIII Airborne Corps headquarters deployed to Afghanistan in support of Operation ENDURING FREEDOM (OEF) in May 2002 to establish the Combined Joint Task Force (CJTF-180) headquarters. Under the Director of Intelligence, initially COL Mike Flynn and later COL Ted Nicholas, the CJ2X section was understaffed, but filled with experi-

ence and expertise. MAJ Ron Stallings, the CJ2X, with over 10 years' experience in CI and HUMINT, had commanded an interrogation company, served as a G2X in Bosnia, and as the S3 of a Tactical Exploitation Battalion. SFC Michael Foley, serving in a field grade officer position as the Task Force CICA (TFCICA), had served for over 16 years in every progressive CI role from agent, to CI Operations non-commissioned officer (NCO) in Haiti, to Special Agent in-Charge of a forward deployed INSCOM Military Intelligence Detachment, and as First Sergeant of a CI and HUMINT Company. MAJ (Ret) and former XVIII Airborne Corps G2X, Don Gardner, who was responsible for training eight Balkans rotations on CI and HUMINT operations, also deployed as a part of the team. Additionally, the Defense Intelligence Agency's Defense HUMINT Service provided two very seasoned and experienced HOC Chiefs.

Prior to the arrival of CJTF-180, INSCOM's 202d Military Intelligence Battalion of the 513th Military Intel-



Rebuilding a destroyed bridge near Bagram Airfield, Afghanistan.

Photos courtesy of the authors.

ligence Brigade led the CI and HUMINT efforts. Their outstanding efforts established tactical CI and HUMINT collection and interrogation operations in Afghanistan. They had produced nearly fifteen hundred Intelligence Information Reports (IIRs) in just over seven months. Their reports database was absolutely superb and was instrumental during the hand-off to CJTF-180.

Immediate CI and HUMINT challenges included improving reporting timeliness and procedures, developing and managing source administration and records, redesigning the CI and HUMINT force structure, and focusing and synchronizing all related operations throughout the theater.

With a tremendous amount of support, CJTF-180's CJ2X team acquired authorization to publish and release IIRs locally, thus reducing reporting timelines significantly. It required an incredible work ethic and unbelievable numbers of work hours from the CJ2X and TFCICA; however, their commitment to "from collection to the community in less than 12 hours" was an internal slogan. Draft reporting and CI and HUMINT products were posted to Web pages (SECRET and TOP SECRET levels) within six hours of receipt, focusing primarily on units on the ground in Afghanistan. Final IIRs followed in less than six hours and were distributed to the intelligence community via standard intelligence reporting methods (AMHS-M3). Once the CJ2X became the release authority for the theater's tactical CI and HUMINT reporting, no longer did collected information have to leave the area of operations (AO) and return prior to being released to units and intelligence analysts throughout the intelligence community. This initiative made CI and HUMINT reporting a critical player in the targeting process and helped to synchronize all intelligence efforts in theater.

Local records and source administration procedures were emplaced

and controlled by the 2X section which set the stage for combined, joint, and multi-agency CI and HUMINT operations and deconfliction which followed. The TFCICA (SFC Michael Foley) created the first Theater Source Registry containing nearly three hundred active and inactive sources. He used this registry to deconflict active and inactive sources being used by all U.S. strategic and tactical CI and HUMINT collectors. Deconfliction and synchronization of operations were necessary to establish operational and technical control over theater CI and HUMINT operations and provide unity to the intelligence effort. The TFCICA put additional systems in place that led to the development of individual source files or dossiers and management. This gave the local command visibility and positive control of activities throughout the Combined Joint Operational Area (CJOA). By design, the TFCICA is the tool by which the command directs and coordinates tactical CI and source operations. With the advent of the TFCICA, the much needed structure, management, and control of CI and HUMINT source operations directly impacted the tactical commander's plans and intentions.

Standing operating procedures (SOPs) and tactics, techniques, and procedures (TTPs) were written and instituted; routine coordination between units and agencies occurred; reporting was standardized and localized for review, approval, and publication; collectors were given constant target focus and guidance; and CI became synchronized with HUMINT. Reporting became more accurate and timely and, most importantly, targetable and mission enhancing. Positive relationships between all CI and HUMINT organizations in theater were fostered.

The redesign of the CI and HUMINT force structure provided both direct and general support to commanders on the ground at all levels and facilitated better area coverage, responsiveness, and a balanced approach to CI and HUMINT collection management. Prior to CJTF-180's arrival CI and HUMINT collection planning and management were not synchronized with the efforts of the local intelligence collection manager. The number of CI teams in theater increased from 4x (6- to 9-soldier) teams to 9x (4-soldier) teams. The largest increase in teams went to Kandahar and the southeastern portion of the AO. The number of inter-



Wreckage found in Afghanistan.

rogators working in the interrogation facility increased from 7 to 15 personnel. This restructure took place with the arrival of the 519th Military Intelligence Battalion and the TF Panther (3D Brigade 82D ABN DIV) from Fort Bragg, NC, but with little to no increase in the total numbers of CI and HUMINT personnel in the theater.

Probably the most apparent change and most significant contribution of the 2X concept arriving with CJTF-180 was local command and control and synchronization to all CI and HUMINT operations. By design, the CJ2X coordinated and ensured CI and HUMINT support to both local commanders and national requirements. Collection efforts were aligned with the intelligence requirements of commanders (at all levels) on the ground in Afghanistan, and CI and HUMINT collection became a key player in the targeting process. CI and HUMINT reporting became a source of timely, accurate (in most cases, immediately verified by multiple other intelligence platforms), and targetable data. We also created systems to dynamically re-task CI and HUMINT sources that worked for various agencies and organizations from one location (the CJ2X section). Source operations became synchronized with interrogation operations, and tactical and strategic CI and HUMINT merged in both locations (source operations outside the wire and interrogations inside the wire).

CI and HUMINT lessons learned were numerous with CJTF-180's assumption of the OEF mission:

- ❑ **Prior to Deployment.** Coordinate manning (to include national augmentation), equipment, communications, and other unique requirements (such as Intelligence Contingency Funds [ICF], Incentives, analytical and reporting tools, Collector Reporter Codes, Field Reporter Numbers and methods, operational uniform/clothing, and critical reach-back

relationships). Prior planning cannot be emphasized enough on much of these tasks. CI and HUMINT operations must be in place and operational before the warfighter hits the ground. Protecting the force is a continuous process and must be command supported.

- ❑ **Source Administration.** Cut no corners when it comes to source administration and records keeping. There is no substitute for training and SOPs. Failing to maintain proper dossiers and registries is a costly mistake. Demand detailed and timely efforts in the development and maintenance of local dossiers and registries at all levels. SOPs may differ slightly between units, but regulations require these items be maintained. They are absolutely mandatory when conducting hand-offs, deconfliction, and source validation.
- ❑ **SOPs and TTPs.** Ensure these are emplaced, rehearsed, tested, and improved with performance. These operating procedures can be easily tailored to fit the requirements of various AORs.
- ❑ **CI and HUMINT Collection Management.** Ensure the Collection Management Officer (CMO) in the intelligence center integrates and manages CI and HUMINT into the unit collection plan. The CMO manages the collection plan, and CI and HUMINT represents one of many pieces to the puzzle. The CMO must work closely with the embedded CI and HUMINT technicians of the intelligence center. CI and HUMINT specialists constantly track all intelligence requirements to ensure that CI and HUMINT operations are focused on the commander's priorities. The HUMINT Analysis and Requirements Cell (HARC) (requirements being the operative word) is a unique tool, organic to an intelligence center... but guided by the 2X team and used to provide the necessary constant analysis of both CI and HUMINT information and sources. The HARC is additionally charged with ensuring that CI and HUMINT collectors are focusing on the HUMINT collection "Requirements" priorities of the commander and integrated into the overall unit collection plan. These requirements must be shared and tasked down to even passive HUMINT collectors (Civil Affairs, Military Police, Criminal Investigation Division, presence patrols, psychological operations, Medical units, information operations); this was underway in Afghanistan by late October 2002.
- ❑ **Deconfliction.** Consider both active and passive HUMINT collectors throughout deconfliction of CI and HUMINT operations. This is probably the most difficult task assigned to the TFCICA and the 2X team. The standard approach is to execute deconfliction from the lowest and most internal elements outward to ultimately national and coalition collectors. Deconfliction begins with proper source administration and ends with extensive coordination and good work relationships. Three areas must be addressed on the subject of deconfliction:
 - Registries and rosters.
 - Meeting sites and times.
 - Managing placement and access.Once deconfliction extends beyond the borders of the standard chain of command (that is, national collectors, special operations forces, sister services, and coalition forces), working relationships and mutual objectives become critical. The process begins with requiring and managing meticulous source rosters and constantly updated operational schedules. It requires cooperation between units,

agencies, and coalitions. Command support and emphasis is a must in order for deconfliction to work. Deconfliction of CI and HUMINT operations and sources is extremely difficult and frustrating to execute; therefore, it is one of the biggest challenges for the 2X and TFCICA. In Afghanistan, a tiered approach to deconfliction of sources was used. We obtained source registers from the (U.S.) tactical organizations (Army, Air Force, Marines, and the Special Operations community); deconflicted those, and created a (U.S.) theater source registry for “tactical” collectors. We continued to deconflict with (U.S.) national agencies. At this point, we had a totally deconflicted (U.S.) theater source registry. Special emphasis was placed on the selection of sources based on placement and access and level of information; that is, tactical versus strategic information. By early October 2002, we were beginning to conduct deconfliction with Coalition CI and HUMINT collectors. Once completed, we could be certain that no source was being seen, paid, or supported by multiple organizations. [Note: There is an order merit or precedence (often first come, first serve) that aids in deciding the fate of sources when there is a conflict.] Finally, this process is strictly managed by the G2X and TFCICA.

- **Screening Cell Operations.** Immediately implement screening operations for local and civilian hires. For obvious force protection reasons, questioning local hires is required to determine placement or access and possible associations that would be of U.S. interest. Screening locals and civilians that operate within the wire is imperative. This requirement is often overlooked and therefore not built into our

force structure. The use of CI and HUMINT soldiers as screeners supported by linguist is the preferred method of establishing screening operations. With operations ongoing and SOPs in place, the screening cell should transition to a 90 percent (civilian contractor) 10 percent military mix, with 351E as the cell officer in charge. The mission of the screening cell is not as flamboyant as conducting CI and HUMINT source operations; however, it is equally important.

- **Interrogation Facility Operations.** Manage and coordinate interrogation facility operations. Detention facility and interrogations add a whole new set of challenges to the 2X team. The HOC Chief is the point man for the 2X in the management and coordination of interrogation operations. As the Defense Intelligence Agency is also the lead proponent for the Joint Interrogation Debriefing Cell (JIDC), the HOC Chief has a direct interest in the operations of the interrogation facility. The JIDC, from within the interrogation facility, functions as the national and strategic interrogations cell (non-tactical and nonmilitary organizations). The facility should be directed by intelligence requirements and should report like any other HUMINT resource.
- **Screening Released Detainees.** Exploit released detainees; they make excellent candidates for leads and/or continued intelligence sources. Part of the release process (after the determination has been made to release) should include a CI screening of potential sources.
- **Effective Use of Mobile Interrogation Teams (MITs).** Implement screening and interrogation operations forward (on or near the battlefield or point of capture) to reduce the chance of detaining personnel with no intelligence

or target value. This method helps to eliminate overcrowding facilities, associated costs, and administrative issues. Forward screening and tactical interrogations forward allow capturing units to sift through potential detainees and enemy prisoners of war (EPWs) on or near the point of capture, reducing the population to only those of intelligence, criminal, tactical, or strategic value. When an MIT is used, it should consist of only the most experienced and senior interrogators (97Es/351Es) and best qualified linguist support available. Battlefield, on-the-spot tactical screening or interrogation is not the time to educate or train young questionable soldiers, nor is it the time to assume that 97Bs can perform the mission of 97Es without prior training.



MAJ Ron Stallings is currently the G2X (Director of CI/HUMINT Operations) for XVIII Airborne Corps. He recently served as the initial CJ2X for CJTF-180 in Afghanistan in support of Operation Enduring Freedom. MAJ Stallings also served as the G2X at Multinational Division North in Bosnia-Herzegovina in support of Operation Joint Forge. He commanded an interrogation company, served as the Executive Officer and Operations Officer of a CI Company, and the S3 of a CI/HUMINT Battalion. Readers may contact MAJ Stallings via E-mail at g2xxviii@bragg.army.mil and by telephone at DSN 236-6965/5975.

SFC Michael Foley is currently the NCOIC of the G2X for XVIII Airborne Corps. He recently served as the Task Force Counterintelligence Coordination Authority for CJTF-180 in Afghanistan in support of Operation Enduring Freedom. SFC Foley previously served as the Special Agent in Charge of the Uijongbu Military Intelligence Detachment, as well as the First Sergeant of a CI and HUMINT Company in the 501st MI Brigade, Seoul Korea. Prior to his assignment in Korea, SFC Foley served as the G2/CI Officer for the 82D Airborne Division at Fort Bragg, NC. Readers may contact SFC Foley via E-mail at g2xNCOIC@bragg.army.mil and by telephone at DSN 236-6965/5975.

Transforming Counterintelligence and Human Intelligence

by CW3 Larry Norris

Identifying Future CI and HUMINT Requirements

In November 2001, the Commanding General, United States Army Intelligence Center and Fort Huachuca (USAIC&FH), chartered the Counterintelligence (CI) and Human Intelligence (HUMINT) Integrated Concept Team (ICT) to identify the requirements needed to transform today's CI and HUMINT forces to meet the information demands of the Army's Objective Force (OF).

The CI and HUMINT ICT was chaired by the Director of Combat Developments, USAIC&FH, co-chaired by Department of the Army (DA) Military Intelligence (MI) CI Division (DAMI-CD), Deputy Chief of Staff, Army G2, and consisted of senior military and civilian representatives from Forces Command (FORSCOM), Intelligence and Security Command (INSCOM), National Guard Bureau (NGB), Office of the Chief of Army Reserve (OCAR), U.S. Army, Europe (USAREUR), U.S. Army Pacific (USARPAC), U.S. Army South (USARSO), and U.S. Army Special Operations Command (USASOC). The ICT also included senior CI and HUMINT noncommissioned officers (NCOs), warrant officers, and officers as subject matter experts (SMEs) who identified requirements and solutions on how to transform the CI and HUMINT communities.

The end-state or products of the ICT were two separate CI and HUMINT Operational and Organizational (O&O) plans that would provide detail on the CI and HUMINT capabilities required in the OF. The CI and HUMINT O&O plans are the foundation documents to establish a transformation strategy that ad-

dresses all aspects of both the CI and HUMINT disciplines. The Army categorizes requirements by Doctrine, Organization, Training, Materiel, Leader and Education, Personnel, and Facilities (DOTMLPF). These categories are arranged in a specific order based upon the complexity and amount of resources required to successfully implement validated requirements.

Declination of CI and HUMINT

The U.S. Army has always been a threat-based organization. Force structure, manning levels, weapons systems, doctrine, and war plans were based upon a specific threat. Since the end of World War II, that threat was the Soviet Union. During the Cold War era the roles, responsibilities, and functions were clearly defined for both CI and HUMINT. CI was focused on countering the intelligence collection efforts of the Soviet Bloc to deny them information for the development of countermeasures to plans and systems. HUMINT focused on collecting information on Soviet intentions, capabilities, disposition, etc., to support policy makers and military planners.

After the collapse of the Soviet Union, the focus of Army CI and HUMINT became confused due to a lack of identifiable threat. Compounding this confusion was the assumption of all separate military service Title 10 HUMINT missions under the Defense Intelligence Agency (DIA) Defense HUMINT Service (DHS) in October 1995. This realignment caused a void in the Army's ability to conduct HUMINT operations under the auspices of **Title 50, War and National Defense**, during any contingency operations to support the information requirements of combatant commanders.

Throughout the 1990's, as operational deployments in stability operations and support operations environments increased, so did the requirement to satisfy the information needs of combat commanders. With a lack of validated tactical HUMINT (TAC HUMINT) collection capability prescribed in policy and defined in doctrine, commander's developed a task organization of both CI and HUMINT soldiers to fulfill their information requirements. This task organization capitalized on skill sets of CI and HUMINT, the language capability of HUMINT, and the only validated collection program available, CI Force Protection Source Operations (CFSO). However, CFSO was not established to be an all-encompassing HUMINT collection mission, but rather a collection program focused primarily on identifying collection efforts targeting U.S. or allied interests, as well as hostile threats or force protection issues.

The task organization of both CI and HUMINT to accomplish a HUMINT collection mission has significantly degraded the CI mission. Although done out of necessity, the emergence of TAC HUMINT elements, which has never been established in policy or doctrine, substituted one void for another. Throughout the 1990's, the Army's intelligence community lost focus on countering the adversarial intelligence threat, seeking instead to demonstrate their responsiveness to the warfighter by supporting predominantly HUMINT missions during contingency operations. This included CI elements at all echelons, echelons corps and below (ECB) to echelons above corps (EAC).

The success of both CI and HUMINT to satisfy the combat

commander's need for tactical HUMINT information has resulted in the perception throughout the Army, to include the MI community, that CI equals HUMINT collection, or CI and HUMINT are one and the same. This perception has also resulted in numerous Force Design Updates that have, or will, cause significant increases in CI authorizations to meet HUMINT collection requirements while HUMINT continues to stagnate.

This blurring of missions, roles, responsibilities, and functions sets the stage for the CI and HUMINT ICT to develop the requirements to transform Army CI and HUMINT to help ensure complete information dominance in the OF.

The Army's Objective Force

The purpose of the Army is to fight and win our nation's wars. To accomplish this, the Army must act in union with all the military services, other allied and coalition forces, and nongovernmental organizations to operate as a joint, multinational, combined, or coalition team. Based upon the current National Military Strategy (NMS), the Army will transform into an organization that will be able to deploy to increasingly complex operational environments to engage a wider range, and often, less identifiable adversary. The former Army Chief of Staff established seven characteristics that the Army's OF must embody to successfully execute future operations:

- Responsive.
- Deployable.
- Agile.
- Versatile.
- Lethal.
- Survivable.
- Sustainable.

As a network-centric force, the OF will increasingly depend on high levels of information collection, fusion, and synthesis. Rapid, relevant, and accurate intelligence, surveillance, and reconnaissance (ISR) will give combat commanders the situational

awareness required to develop the situation out-of-contact and maneuver to a place and time on the battlefield to engage and destroy the enemy with minimal impact to friendly forces. ISR will be a key enabler to achieving the quality of "Firsts" emphasized by the Chief of Staff of the Army—See First, Understand First, Act First, and Finish Decisively!

As part of the ISR community, CI and HUMINT have become an increasingly valuable commodity to combatant commanders. As the eyes and ears of the combat commander, CI and HUMINT operators are one of the few all-weather, all-terrain, general support (GS) and direct support (DS) assets that can respond directly to a commander's information need with little warning, preparation, or asset bureaucracy.

CI and HUMINT Operational Environment

Analysis of recent operations and preparation for future operations requires the Army to rapidly deploy to any operational environment in the world in order to quickly accomplish its assigned mission. The NMS addresses Strategic Responsiveness as a key tenet of the OF. Future military operations require a reduced footprint and focused logistics to achieve surprise and rapid response to emerging crises. OF CI and HUMINT elements must be equipped and structured to provide a rapid deployment capability. Equipment will be small, lightweight, and interoperable with all intelligence information processing equipment in the Army and with other military services to ensure immediate reporting, dissemination, and database sharing. CI and HUMINT elements will be structured so that all operational, management, and analysis elements are modular and can be tailored to any military operation. CI and HUMINT elements located at echelons above their supported unit should be able to provide plug-in

packages and quickly link-up, assimilate, and provide support to the unit commander.

Threat

CI and HUMINT elements will continue to deploy into complex environments when directed. The OF will encounter a multitude of asymmetric and asynchronous threats including—

- Attacks by insurgents, terrorists, and other organized criminal organizations.
- Information warfare attacks.
- Direct, armed conflict with conventional military forces.
- Proliferation and use of Weapons of Mass Destruction (WMD).

These threats may be encountered at any time, in any place, across the spectrum of conflict. CI and HUMINT will play an increased role in developing information that supports predictive analysis to allow combat and response forces to neutralize conventional and unconventional threats before they can counter or execute offensive actions against U.S. or allied interests.

Transforming CI and HUMINT

While the focus of the CI and HUMINT ICT was to identify CI and HUMINT requirements in the OF, the ICT realized there were many problems and issues with today's (i.e., Current Force) CI and HUMINT that must be addressed to posture both CI and HUMINT for Transformation. The ICT identified seven Macro Requirements for both CI and HUMINT. (See Figure 1.)

*2X Concept

The *2X staff provides advice to the senior intelligence officer (SIO) and command on the employment of CI and HUMINT assets in the commander's area of intelligence responsibility (AOIR). Due to the legal complexities and sensitive nature of CI and HUMINT operations, the 2X provides technical control and oversight of all CI and HUMINT assets

Balance MOS versus Mission Requirements. All major Army commands (MACOMs) represented in the ICT were charged with analyzing their individual tables of organization and equipment (TOE) or tables of distribution and allowances (TDA) manning documents and restructuring the ratio of CI to HUMINT based upon their unique mission profiles. The best example is the CI to HUMINT ratio within ECB units in which there is parity in numbers between CI and HUMINT. However, the predominant mission in these units is HUMINT collection.

Establish a HUMINT Collection Capability. A validated HUMINT collection mission will be prescribed in policy and defined in doctrine. This will be accomplished through the revision of AR 381-100 and address a specific HUMINT collection program to satisfy the Army's Title 50 requirements during contingency operations. These changes also require an increased HUMINT force structure, which will be achieved by re-coding a majority, not all, CI positions in ECB units to HUMINT positions.

Refocus CI on Countering the Intelligence Threat and Activities of Our Adversaries. Once HUMINT fully reassumes the tactical HUMINT mission, CI will focus solely on countering the adversarial intelligence threats' ability to successfully target and collect on US or allied interests.

Educate Leaders. Senior leader courses need to include formal programs of instruction on the distinct functions between CI and HUMINT and their proper employment. These courses include Advance Courses, Pre-Command Courses, and Senior Staff Courses.

Provide *2X Capability At All Echelons. The 2X is established in Joint Pub 2-01 and has been used successfully in all contingency operations since Operation DESERT STORM. The Army will institutionalize and professionalize the 2X concept from Corps to Army level. The 2X at different echelons will help to decentralize the current stovepipe approval and oversight of CI and HUMINT operations to give more control and flexibility to individual command elements. The *2X will also establish an Army 2X which will serve as the Army level executive agent to serve the interests for all Army CI and HUMINT activities, provide policy, and coordinate resource issues between the Department of the Army and Department of Defense.

Support Full Spectrum of Military Operations. Army CI and HUMINT elements must be trained, equipped, and organized to support the full range of military operations (peacetime military engagements [PMEs], small-scale contingencies [SSCs], and Major Theaters of War [MTWs]). The ability to support full spectrum operations in the OF construct will mean that Army CI and HUMINT elements must be composed of modular and standardized team formations. These standardized team formations will be force pooled at different echelons and can rapidly integrate into and support a designated combat force during contingency operations as described in the CI and HUMINT operational environment described above.

Invest In Technologies To Enhance Capabilities. Emerging technologies will allow the formation of distributed, interdependent, and collaborative network environments. These network centric information grids will facilitate tipping and cueing of intelligence resources at all levels and will significantly increase the Army's advantage in intelligence collection, analysis, and security. Nano-technology may result in miniature, mobile, autonomous sensors that can penetrate the secure and remote facilities of an adversary. Biometric technologies will allow rapid identification, coding, and tracking of adversaries, human sources; and cataloging of information concerning enemy prisoners of war (EPWs), detainees, and civilians of CI and HUMINT interest throughout the battlespace. Biometrics will also provide secure authentication of individuals seeking network or facility access.

NOTE: “*” denotes the 2X at all echelons S/G/J/C.

Figure 1. CI and HUMINT Macro Requirements.

operating within his designated AOIR. The *2X ensures unity of effort of all CI and HUMINT assets for the supported commander.

The *2X staff will be responsible for the integration, correlation, and fusion of all human sensor information into the Distributed Common Ground System-Army (DCGS-A), the future Intelligence Battlefield Operating System (IBOS) within the *2X AOIR. The *2X staff will also provide single-source analysis and help build the all-source picture and populate the commander's common operational picture (COP). (See Figures 2 and 3.)

Individual DOTMLPF Requirements

Although, DOTMLPF functional areas have a specific order when as-

sessing solutions for identified requirements, the following DOTMLPF implications are listed in a specific order to better articulate the changes to the CI and HUMINT disciplines to better support extraordinary evolution in how the Army will conduct operations in the future.

Counterintelligence Personnel

MOS 97B will be a skill level 20 and above Military Occupational Specialty (MOS) and will no longer be accessed as initial entry training (IET) due to the personnel qualification criteria and the U.S. Code minimum age requirement for CI Special Agents to conduct sensitive investigations and operations. CI Special Agents will be accessed from three source pools:

1. Primary Feeder MOS (97E). 97E, HUMINT Collector, will be the primary feeder MOS for 97B. A number of the skill sets used by both MOSs are similar in their application. However, differences in mission focus, operational execution, and legal requirements make it necessary for the two MOSs to remain separate.

- 97E First Term.** First-term 97E enlisted soldiers attending HUMINT IET and meet all qualification criteria with the exception of rank may be identified by USAIC&FH proponent training organizations for follow-on CI training and assignment to a CI organization or position. These by-exception applicants will be screened and approved at the proponent in accordance with

2X STAFF OFFICER	<ul style="list-style-type: none"> <input type="checkbox"/> The 35E who attended advanced training that provides necessary perspective of worldwide CI and HUMINT operations. <input type="checkbox"/> Principal advisor to the SIO and commander on all CI and HUMINT operations within their respective AOIR. <input type="checkbox"/> Exercises technical control over his assigned Army CI and HUMINT entities in the designated AOIR. <input type="checkbox"/> Is the principal representative of the SIO and the commander when coordinating and deconflicting CI and HUMINT activities within national or theater agencies operating in the AOIR. <input type="checkbox"/> Supports and functions as an extension of the collection and requirements managers for— <ul style="list-style-type: none"> ➤ Planning and coordinating CI and HUMINT operations. ➤ Reviewing and validating CI and HUMINT requirements. ➤ Recommending assignment of tasks to specific teams. ➤ Conducting liaison with non-organic HUMINT collection elements. <p><i>*This liaison includes national level and coalition force assets for source deconfliction and special activities outside the *2X AOIR.</i></p>
CI COORDINATING AUTHORITY (CICA)	<ul style="list-style-type: none"> <input type="checkbox"/> Coordinates and synchronizes all CI activities in the designated AOIR. <input type="checkbox"/> Exercises technical control over all CI entities in the designated AOIR and deconflicts CI activities with higher, lower, and adjacent CI elements. <input type="checkbox"/> Accomplishes all responsibilities through coordination with the operational units, the HOC, and the OSC.
HUMINT OPERATIONS CELL (OSC)	<ul style="list-style-type: none"> <input type="checkbox"/> Coordinates and synchronizes all HUMINT activities in the AOIR. <input type="checkbox"/> Exercises technical control over all HUMINT entities in the designated AOIR and deconflicts HUMINT activities with higher, lower, and adjacent HUMINT elements. <input type="checkbox"/> Accomplishes all responsibilities through coordination with the operational units and the CICA and OSC.
CI ANALYSIS CELL (CIAC) AND HUMINT ANALYSIS CELL (HAC)	<ul style="list-style-type: none"> <input type="checkbox"/> Analyzes their respective discipline reporting and other intelligence discipline reporting and analysis to provide a single-source analysis of the adversarial intelligence capability targeting friendly forces. <input type="checkbox"/> Determines gaps in reporting and coordinating with other analysis elements and technical controllers to cross-cue other collection sensor systems. <input type="checkbox"/> Produces and disseminates discipline-specific products and provides input to intelligence summaries (INTSUMs). <input type="checkbox"/> Uses analytical tools to develop long-term collection plans and provide reporting feedback that will support all CI and HUMINT elements in the supported command's AOIR.

Figure 2. Roles and Responsibilities of the *2X Staff.

AR 614-200, DA Pamphlets 611-21, 600-8, and 351-4. HUMINT IET soldiers approved for follow-on CI training and assignment will retain the HUMINT MOS until completion of probationary requirements and promotion to E-5/SGT, at which time they will be permanently awarded the CI MOS code.

97E Voluntary Reclassification. 97Es who meet 97B MOS eligibility requirements can volunteer for reclassification to 97B upon promotion to E-5/SGT or first re-enlistment. Completion of the Basic CI Special Agents Course (BCISAC) is required prior to temporary awarding of 97B MOS and assignment to a CI position. After successful completion of the BCISAC and the one-year probationary period in accor-

dance with applicable regulations, MOS 97B will be permanently awarded as the primary MOS. The probationary period will begin upon assignment to a CI position.

2. Inter/Intra-Service Personnel (Non-HUMINT). Army and other military service personnel can apply for reclassification to 97B if they meet MOS eligibility requirements. Inter/ Intra service applicants (non-HUMINT) must hold the rank of E-5/ SGT for awarding of the CI MOS code. All personnel applying for Army's CI Program will be screened and meet the eligibility criteria outlined in AR 614-200, DA Pamphlets 611-21, 600-8, and 351-4 before being considered for selection and training for 97B CI Special Agent.

3. Army Civilian Acquired Skills Program (ACASP). Use of the

ACASP program will require revision of the current AR 611-21 and 614-200, and will be the exception and not the rule for CI program accessions. Accessions through ACASP will identify those personnel who hold certain qualifications such as education and law enforcement certification and employment that would provide them unique skills to succeed in CI training and assignments. Under the ACASP program IET who meet the criteria in accordance with applicable policies and regulations will be required to complete the BCISAC and a follow-on utilization assignment. ACASP enlistees will be eligible for accelerated promotion to E-5/SGT upon completion of training and evaluation by unit commander at first operational assignment.

CI Probation Program. The Probationary Program has existed for

years. However, the program has failed due to the lack of a centralized Office of Primary Responsibility (OPR) to track CI Special Agents in probationary status and hold commanders and supervisors accountable for evaluating and recommending retention or removal of probationary agents. The revised AR 381-20 will establish an OPR for the CI Probationary Program as well as mandatory evaluations and retention and removal criteria to ensure only qualified and competent probationary CI Special Agents are retained in the MOS.

Human Intelligence Personnel

The most significant change to the HUMINT MOS, besides being designated as the feeder MOS for CI, will be the elimination of the language requirement for awarding of the MOS after completion of advanced individual training (AIT). The recommendation for eliminating 97E as a language-dependent MOS considered the following issues:

Language Training. The Army has not been able to adequately train the right mix of language-trained HUMINT soldiers to accomplish the varied contingency operations over the past several years. Increased operations tempo (OPTEMPO) for HUMINT organizations makes it difficult for soldiers to maintain required

language proficiency to retain the HUMINT MOS. While there are extremely language-gifted HUMINT soldiers in the Army, most only have ability to carry on generic conversational dialogues. The majority of HUMINT soldiers do not have the ability to effectively communicate, translate, and interpret complex data required in intelligence operations. These problems have led to an increased reliance on contractor linguists to successfully accomplish the HUMINT mission.

Retention. The Army has not achieved accessions goals for IET HUMINT soldiers for the past five years, averaging 56 percent of established recruitment goals. Of the first-term enlistees the Army recruits, only 30 percent opt to reenlist for a second term. Considering the cost to train HUMINT soldiers and the amount of time the Army benefits from the expense, training all IET HUMINT soldiers is not cost beneficial. Our current recruiting problems, coupled with the fact that the Army is seeking to increase the overall numbers of HUMINT soldiers, requires a larger accessions source pool. However, meeting our accessions to fill our HUMINT positions has to be done without compromising the high standards that HUMINT operators must have to be trusted to carry out sensitive intelligence operations.

Language Positions. Eliminating language dependency from the HUMINT MOS does not mean we are eliminating the requirement for a language. The goal is to code most, if not all, language positions to E-5 and above HUMINT positions and to use language as an additional incentive for first-term soldiers to reenlist. Re-enlistment rates for second-term or mid-career soldiers significantly increases to 62 percent. This would provide more long-term use of language-qualified HUMINT soldiers. Coding language positions at the E-5 and above level also makes sense considering the operational employment of HUMINT teams. Most HUMINT elements operate in four-person teams or two-person sub-teams, with the team sergeant or assistant team sergeant the focus on conducting the operations while junior soldiers assist and learn.

An argument could be made that the main incentive for persons to enlist for 97E is the language training. This may have some truth, but one could also argue it is more a failure in appropriately marketing the MOS. Interrogator versus HUMINT operator: which would be more appealing to a new recruit interested in the intelligence field? By broadening the accessions pool and effectively marketing the MOS, the Army will be able to achieve a higher accessions rate which will be needed to fill increases in HUMINT requirements. However, with the projected increases in HUMINT positions, the Army may still have to explore establishing other incentives and bonus options to attract more attention.

A thorough analysis will have to be made based upon new force designs and standards of grading across the force to assess the impact upon the training throughput for the Defense Language Institute. As a snapshot analysis, the total training throughput requirements probably will not be severely impacted. Even though we are eliminating the language dependency from the MOS and do not plan

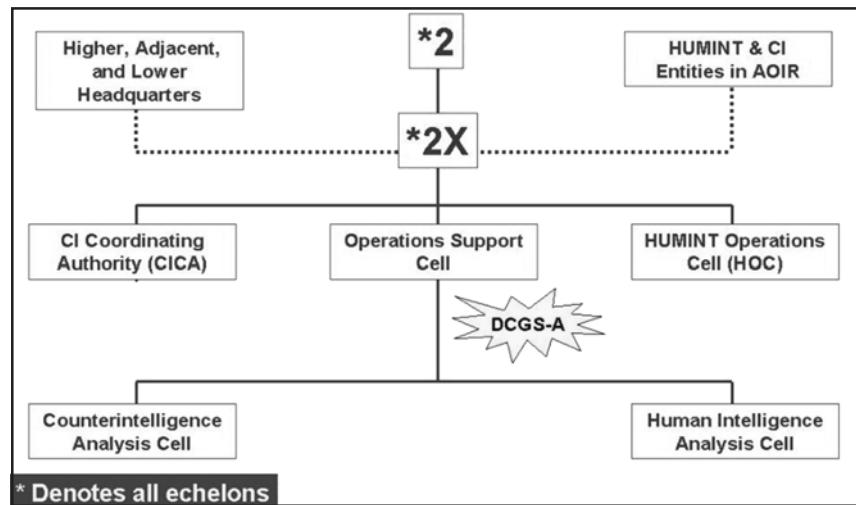


Figure 3. *2X Staff Organizational Structure.

to train IET HUMINT soldiers, with the overall increases in HUMINT positions, throughput should stay near current numbers. If there are decreases in training throughput, the money saved will be used to reinvest in additional intermediate and advanced-level language training. MI should not be focused on the quantity of language-trained HUMINT operators throughout the force, but the quality of the HUMINT operators who can support the force in contingency operations. (See Figure 4.)

Warrant Officer Accessions and Sustainability for 351B/E

A major issue for both disciplines is the ability to recruit and sustain the required number of CI and HUMINT warrant officers (WOs). WO recruiting and accessions goals for both CI and HUMINT have not been achieved for the past four years. The total number of active duty CI and HUMINT WOs have continually declined during that time, with the exception of the Stop Loss, leaving a combined vacancy of approximately 100 combined CI and HUMINT positions. This can be attributed to many factors (e.g., pay compression, OPTEMPO, etc.); however, the overall problem in recruitment and accessions has been the extremely low ratio of WO positions to available source pool (enlisted equivalent feeder MOS). The WO to enlisted (not just NCO) ratio for CI and HUMINT is 1:4 and 1:5, respectively. Based upon analysis by The Office of the Chief of Military Intelligence (OCMI), the required WO to enlisted ratio required just to maintain required accessions is 1:8.

The Commanding Generals, USAIC&FH and INSCOM, as well as the Deputy Chief of Staff, G2, have coordinated with all MACOMs to evaluate all CI and HUMINT WO positions for potential conversion to senior NCO positions. Army CI and HUMINT WO positions continue to go unfilled and not supported through

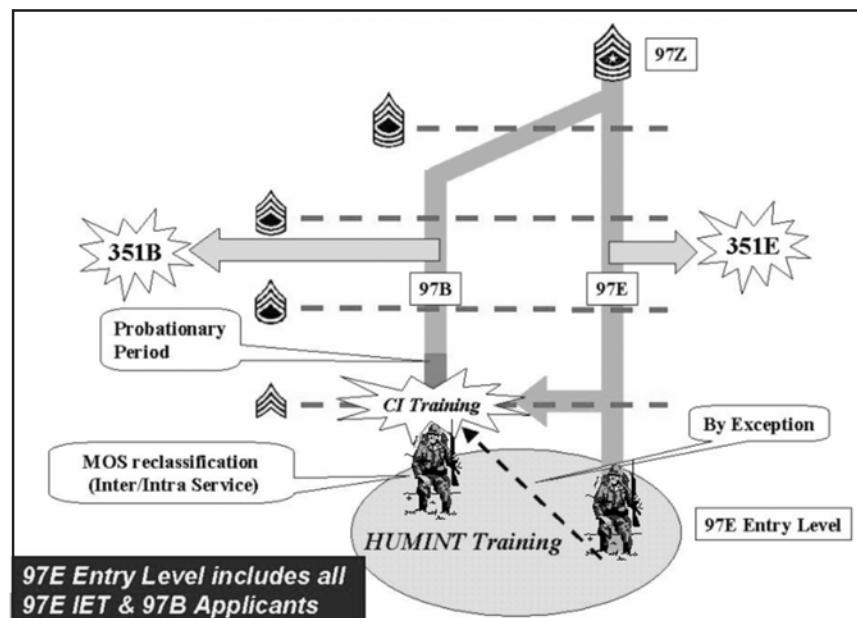


Figure 4. CI and HUMINT MOS Model.

the Personnel Command (PERSCOM) Officer Distribution Plan (ODP). The MI community has essentially two courses of action:

- 1 Recode chronically unfilled CI and HUMINT WO positions to NCO positions and maintain total MOS population (enlisted and WO).
- 2 Allow PERSCOM to completely cut those unfilled WO positions and reduce the total MOS population.

Recoding is the most viable option because many CI and HUMINT WOs are filling team-leader positions that should be filled by NCOs, especially at the tactical (ECB) level.

ORGANIZATION

CI and HUMINT force structure will be a key tenet in supporting Army OF operations. CI and HUMINT assets have to be tailored to the mission focus at all echelons. To support the OF construct, CI and HUMINT organizations have to be standardized to support contingency operations planning and modular to provide scaleable plug-in packages to combat elements and combined joint task force (C/JTF) organizations.

Mission focused CI and HUMINT force structure at the tactical level. In

today's force, structure parity exists between the CI and HUMINT assets in ECB organizations. However, the predominant mission required by commanders in the tactical force is for HUMINT collection to support their information requirements on enemy activities. This situation has been a key factor in the TAC HUMINT phenomena, using CI assets to accomplish a HUMINT mission. This does not mean that there is no CI mission, only that it is smaller in scope than in operational or strategic environments.

The Battle Command On-the Move and OF concepts developed by the Combined Arms Center dictate force pooling a majority of all combat support and combat service support at the Corps level. In keeping with this requirement, all tactical level CI and HUMINT elements will be force pooled at the Corps-like level or unit of employment (UE) and provided as plug-in packages down to division and brigade-like or unit of action (UA) elements.

Providing modular and scaleable packages to Army Forces (ARFOR), joint and combined elements will require standardized team configurations. (See Figure 5.) Both CI and HUMINT will use two basic team formations: OMTs and OTs.

Operational Management Teams (OMTs). The OMT will be a four-person team. Generally the team will be led by a WO; however, in some cases, especially at the operational and strategic level, the team may be led by a civilian CI Special Agent (Military Intelligence Civilian Excepted Career Program [MICECP]). The other team members will be enlisted. The standards of grade for all OMT members are subject to the skill sets and experience required to accomplish the assigned mission.

Example: An OMT at Corps would consist of a CW2, SSG, SGT, and a junior-enlisted soldier; whereas an OMT for a strategic element may be a CW4/GS-14, a SFC, SGT, and one junior-enlisted soldier, with three enlisted.

OMTs will provide operational guidance for 1 to 4 OMTs, depending on mission focus and OPTEMPO. When two or more OTs are deployed in DS of a maneuver element, an OMT will also be deployed to provide technical control. The OMT will work closely with the supported S2, 2X, and Analysis and Control Team (ACT) to furnish current threat information and answer the supported commander's PIRs and information requirements (IRs). OMTs will coordinate with the supported *2X and manage subordinate operational CI and HUMINT teams to—

- ❑ Provide guidance and technical control of operational activity.
- ❑ Provide collection and operational focus for all subordinate operational CI and HUMINT teams.
- ❑ Provide quality control and dissemination of reports for subordinate operational teams.
- ❑ Conduct single-discipline analysis and assist in mission analysis for the supported commander.
- ❑ Act as a conduit between subordinate operational teams, the

*2X staff, and supported unit headquarters.

- ❑ Provide administrative support for subordinate operational teams to include reporting mission and equipment status to the *2X staff and the supported unit headquarters.
- ❑ Educate the supported commander on the capabilities of the OMT and operational CI and HUMINT teams.
- ❑ Integrate the CI and HUMINT teams directly into the maneuver commander's reconnaissance and surveillance (R&S) planning.

Operational Team (OT). OTs will be a four-person team. CI OTs will consist of three NCOs and a junior-enlisted soldier. A HUMINT OT will consist of two NCOs and two junior-enlisted soldiers. At the operational and strategic level civilians may be inserted into this structure, as appropriate. The standards of grade (SOG) for all OMT members are subject to the skill sets and experience required to accomplish the assigned mission. OTs will be trained to execute the full range of functions for the discipline of the team. CI and HUMINT OTs will be discipline pure, but may be task-organized by the commander as required. Some specialized OTs may require additional

advanced-level training prior to personnel being assigned to the team. For example:

- ❑ CI: Technical Surveillance Countermeasures (TSCM), Polygraph.
- ❑ HUMINT: Media Exploitation (document exploitation [DOCEX], strategic debriefing).

DOCTRINE

CI and HUMINT regulations and doctrinal manuals are out of date and are scheduled for revision to include the recommendations established in the ICT. AR 381-20 and AR 381-100 are currently under revision. Field Manuals 34-60 and 34-52 are scheduled to be revised; however, operational deployments have impacted the ability of the USAIC&FH Doctrine Division to resource this requirement.

Updates of both discipline manuals will include doctrine on the roles, responsibilities, and functions of the *2X staff. This will standardize the *2X positions and provide personnel and organizations assigned to *2X staffs the tools to successfully execute Army, joint, and combined CI and HUMINT operations.

TRAINING

Today's CI and HUMINT training has been modeled on the tactical merger of CI and HUMINT elements in ECB organizations with the focus of training on HUMINT-oriented

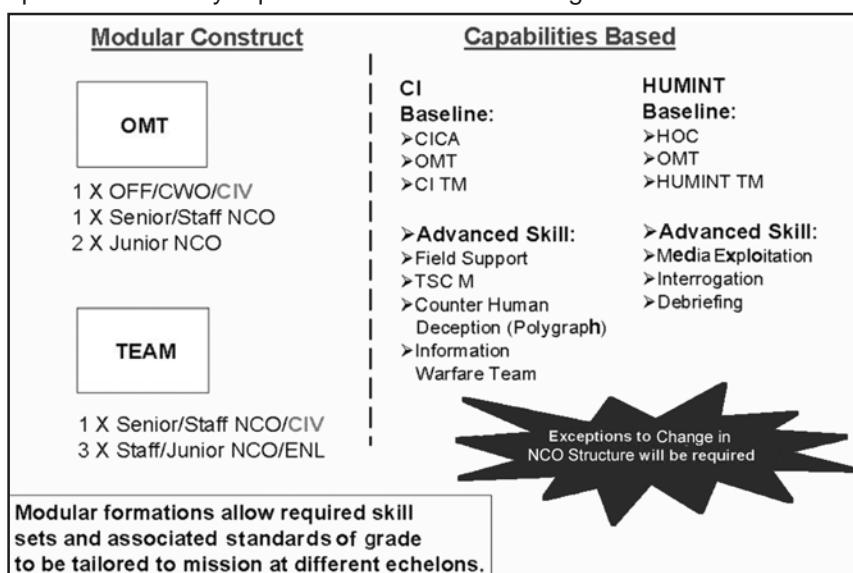


Figure 5. Building Blocks for Force Structure.

source operations. This training model has reinforced the perception that CI and HUMINT are one and the same or interchangeable. This training has been beneficial for HUMINT soldiers whose previous training focused primarily on interrogation skills. However, this training model has overshadowed the investigative skills necessary for CI personnel. Changes in training have to be made to reorient the focus of both disciplines. Changes recommended by the ICT require the establishment of a new Critical Task Site Selection Board (CTSSB) to validate proposed Critical Task Lists (CTLs) developed during the course of the ICT. DCS G2 and CG, USAIC&FH, have forecasted the implementation for the new CI and HUMINT courses in fiscal year 2006. This will coincide with projected implementation in personnel requirements initiated by the Military Occupation Classification and Structure (MOCS) package submitted to PERSCOM by OCMI.

□ 97E/HUMINT. The new HUMINT course will provide training in HUMINT specific skills such as basic interrogation and debriefing skills. The course will also address common skills used by both the HUMINT and CI disciplines. These skills consist of interpersonal communications, interviewing, report writing, source operations, etc. Students will consist of all HUMINT IET soldiers.

□ BCISAC. The BCISAC will be an all-ranks (military and civilian) course focused on CI investigative and operational skills.

□ 2X Course. Another training goal is to establish a 2X course. The ICT concluded that the current J2X course sponsored by CI Field Activity (CIFA), while a good overview, does not adequately train and prepare officers, warrant officers, and NCOs for assignment to Army, joint, and combined 2X staff management positions. The ICT recommended the establishment of a proponent (USAIC&FH) course to teach stu-

dents how to serve in a 2X staff position. The goal is to institutionalize the 2X staff and standardize the roles, responsibilities, and functions rather than to staff ad hoc and use the trial-by-fire training method.

The Army provides the majority of all CI and HUMINT assets and 2X staff personnel supporting joint and combined operations. This fact, coupled with the adoption of the 2X concept throughout the Army, makes the 2X course a necessity. Although the target audience for the 2X course are Army NCOs, WOs, officers, and civilians serving in Army, joint, or combined 2X positions, a two- to three-week course would be beneficial to sister services as well as national agencies supporting contingency operations. (See Figure 6.)

LEADER DEVELOPMENT

In today's NCO Education System (NCOES) and WO Education System (WOES), technical training does not keep pace with changes in emerging tactics, techniques, and procedures (TTPs) and technology. While leadership and staff managerial skills are important, more emphasis needs to be placed on the technical competence of NCOs and WOs. Currently the only technical training within NCOES and WOES occurs

in basic-level courses such as Basic NCO Course (BNCOC) and WO Basic Course (WOBC). All other advance courses do not include MOS-related TTPs or technically focused training.

With emerging technology, fielding of systems and especially the Army Transformation Campaign Plan, this is a critical shortfall, which must be addressed in courses like Advanced NCO Course (ANCOC) and WO Advanced Course (WOAC). This is especially true for WOs who are considered the technical experts in their fields, but receive significantly less professional development than NCOs or commissioned officers.

MATERIEL

Unlike the other intelligence disciplines (imagery intelligence, signals intelligence, measurements and signatures intelligence, and technical intelligence), CI and HUMINT obtain information through human interaction and not through the capture of data from the electromagnetic spectrum. All materiel and equipment requirements for CI and HUMINT are used to process and report information (e.g., CI and HUMINT Automated Tool Set [CHATS] communications) or to support unique skills (e.g., polygraph, TSCM) and not the collection of in-

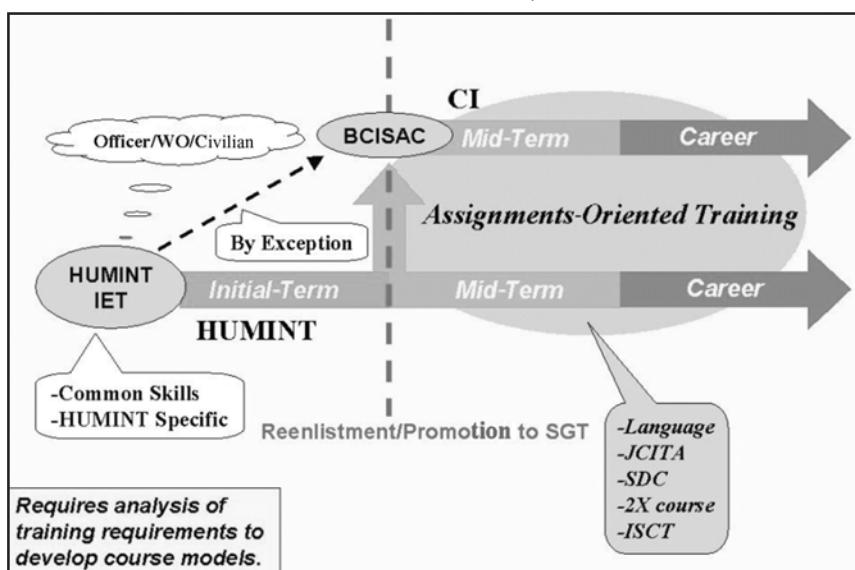


Figure 6. Proposed Training Model.

formation. However, emerging technologies will continue to enhance the basic capabilities of the individual CI and HUMINT soldier by creating faster information processing, data mining, information dissemination, and archival.

As we move to a network-centric force, future CI and HUMINT support systems will have to keep pace with joint interoperability requirements. This is especially true with the DOD mandated requirement to establish the Distributed Common Ground System (DCGS), which is not only multiservice interoperable but also must be interoperable within the joint, inter-agency, and multinational (JIM) environment.

Conclusion

In recent deployments, and especially with the Global War on Terrorism, CI and HUMINT have been the most deployed intelligence collection asset to support maneuver elements in contingency operations. Contingency operations in under-developed, third-world nations with limited infrastructure often diminish the effectiveness of other technically focused intelligence platforms. In these environments, combat commanders have recognized the value of CI and HUMINT as their eyes and ears on the battlefield.

However, senior leaders and commanders are easily mesmerized by

- AR 381-20, The Army Counterintelligence Program, 15 November 1993.
AR 381-100, Army Human Intelligence Programs, 15 May 1988.
AR 614-200, Enlisted Assignments and Utilization Management, 30 April 2003.
DA Pam 351-4, U.S. Army Formal Schools Catalog, 30 October 1995.
DA Pam 600-8, Management and Administrative Procedures, 1 August 1986.
DA Pam 611-21, Military Occupational Classification and Structure, 31 March 1999.
FM 34-52, Intelligence Interrogation, 28 September 1992.
FM 34-60, Counterintelligence, 3 October 1995.
Joint Publication 2-01, Joint Intelligence Support to Military Operations, 20 November 1996.
Title 50, War and National Defense.

the visual (i.e., Light Emitting Diode [LED] displays, digitized maps, satellite and unmanned aerial vehicle [UAV] imagery, and PowerPoint presentations). They are often willing to expend a significant amount of resources to have a new system or gadget. At the same time, even while the OPTEMPO for CI and HUMINT continually increases, there has been no commensurate increase in dedicated resources for manning, training, and/or equipment. The length of CI and HUMINT training courses continues to be cut; our instructor and doctrine writer positions go unfilled; and mis-utilization of our CI and HUMINT soldiers force valuable and scarce assets from our ranks. CI and HUMINT must be prop-

erly trained, equipped, and organized in order to successfully transform and meet the challenges in the Army's OF.



CW3 Larry Norris is currently assigned as a Combat Developer, CI and HUMINT Team, Requirements Branch, Directorate of Combat Developments, U.S. Army Intelligence Center and Fort Huachuca. His last assignment was as the Regimental CI Technician, 75th Ranger Regiment, Fort Benning, GA. CW3 Norris has also been assigned to 519th MI BN (Tactical Exploitation) with deployments to Haiti and Bosnia; 902d MI Group, White Sands Missile Range; 5th Infantry Division, Fort Polk, LA; 3d Aerial Exploitation BN and 524th MI BN, Republic of Korea. Readers may contact the author via E-mail at larry.norris@us.army.mil and telephone at DSN 879-7217.

ATTENTION READERS

Send us your articles, photos, book reviews, and letters to the editor. If you have any experience you can share on MI doctrine, professional development, or "how-to" tips, please send them to us. Recurring themes and topics for issues include Intelligence, Surveillance, and Reconnaissance (ISR), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Global War On Terrorism (GWOT), observations and lessons learned, Operation Enduring Freedom (OEF), Operation Iraqi Freedom (OIF), and tactical operations. Please email them to mipb@hua.army.mil or mail to ATTN ATZS-FDT-M, US ARMY INTELLIGENCE CENTER AND FORT HUACHUCA, 550 CIBEQUE STREET, FORT HUACHUCA, AZ 85613-7017. Information on how to submit articles appears on the last page of this issue.

Al-Qaeda Threat to Oil Industry and U.S. Allies

by Ben N. Venzke
and Aimee Ibrahim

Copyright 2002 IntelCenter/Tempest Publishing, LLC, All Rights Reserved—Permission to redistribute this report in its complete form, including this notice, with proper attribution to IntelCenter (<http://www.intelcenter.com>) may be obtained by emailing info@intelcenter.com. Permission must be obtained in writing before redistributing the entire report or any portion of it.

ASSESSMENT

Attacks during the past seven months against the Germans in Tunisia; French in Pakistan and Yemen; and Australians in Indonesia have illustrated al-Qaeda's current primary focus on targeting the major allies of the United States (U.S.) in its campaign in Afghanistan. While there have been attacks against U.S. forces in Kuwait and the Philippines, it is our opinion that the current primary focus is U.S. allies.

On 9 October 2002, Ayman al-Zawahiri said in a newly released video, "We have sent some messages to the allies of America so that they may stop their involvement in its Crusade. The mujahideen youth have issued messages to Germany and another one to France. So if this is not enough, then we are prepared to increase it by the help of Allah." This current focus does not, however, alleviate the threat against U.S. interests either within U.S. borders or abroad.

It is our strong opinion that long-term pre-11 September 2001 plans for another major attack designed to match or supersede the 11 September 2001 attack will be executed when al-Qaeda believes it is most advantageous to do so. An assessment on the most likely window for

such an attack within the continental United States (CONUS) is included at the end of this report.

Without addressing threats to U.S. targets, we believe there exists a significant threat of additional attacks against the oil industry as well as U.S. allies. Specifically:

- ❑ Tankers transiting oil shipping lanes, particularly the Arabian Gulf and Horn of Africa areas, are under a high risk of attack. The threat from al-Qaeda is not limited to shipping lanes but also includes ports, loading/off-loading facilities and even support infrastructure located inland. This is emphasized in the 13 October 2002 statement from al-Qaeda's Political Bureau which said, "The operation of attacking the French oil tanker is not merely an attack against a tanker—it is an attack against international oil transport lines and all its various connotations."
- ❑ German, French, and Australian interests both within and outside their geographical borders will remain threatened. However, we believe that an even greater risk exists to U.S. allies not previously attacked, such as the United Kingdom (UK) and Canada. While arguments within the Islamic extremist community exist against targeting countries such as the UK, it cannot be presumed that this position will dominate the debate. There also exists a significant threat to Saudi and Jordanian interests.

Note on Dual-Purpose Targeting:

The three attacks against U.S. allies have all served dual targeting interests (i.e. Germany/synagogue, France/oil, Australia/tourism). It can

be expected that al-Qaeda will continue to seek dual-purpose targets whenever possible.

Note on Afghanistan and Pakistan:

Over the course of the past 10 months there has been a steady stream of al-Qaeda-affiliated attacks in Afghanistan and Pakistan against U.S. and allied interests. Due to the political environment in these two countries, those operations have been excluded from consideration in this assessment. However, the 8 May 2002 bombing operation in Karachi, Pakistan, which resulted in the death of a number of French nationals, may be considered as another significant operation against a U.S. ally if it is concluded that the prime target was the group of French nationals, rather than the Sheraton Hotel.

ATTACKS AGAINST U.S.

ALLIES

Australia

Around 2330 local time on 12 October 2002, two suspected car bombs detonated next to the Sari Club and other nightlife establishments on Kuta Beach in Bali, Indonesia. At least 187 people were killed and at least 300 injured. The majority of the victims were Australians and other foreign nationals.

Germany

On 11 April 2002, al-Qaeda member Nizar Sayf-al-Din crashed a fuel tanker into the Ghriba Synagogue in Djerba, Tunisia. Nineteen people were killed, including 14 German tourists.

France

On 8 May 2002, a car bomb in Karachi, Pakistan, detonated next to a bus carrying French naval engi-

neers. Fifteen people were killed, including 11 of the French engineers. Al-Qaeda is suspected of being involved in the attack.

On 6 October 2002, a boat packed with explosives rammed into the French-owned tanker Limburg as it headed into the port of Ash Shihr at Mukallah, Yemen, to bring on more oil. The crew abandoned ship at 1200 local time [0900 Greenwich Mean Time [GMT]] when they were unable to put out the ensuing fire after the blast.

The ship is managed by the French Ship Management Company and owned by Euronav. France Ship Managing Director Peter Raes stated: "A junior officer saw a craft approaching the Limburg. He was of the opinion that we touched that craft and then there was an explosion." Raes went on to say that the ship, which was built in 2000, is a double-hulled tanker that was barely moving at the time of the explosion. He said the blast/impact penetrated through both hulls and 7 to 8 meters into the cargo hold filled with crude oil. One member of the crew was killed. The ship lost 90,000 gallons of oil after the blast. According to a 10 October 2002 report in *Asharq al-Awsat*, the newspaper received a statement from the Aden-Abyan Islamic Army claiming responsibility for the attack.

On 14 October 2002, a 4-page Arabic statement from Osama bin Laden dated 12 October began circulating in *jihadi* circles. In the statement, bin Laden refers to the 8 October attack on U.S. Marines in Kuwait and the attack on the Limburg. He says, "We congratulate our Islamic nation for heroic and brave *jihadi* operations that were undertaken by its justified mujahideen sons in Yemen against the crusader oil tanker and in Kuwait against the invading forces and the American occupation. By hitting the oil tanker in Yemen, the

mujahideen hit the secret line, the provision line and the feeding to the artery of the life of the crusader's nation. They reminded the enemies of the heaviness of the blood bill and the enormity of losses, that they will pay a high price for the continuation of their aggression on our nation and their plunder of our good and our wealth."

STATEMENT FROM AL-QAEDA'S POLITICAL BUREAU – DRAFT ENGLISH

"Statement from the al-Qaeda organization regarding the explosion of the Christian oil tanker in Yemen," dated 13 October 2002, released in wide circulation on 15 October; translated by Aimee Ibrahim.

After the United States and its Christian allies had assumed that they had suppressed the hazard of the mujahideen and secured their strategic, military, and commercial interests in the region and deluded themselves and their people domestically, and the world, internationally; and after giving deception and treachery to the regime in Yemen and everything was done to catch, pursue, and detain the Muslim mujahid youth in Yemen; and we have experienced the passage of a complete full year since the Christian world war against the jihad of the mujahideen throughout the world, and the passage of two full years since the attack on the American destroyer, the USS Cole, in the Yemeni port of Aden (sic).

At this time, and in Yemen specifically, close to where the destroyer exploded at Aden and at a close distance to Bab al-Mandab which is of strategic importance, the mujahideen attacked anew at a strategic Christian target. Attacking a commercial target of this size, at this time, under these circumstances, and in this way has more significance and meaning. For it means:

1) All the military, security, and political, etc., efforts that America and its allies have done to protect their strategic interests in this area have been futile.

2) The mujahideen by the grace of God, no longer have restraints on action and are capable of surprising their enemy and [carrying out] attacks that are decisive, lethal, and strategic and in the appropriate time and place they determine.

If al-Qaeda were the entity that carried out that attack or if it were another of the mujahideen bases that adhere to the same ideology, thought and methodology, both assumptions are disfavorable with respect to the Americans and their Christian allies. Because, the assumption that al-Qaeda is the one that carried out the attacks means, first, that al-Qaeda remains strong, and is able to attack in the same place in which it attacked before; [translation uncertain: and all the international horrors the Americans are known for in what they call their "war on terrorism" and their unusual successes in "uprooting terrorism, its leaders, its bases and its roots" is merely (propaganda) and their deceptive words will go up in the first cloud of smoke rising from the ship.]

And if it were mujahideen other than al-Qaeda that carried out the attack, then the situation is graver because that simply means that the Qaeda that is led by Sheikh Osama bin Laden is only one base of the many bases that are prevalent in this Ummah. So America and its Christian allies should strongly heed this.

So that we don't grant a complimentary security consultation to the enemy, we won't specify which assumption is the correct one, but we leave [the enemy] to drown in all the assumptions and possibilities that have arisen in the two years without arriving at anything in the case of the attack against the destroyer, the USS Cole.

3) Likewise, the operation revealed the true danger the mujahideen pose to the strategic, commercial, and military interests of the enemy.

If a boat that didn't cost US\$1,000 previously managed to ruin a destroyer worth over US\$1 billion, and its symbolic value cannot be measured, and a similar boat managed to devastate an oil tanker of that magnitude, so imagine the extent of the danger that threatens the West's commercial lifeline which is petrol. This region sits on the largest [oil] reserves, owns the largest quantities and contains [the industry's] most important passages and lanes.

The operation of attacking the French oil tanker is not merely an attack against a tanker—it is an attack against international oil transport lines and all its various connotations.

4) And beyond the security, military and commercial significance, the attack carried a strong political message to the alliance of Washington and its enemies in their war against the Islamic nation—that they will never be far away from the hand of God's retaliation through the mujahideen.

(Additional text praises Yemenis for their bravery and courage.)

[Signed]

Political Bureau of the Organization of al-Qaeda al-Jihad, Sunday 6 Sha'ban 1423h 13 October 2002.

AL-QAEDA'S NEXT ATTACK WITHIN CONUS

Assessment

The assessment reflects what the Intelligence Center currently views as the most likely scenario for the next attack by al-Qaeda within CONUS. The points are by no means concrete rules that al-Qaeda will necessarily abide by and consequently need to be viewed in their appropriate context. Al-Qaeda's tactical and targeting options are numerous and varied,

and security planning must therefore remain flexible.

The assessment is based on our analysis of previous al-Qaeda operations, statements, and other information.

Time Frame

0800 - 2100 ET - Monday - Friday - August-December

Notes:

Major al-Qaeda operations have historically occurred between August and December, and on average have been spaced apart by about one year.

The exception for the time frame would be for attacks aimed at special events or other circumstances which would necessitate a variation, such as an attack against a military housing facility (where an evening attack would be more effective).

Targets

Financial institutions or targets against which a successful attack would have a perceived financial impact—Government facilities, especially those with a high-profile or those serving a critical function.

Notes:

The most likely targets will be those that allow for flexibility in attack execution. One-time events or events for which there is a small window of opportunity are less likely to be hit than targets that can be hit any day of the week with equal effect.

Tactics

Piloted vehicular assault like the 11 September 2001 operation (may utilize planes, boats, trucks, or other vehicles)—Large vehicular bombing.

Notes:

There is a high probability that either tactic will involve multiple, simultaneous attacks against geographically separated targets.

If al-Qaeda has successfully obtained chemical or biological weap-

ons, a dirty device or a nuclear weapon, there is a high probability it will attempt to use it.



Ben Venzke is the founder and CEO of IntelCenter which provides intelligence support to the intelligence, law enforcement, military and security communities. He has been working for the past 14 years to create professional-level intelligence products that place timely, actionable intelligence into the hands of those who need it, whether it is an operator prepping to perform an entry, an analyst sitting at Langley, or a chief of police attempting to assess the threat to his or her city. Mr. Venzke has recently co-authored "The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics & Targets," which has provided readers for the first time in a publicly available format the ability to see what al-Qaeda has said in its own words about targets and tactics. Counterterrorism mission has been his core focus for the past eight years. While running IntelCenter and its sister company Tempest Publishing, Mr. Venzke has managed intelligence products at Jane's Information Group where he worked as an Editor and iDEFENSE where he was the Director of Intelligence Special Projects. He also spent two years as Pinkerton Global Intelligence Service's senior consultant for the Middle East and Africa. He can frequently be seen appearing on CNN, MSNBC, and NBC. Readers may contact Mr. Venzke via E-mail at bvenzke@intelcenter.com.

Aimee Ibrahim is currently an associate at Community Research Associates where she works on projects designed to help the first responder and military communities deal with terrorist attacks. She also collaborates with IntelCenter on terrorism intelligence issues and is the co-author of "The al-Qaeda Threat: An Analytical Guide to al-Qaeda's Tactics & Targets." Readers may contact her at aibrahim@intelcenter.com and telephonically at (703) 370-2962 or Fax (703) 370-1571.

Commentary: Don't Let Terrorists Spread Fear

by John W. Davis
(Major, U.S. Army, Retired)

A copy of this article first appeared in *Army News Service*, 25 March 2003, and is republished with permission of the author.

Shortly after police alerted the nation that a vehicle license plate was being sought in connection with the D.C. sniper, a citizen reported it, and an arrest was made. The alleged killer was off the street.

Recently, a waitress at a Shoney's Restaurant in Georgia notified authorities of an apparent criminal discussion she overheard. Three men seemed to be planning to bomb a building in Miami. After police investigated, the bomb plot was alleged to be a hoax. In both cases, these citizens did what any civic-minded American should do. They reported a threat to the proper authorities. Such acts are our civic duty.

Not long ago my dad and I were comparing the surprise attack on Pearl Harbor with the suicide assaults on the World Trade Center and the Pentagon. "Something a lot of people don't remember about those days," he reflected, "is that Americans were afraid. There were rumors across the land that Japanese had landed in San Francisco, at Los Angeles, and that saboteurs and spies were everywhere. Rumors spread fear, and fear fanned more fear."

The greatest human emotion is fear, and the greatest fear is fear of the unknown. It was for that very reason that President Roosevelt reminded everyone that, "The only thing we have to fear is...fear itself." "You can't imagine what a calming

effect the president's reassurance had for everyone," dad said. "We were sucker punched at Pearl, but pulled together for the fight to come. We believed the situation was dangerous, but that the right people were doing their best to take care of the nation. And it wouldn't be over till we finished it."

Today we too might believe the enemy appears to be everywhere. He seems capable of any number of horrific means of visiting destruction on us. We feel helpless to defend ourselves against an adversary we can neither see, nor identify, nor anticipate. We feel an unspecified dread. We don't feel safe anymore. That is just what the enemy wants us to feel. My favorite quotation came the day after the September 11 attack. A German investigator, asked to comment on the apprehension of several al-Qaida terrorists in Hamburg, offered this matter-of-fact observation, "Don't forget. These people are criminals. Each of these terrorists has a face, a name, and an address."

That comment, echoing President Bush's determined assurance that we will patiently but relentlessly pursue these killers anywhere they may hide, did much to reassure Americans. But how, Americans ask, can we take part? We want to pull together, so what do we do? The answer has been here all along; we've known it intuitively, but never until now really had an immediate need in this generation to act upon it.

Working for the government, we know that loose lips sink ships. But now we know that our eyes catch spies...and the criminal killers they report to. Each of the terrorists has

a face, a name, and an address, and now they too know fear. Their leaders have abandoned them, world law enforcement is seeking them, and every day more Americans become more astute in what to watch for and report. There are many practical hurdles to overcome, and the road won't be easy. Whereas yesterday we weren't aware, today we know who to call if something just doesn't seem right. We help each other. Americans are pulling together. We watch our surroundings in ways we didn't before.

We are protecting ourselves, informing ourselves, and not letting fear defeat us before we've entered the fight. No one today will turn away if a security problem seems to require a solution. We offer assistance to others and make sure someone takes action to protect us. If we see a better way, we speak up.

The only thing we have to fear is fear itself. Remember that every terrorist has a face, a name, and an address. We'll get them if we help each other. We are a quarter billion Americans whose eyes are watching in restaurants, at gas stations, in the office, and on the road. Now the cowards who murdered our people really have something to fear. We are out to get them.



John Davis is a retired US Army intelligence officer, currently employed as a civil servant at the US Army Space and Missile Defense Command, Huntsville, AL, as an intelligence specialist. Readers may contact him at john.davis@smdc.army.mil, or (256) 955-1727.

Doctrine Corner

U.S. Army Intelligence Center and School Requirements for Lessons Learned

by CW5 Clyde Green and CPT Kevin J. McGuire

Recognizing the need to incorporate lessons learned, at all echelons, regarding all functions (e.g., processes, equipment functionality, procedures, etc.), below are some of the general themes and specific requirements for collecting lessons learned from Operation Iraqi Freedom (OIF). These themes and requirements will be used by the U.S. Army Intelligence Center (USAIC) subject matter expert (SME) supporting the Center for Army Lessons Learned (CALL) Combined Arms Assessment Team (CAAT) as a guide to facilitate collection of initial intelligence lessons learned during OIF. These lessons learned will be used to—

- Validate current doctrine and assist in the development of emerging and/or new doctrine.
- Validate current systems and assist in the upgrade of those systems.
- Assist in the development of future individual and collective training.

The following are general and specific doctrinal requirements developed by Doctrine Division, USAIC, to assist in the collection of lessons learned during OIF.

DOCTRINE	If organizations and users could change 1 or 2 things in doctrine, what would those be?
JOINT INTELLIGENCE OPERATIONS AND INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) INTEGRATION	1. How effective was the lash-up to Combined Air Operation Center (CAOC)? 2. Were Army requirements and Joint Forces Land Component Commander and Staff (JFLCC) requirements adequately pre-addressed (conflict and during combat operations)?
REACH OPERATIONS	1. Were reach operations conducted at all echelons (i.e., specifically at the lowest echelon)? 2. How was connectivity established and maintained? 3. How useful was reach (i.e., was it timely, accurate, and what was the quality of the information obtained)? 4. What type of intelligence and/or information was provided? 5. Was it from the Information Dominance Center (IDC) or Home Station Operations Center? 6. What type of Intelligence and/or information was provided by the IDC? 7. Is the 513th MI Brigade (Bde) (supporting U.S. Army Central Forces Command [(ARCENT)]) actually testing the Home Station operational concept? If so, what were the procedures? How well did it work?
INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS (IO)	1. How were affects and effects assessed? 2. What were the Intelligence procedures for support to IO? 3. How did the various Division and Corps Analysis Control Elements (ACEs) divide their analytical efforts (e.g., close, deep, rear, threat battlefield operating system (BOS), decisive, shaping, and sustaining)?
HUMAN INTELLIGENCE (HUMINT) AND COUNTERINTELLIGENCE (CI) OPERATIONS	<input type="checkbox"/> Comments and observations
PROPHET	Did divisions use PROPHET? If so, how often, when, and how was PROPHET employed during extended road marches, movement to contact, and combat operations?

INTELLIGENCE SUPPORT TO SPECIAL OPERATIONS FORCES (SOF), INCLUDING PSYCHOLOGICAL OPERATIONS (PSYOP) AND CIVIL AFFAIRS (CA)	<input type="checkbox"/> Comments and observations
INTELLIGENCE SUPPORT TO TARGETING, INCLUDING— <input type="checkbox"/> SOF <input type="checkbox"/> FIELD ARTILLERY (FA) <input type="checkbox"/> JOINT AIR UNMANNED AERIAL VEHICLE (UAV) OPERATIONS <input type="checkbox"/> BATTLE DAMAGE ASSESSMENT (BDA)	<input type="checkbox"/> Comments and observations
INTELLIGENCE SUPPORT TO FORCE PROTECTION (FP)	<input type="checkbox"/> Comments and observations
INTELLIGENCE SUPPORT TO URBAN OPERATIONS, INCLUDING INTELLIGENCE PREPARATION OF THE BATTLEFIELD (IPB) ANALYSIS	1. Was IPB automated? 2. Collection and analysis—strengths and weaknesses noted?
INTELLIGENCE SUPPORT TO STABILITY OPERATIONS AND SUPPORT OPERATIONS	<input type="checkbox"/> Were stability operations and support operations requirements integrated at times when units were engaged in combat operations? If so, how were the requirements integrated?
GENERAL INTELLIGENCE OPERATIONS AND THE INTELLIGENCE ESTIMATE (WITH EMPHASIS ON PREDICTIVE ANALYSIS)	1. Was the Intelligence Estimate continuous? 2. Was the Intelligence Estimate automated? 3. Was the Intelligence Estimate implemented as an Intelligence Running Estimate? 4. What products were most useful? 5. How did intelligence elements support each command post element (echelons)?

The following questions were developed by New Systems Training and Integration Office (NSTIO) to assist in the collection and performance of deployed Military Intelligence (MI) systems:

GENERAL QUESTIONS	1. What tactics, techniques, and procedures (TTPs) needed improvement to better meet mission requirements? 2. Were there significant shortfalls in Institutional training? 3. Are there any changes recommended for military occupational specialty (MOS) or officer courses?
GROUND SYSTEMS	1. How did Prophet maneuver with the Brigades in 3d Infantry Division (ID), and was it effective? Was it utilized in a direct or general support role? 2. Where was the Prophet Control systems emplaced and did the communications function correctly? What were the average communications ranges between Prophet and Prophet Control? 3. What types of targets was Prophet unsuccessful against? 4. Could Prophet and Prophet Control keep pace with the battle? 5. Was crew size for Prophet and Prophet Control adequate?

	<p>6. How were Prophet and Prophet Control incorporated in the maneuver of 101st ID (Air Assault)?</p> <p>7. How was Prophet employed in urban operations?</p> <p>8. What were the system failures?</p> <p>9. What did Prophet and Prophet Control do well?</p> <p>10. How often were 98G's able to utilize their language skills? What percentage of intercepted communications were enciphered/encrypted or frequency hopping vice plain text?</p> <p>11. How well did leadership understand capabilities and limitations of the Prophet? What were the primary misconceptions? What was the impact of the Prophet on providing support to intelligence operations and/or targeting?</p>
COMMON GROUND STATION (CGS)	<p>1. What was the most useful portion of the CGS NET they received? Explain how it helped them perform their missions?</p> <p>2. What is the one thing or area units and/or individuals could have most used training on (regarding CGS NET) prior to their deployment that would have most benefited them in the area of responsibility (AOR)?</p> <p>3. What works as advertised and what did not? What work-arounds were employed for problems and how were they implemented? Were there any hardware/software problems that severely or moderately impacted operations?</p> <p>4. Were on-the-move operations used with the CGS? Was satellite communication (SATCOM) reliable for providing a moving update of the "now" battlefield picture? Were there problems with generator power while hauling? Are there concerns, incidents, or suggestions regarding lack of ability to ground generator under these conditions?</p> <p>5. What interfaces were used most frequently? At each level (i.e., Brigade, Division, etc)? What were they tasked for? At what level? How effective were they? What types of data were shared and/or transmitted? How were they connected to the CGS (hardwire, digital via Single Channel Ground and Airborne Radio System [SINCGARS], SATCOM, ultra-high frequency, etc.)?</p> <p>6. How well did signals intelligence (SIGINT) work? Did any particular IBS work better than the others?</p> <p>7. Was all required Crypto/Communications Security (COMSEC) material available on a timely basis? If not, why not?</p> <p>8. Did you have adequate standing operating procedures (SOPs) prior to deployment? Can we have a copy for use and reference?</p> <p>9. How well did leadership understand capabilities and limitations of the CGS? What were the primary misconceptions? What was the impact of the CGS on providing support to intelligence operations and/or targeting?</p> <p>10. How was the CGS used when Joint Surveillance Target Attack Radar System (JSTARS) flights were not available?</p> <p>11. Are there any special maintenance requirements needed to keep the CGS operational?</p>
ALL SOURCE ANALYSIS SYSTEM (ASAS)-REMOTE WORK STATION (RWS)	<p>1. How is the interoperability? (Are they talking to each other?)</p> <p>2. Is the system locking up often?</p> <p>3. Are they using the system for IPB/Military Decision-Making Process (MDMP)?</p> <p>4. Are they still using markers, maps, and overlays?</p> <p>5. Are the systems able to handle the message loads?</p> <p>6. Is the sand wreaking havoc on the systems?</p> <p>7. What ASAS-RWS related TTPs have they been developed? Refined?</p> <p>8. Who are the boxes talking to?</p> <p>9. What are their mission threads?</p> <p>10. What are their workarounds if something is not working?</p>

	<ol style="list-style-type: none"> 11. Are their communications up? 12. How often are they sending information? 13. What type of maintenance are they performing? 14. What version and type of ASAS is being used? 15. How is the joint communication package working? 16. What units are using the ASAS-RWS? ASAS-Light (ASAS-L)? ASAS-All Source (ASAS-AS)? ASAS-Single Source (ASAS-SS)?
NATIONAL/TACTICAL EXPLOITATION SYSTEM (TES)	<ol style="list-style-type: none"> 1. Was the user training given by Northrop Grumman upon issue to the unit sufficient to allow operators to effectively employ the system on their own after training? 2. Were service and support contracts given to contractors based on projected system down time and mean time between faults? This in turn influences the number of maintenance personnel and slots allowed in the unit. Has the system performed to the standards set forth in the Operational Requirements Document and its supporting maintenance contract? 3. Due to budgetary constraints facing all systems many contractors have been cutting back their level of Field Service Representatives (FSRs) support. Have units experienced degradation in number of FSRs or availability of FSRs and, if so, how has units worked around this issue? 4. How has your unit worked the issue of support for deployed portions of the system? (Usually there are a specified number of FSRs at a given location; with portions of the systems possibly deployed, the question arises as to how the contractor will support split-based operations).
AVIATION	<ol style="list-style-type: none"> 1. How was the Hunter UAV integrated with ASAS, Advanced Field Artillery Tactical Data System (AFATDS) and JSTARS? 2. How were the Remote Viewing Terminals (RVTs) utilized? Who primarily used them? 3. Were the UAV units able to keep pace with the units they were supporting? 4. What were the greatest challenges for UAV units? For example: Selecting suitable launch and recovery sites? Maintenance? Security? COMSEC? 5. What effects did the desert environment have on the deployment and/or operations? 6. Were the system and its capabilities and weaknesses well understood by the battle captain and therefore utilized to their fullest potential? 7. Primarily what missions were the Hunter and Shadow utilized for? For example: Urban terrain? Searching for high-value targets (HVTs)? Targeting? Air defense pacification? 8. What challenges did the unit have with airspace coordination or getting on the Air Tasking Order? (ATO) or Air Combat Order (ACO)? Did the UAV use blanket altitudes or Restricted Operation Zones (ROZs)? 9. What challenges did the unit have with frequency management? 10. What lessons were learned in reference to coordination between the UAV units and the Tactical Operations Centers (TOCs)? 11. List 5 things that worked well and 5 things that need improvement in UAV operations and/or training. 12. What improvement is needed in current training to support future operations? For example: Payload operation? Target recognition? Command, communications, control, intelligence messaging? Crew coordination? Airspace management? Artillery adjustment, etc? 13. Were the UAVs following a mission profile or were they primarily re-tasked? If they were re-tasked was there a problem with airspace coordination and how was that resolved? 14. What was the primary role of the 350U?

	<p>15. What Identify Friend/Foe (IFF) challenges did the operators/planners encounter?</p> <p>16. What problems did the UAV units have with supply of UAV specific parts and fuel (MOGAS)?</p>
--	--

The following questions were developed to assist in the collection facts about the performance of MI systems and the effectiveness of individual and collective training of deployed personnel:

WHAT WERE THE EFFECTS OF DENIAL AND DECEPTION ON ENEMY FORCES?	
WAS INSTITUTIONAL TRAINING FOR 96DS, 350DS ADEQUATE FOR THE TASKS THAT WERE REQUIRED DURING OIF?	<input type="checkbox"/> Are there additional tasks that were required that had not been institutionally trained? <input type="checkbox"/> Were additional training requirements identified prior to deployment? <input type="checkbox"/> What were they? <input type="checkbox"/> What training materials were required? <input type="checkbox"/> Were they available?
Could use same question for all MI MOSs	
SIGINT ISSUES	<ol style="list-style-type: none"> 1. Were there enough outside continental United States (OCONUS) frequencies for all the MI systems to operate without interference (e.g., UAV, TROJAN, Guardrail, etc.)? <p>NOTE: This is for both the data links and for the rebroadcast to the information to the troops (sensor- to-shooter).</p> <ol style="list-style-type: none"> 2. If there were problems with frequencies management? What actions were taken to correct them? How can we prevent this from happening in the future? 3. Was cross-cueing utilized to verify Intelligence? If so, how complicated was the routing to task other MI resources? How long did it take? 4. What difficulties did the PROPHET system come up against when operating in an urban environment? 5. How well did the embedded linguists work with the Infantry?
SYSTEMS ISSUES	<ol style="list-style-type: none"> 1. What type of systems would have been more beneficial for this type of operation? 2. What type of training would have better prepared our MI Warrants to work more efficiently? 3. How did equipment such as PROPHET, UAV, Hunter, Guardrail, TES, CGS, and Trailblazers operate during this operation (i.e., deployment efficiency, actual reporting time, time on target, etc.)? 4. What urban analytical would have better served our commanders? 5. If you had a tactical SOP, did you use it? If you did not have a tactical SOP, do you think one would have been beneficial?

The following questions were developed by Concepts, Architecture, and Requirements (CAR) to assist in the collection facts about the performance of MI systems and the effectiveness of individual and collective training of personnel deployed to OIF:

ISSUE: ANALYSIS IS A CRITICAL COMPONENT OF OUR POSTURE FOR THE OBJECTIVE FORCE; AND PART OF THIS EVOLUTION IS AN UNDERSTANDING WHERE IT IS BEST ACCOMPLISHED	<ol style="list-style-type: none"> 1. What was the level of effort directed toward analysis at each tactical echelon (Battalion, Brigade, and Division)? 2. How were the results of that analysis made available to the decision makers? 3. What were the primary sources of information that contributed to the analysis effort by echelon?
---	---

ISSUE: THE ROLE OF COLLECTION IS RAPIDLY EVOLVING. WE NEED TO DETERMINE HOW EFFECTIVE OUR CURRENT COLLECTION ASSETS AND PROCEDURES ARE	1. Were there sufficient tactical collection assets to meet commanders' needs? 2. Were collect assets sufficiently mobile to "keep up" with the maneuver forces? (Try to quantify the collection effort in the 3d ID as it raced across Iraq.) 3. What were the primary external sources of information and how was the information from them disseminated to tactical forces?
ISSUE: INTELLIGENCE STAFFS ARE GOING TO BE FLATTENED SIGNIFICANTLY IN THE DEVELOPMENT OF THE UNIT OF ACTION. WE NEED TO GET FEEDBACK ON WHAT WAS EXPECTED OF STAFFS AND THE EFFECT OF AUTOMATION ON THEIR ABILITY TO PERFORM THEIR JOB	1. What was expected from the S2 at Battalion, Brigade and Division? 2. Were there any critical tasks that could not be performed? If there were, what were the reasons those could not be accomplished? 3. What was their primary automation support? 4. Did automation make the tasks significantly easier to perform? 5. What automation assisted capabilities would have made the job easier? 6. Were the staffs sized properly with both numbers and MOS?
ISSUE: LATENCY OF INTELLIGENCE TO COMMANDERS/ LEADERS IS A CONSTANT CONCERN. IT IS ONE WE MUST DOCUMENT TO DEVELOP THE ABILITY TO OVERCOME THE TIME DELAY	1. Was latency of intelligence support a significant problem? Situational Awareness? Targeting? 2. If latency was an issue, what was the primary cause? Communications? Analysis? Processing? 3. What work-arounds were developed to overcome this?
IRAQI DENIAL AND DECEPTION (D&D) AAR (CLASSIFIED SECRET NF WHEN ANSWERED)	1. What Denial and Deception (D&D) TTPs were used by the Iraqi Army? 2. Were dummy/decoy fighting positions used? How were they used in conjunction with real fighting positions? 3. Was derelict equipment (e.g., vehicles, air defense artillery (ADA) launchers, transporter-erector-launchers (TELs), etc.) used? If so, by whom? 4. Were low or high fidelity (multi-spectral) decoys used? If so, what kind of decoy(s) and who employed them? How successful were they in fooling our sensors and/or analysts? 5. Did our analysts have a good understanding (awareness) on how the Iraqis would use D&D? 6. Were any high fidelity (multi-spectral) decoys found that were not used? What type? Who had them? 7. What type camouflage materials were used (multi-spectral, other)? Were they used with decoys? How were they employed? 8. Was communications deception used? By whom? Was it successful? Did it fool our communications intelligence (COMINT) analysts? 9. Was electronic deception (radars) used? By whom? Was it successful in fooling our electronic intelligence (ELINT) analysts? 10. Were our sensors able to discern real from false (decoys, dummy equipment, etc.)? 11. Were radar corner reflectors used? If so, to what purpose? 12. What effect did D&D have on our forces? 13. What future changes should be incorporated into our doctrine or technology to— <input type="checkbox"/> Identify D&D on the battlefield? <input type="checkbox"/> Defeat D&D on the battlefield?

In the next edition of **MIPB**, we will discuss some of these lessons learned gathered from these, and other, questions. Readers may provide their input directly to Ms. Cynthia L. Collard (SFC, US Army, Retired) at Cynthia.collard@hua.army.mil or CW3 Timothy P. McGinty at timothy.mcginty@hua.army.mil.

Proponent Notes

by LTC Eric W. Fatzinger

The development of the professional attributes and technical capabilities of enlisted soldiers, warrant officers, and officers to meet the needs of the Army is accomplished through Proponent-designed career development models for each of our military occupation specialty (MOS) and career fields. In this issue we will discuss some of the more important considerations you should take into account when planning your next career move.

However, a word of caution. While these career development models describe the required schooling, operational assignments, and self-development goals for MI soldiers and officers they are neither sacrosanct nor should they be considered the final word. They are based on Army requirements of the numbers and types of soldiers and officers to be accessed, retained, promoted, schooled, and assigned. They are basic guidance and do not apply to every situation. Nevertheless, if we have learned anything it is that to be competitive for promotion the models do come close. You should strive to diversify your experience by serving in both technical and leadership positions listed in the model appropriate to your MOS for your current or next higher skill level. Ideally, you should serve successfully in the appropriate leadership position at every level.

Enlisted Actions

Professional Development Model. If you are serious about getting promoted, one of the first things you should do is to take a hard look at the Professional Development Model for your MOS. While these Professional Development Models are not designed to be all-inclusive, they are intended to provide direction for career progression and an

insight into the types of training to request at each skill level. The Professional Development Model for each MI enlisted MOS can be found at <http://usaic.hua.army.mil/ocmi/enlisted.html>.

Education. Advances in technology have made distance learning easily accessible, convenient, and self-paced. Computer Based Training (CBT), Distance Learning System, military correspondence and Internet courses, all provided by e-learning (SMARTFORCE), DANTES, etc., can be accessed via Army Knowledge Online (AKO). But, in addition to Noncommissioned Officer Education System (NCOES) schools you will also need to pursue self-development opportunities to be fully competitive for promotion. Block G of the Professional Development Model outlines some of the degrees and certifications recommended to give you a competitive edge in your MOS at different times and stages of your career. Additionally, you may find it useful to visit the U.S. Total Army Personnel Command (PERSCOM) promotions webpage and compare your educational goals with the educational profiles of those noncommissioned officers (NCOs) who have successfully competed for promotions. The educational profiles by MOS, found at <https://www.perscom.army.mil/select/enlisted.htm#snsb>, when taken together with the specific MOS Professional Development Models, are a useful template to help guide you in determining the level of civilian education you should be shooting for at different stages of your career.

Updates to DA Pam 611-21. The latest in changes to job descriptions and standards for all Army MOSs can be found in the most recent updates to DA Pam 611-21, Military Occupational Classification and

Structure. These updates are posted as Notification of Future Change (NOFC) and can be viewed at <https://perscommd04.army.mil/NOFC2.nsf/>. (NOTE: An AKO user account and password will be required to enter the site.) To find the specific NOFC number designator and effective date for a given MOS, go first to <https://www.odcsper.army.mil/pamxxi/secured/mosstructure/mos-charts.asp>.

Upcoming NCO Selection Boards.

The CY 2003 SGM Selection Board is scheduled to begin October 2003. The projected release date for the promotion list is 15 January 2004. To view MI Proponent input to this board or any other recent senior enlisted board, go to http://138.27.35.32/ocmi/EN_Info_portal.htm.

Warrant Officer Actions

Warrant Officer Career Development. The development of the professional attributes and technical capabilities of Army warrant officers to meet the needs of the Army is accomplished through proponent-designed career development models. A model for each career field can be found in DA Pam 611-21, Military Occupational Classification and Structure. These career models are based on the three pillars of leader development and built around institutional training and education, operational assignments, and self-development. The management of warrant officers involves continuous interaction between the individual officer, commanders, proponent schools, the Warrant Officer Career Center, and the Warrant Officer Division, PERSCOM. In many respects, warrant officers are their own career managers. Although Army requirements dictate the final outcome of all career development ac-

tions, the officer can and should expect to participate in all career decisions.

Participation in the career development process is accomplished by volunteering for training and education programs, completing assignment preference statements, pursuing civil education goals, and planning long-range career goals. The key to being involved in career development is to make informed logical decisions and to act on them.

To begin with, warrant officers should ensure that their performance data, assignment history, training and education, and administrative data in the official career management files maintained at PERSCOM are accurate. The official military personnel file (OMPF), the officer record brief (ORB), and the career management information file (CMIF) contain the data from which important career development decisions are made for selection, advancement, assignments, and retention. To establish and act on appropriate career goals, warrant officers should request periodic advice and counseling from commanders, supervisors, senior warrant officers, and PERSCOM career managers.

As the Military Intelligence Warrant Officer proponent, I urge each of you to stay current on forthcoming changes in the Army which could impact your career development. Talk to your commanders, fellow warrant officers, and senior warrant officers to ensure that your military career plans are consistent with Army requirements and goals. Take advantage of education programs such as the Degree Completion Program (DCP) and Post Graduate Intelligence Program (PGIP) to enhance your professional expertise. Ensure that you, your rater, and senior rater are in synch with what is expected of you in accomplishing your mission. You are the technical expert, but the commander has the "big picture." In your career plans, don't duck

the tough and challenging assignments. This will help you grow professionally and ensure that you are prepared to take on the challenges of the next higher grade.

MI Warrant Officer Accession Board.

The last Accession Board remaining this year will be held in September. For that board all MOSSs except 352H and 352J were to have been considered. Therefore, it is now time for interested soldiers to start putting their warrant officer applications together for 2004. MI Warrant Officer Accession Boards for 2004 will be held in January, March, July, and September. Also, in another recent Headquarters, Department of the Army (HQDA) G1 policy change, warrant officer applicants will now be considered three times rather than just two. So, if you or someone you know....previously submitted a package, remember the information must be updated with me to keep the applications current.

Warrant Officer Promotion Boards.

The 2004 CW3/4/5 promotion board will be held in May 2004. As always, if you have questions concerning MI warrant officer career development, contact me via E-mail at lon.castleton@us.army.mil and telephonically at 520-533-1183 or DSN 821-1183.

Officer Actions

Officer Career Maps and Branch Qualification (BQ).

DA Pam 600-3, Commissioned Officer Development and Career Management, was last published 1 October 1998. For better or worse this means that many of the most important aspects of Officer Personnel Management System III (OPMS III) have not yet been fully documented in appropriate Army publications. Plans to update and publish a revised edition of DA Pam 600-3 have been put on hold for the moment pending the appointment of a new panel by the HQDA G1. Nevertheless, as we discussed in the last issue of MIPB, a major effort is being made by MI to clarify the necessary steps needed for Branch Qualification at each rank. These changes further emphasize the need for MI officers to seek both leadership and technical developmental assignments to successfully position themselves for promotion and future command.

BQ for MI Captains. In addition to successfully completing the MI Captain's Career Course (MICCC) and MI Officer Transition Course (MIOTC), for branch detail officers, MI captains also must—

- Successfully command a company or detachment for at least 12 months and
- Serve at least 12 months as a battalion S2, assistant brigade S2, or intelligence staff officer at any echelon.

Certainly, service as a battalion S2 is preferable to most other intelligence staff jobs for a captain but currently there are just not enough primary S2 positions to give everyone a realistic opportunity to serve in one. Nevertheless, the intent is that all MI captains should serve in at least one technically qualifying intelligence job while a company grade officer.

BQ for MI Majors. In addition to the Army required schooling, an MI Officer must—

- Serve as executive officer (XO) or S3 of any battalion or as a division analysis and control element (ACE) chief for at least 12 months and
- Serve as a brigade S2 or intelligence officer at any echelon for at least 18 months.

These changes bring the branch qualification requirements for MI officers in line with the recommendations of the Army Training and Leader Development Panel (ATLDP) and will keep area of concentration (AOC) 35 officers on familiar footing with all other Operations Career Field officers. The key consideration is that

(Continued on page 72)

Distance Learning

Understanding Intermediate Level Education:

How It Differs From The Former Command and General Staff Officer Course

by Neal Bralley, Jim Danley, Dan French, Chuck Soby, and Paul Tiberi (Colonels, U.S. Army, Retired)

By now, all of us should know and understand that Intermediate Level Education (ILE) is the third tier of the Officer Education System, and it is linked directly to Army Transformation.

ILE will produce “field grade officers with a warrior ethos and warfighting focus, for leadership positions in Army, joint, Multi-National, and Interagency organizations executing full spectrum operations.”¹

Quite a mouthful—but what does this mission statement mean to the Army, commanders, and field grade officers? What is this course really about? And how does it differ from the old Command and General Staff Officer Course (CGSOC)?

Noted military historian and author Sir Basil Liddell Hart once said, “Nothing is harder than putting a new idea into a military mind, except removing the old.”

This may account for some of the concern that has been expressed about ILE and where we are going with the education of our officer corps. Let’s first clear up exactly what ILE is and then offer our opinions as members of the faculty teaching ILE.

Three areas are inexorably linked and distinguish ILE from the former CGSOC: population, curriculum, and instructional method.

Population

The most fundamental difference between ILE and the former CGSOC is in the Army’s commitment to providing the best possible ILE to all Army majors.

For CGSOC, the Army used a central selection process to pick the top 50 percent of the majors in each year group to attend the 10-month resident course at Fort Leavenworth. The rest could volunteer for a correspondence program to receive the education and to be competitive for promotion to lieutenant colonel.

Under this system, half of the majors did not get an opportunity to undergo a resident program to develop their technical, tactical, and leadership competencies and skills. Also, Information Operations Career Field, Institutional Support Career Field, Operational Support Career Field, and special branch majors—who only needed the common-core portion of the course—were held “hostage” for the remainder of the ten months.

With ILE, all majors in the Operations Career Field attend the 10-month resident course at Fort Leavenworth. They complete a 3-month common-core course followed by a 7-month Advanced Operations and Warfighting Course (AOWC) to further develop their abilities to conduct full spectrum operations in joint, multinational, and interagency environments; and to develop the requisite competencies to serve successfully as staff officers at division level and above.

Information Operations Career Field, Institutional Support Career Field, Operational Support Career Field, and special branch majors will also receive a resident ILE common-core course experience, but not at Fort Leavenworth. Teaching teams from Fort Leavenworth

have already been sent to Fort Gordon and Fort Lee to instruct the ILE common-core course to some of these students.

Most Reserve Components (RC) majors will receive the ILE common-core course via The Army School System or an upgraded Advanced Distributed Learning program. As the student population attending the resident ILE common-core course and AOWC at Fort Leavenworth increases, the number of RC majors attending the Fort Leavenworth course will also increase.

This approach allows the maximum flexibility to the Army, commanders, and students while providing the best possible ILE to all majors.

Curriculum

A totally revamped curriculum is the second area that distinguishes ILE from the former CGSOC. The school’s competency map, linked directly to the Officer Evaluation Report (OER), codifies the skill set students must demonstrate to graduate ILE.

While this is a new concept for the school, the Army has had this OER for nearly six years, and field grade officers attending the ILE course should have been exposed to these competencies numerous times before their arrival at the Command and General Staff College (CGSC).

The focus of this skill set is on students learning how (versus what) to think, problem solving and decision-making. Students soon realize there are no “school solutions”

to the problems they are presented. For many, this will prove frustrating as instructors make them work through the problems and principally critique the link between identification of the problem and the student's solution.

As long as evolving doctrine is not violated and the basic principles of planning are demonstrated, guess what? You're a go!

This is a tremendous step forward as we now develop field grade officers capable of thinking vice regurgitating answers. The 2001 Army Training and Leader Development Panel officer study identified, among other things, that the Army needs officers who are adaptable and capable of thinking in a fast-paced, constantly changing environment. This is the foundation for learning and, hence, for the curriculum in ILE.

The ILE curriculum consists of a 3-month "common core" course, the aim of which is to prepare field grade officers for service at division, corps, echelons above corps (EAC), land component command (LCC), and joint staffs. Graduates will—

- Understand full spectrum operations in today's environment.
- Know how to think.
- Understand complex problem solving.
- Be able to balance focus between current and future operations.
- Understand staff principles and concepts.
- Know how to synchronize effects on the battlefield.
- Understand performance-oriented training and education.

The 7-month AOWC that follows is designed to develop Operations Career Field officers with a warfighting focus for battalion and brigade command who are capable of conducting full spectrum operations in joint, multinational, and interagency environments and who have the requisite competencies to serve successfully as division

Blocks of Instruction

- Foundation of Critical Reasoning and Leader Assessment and Development
- Strategic Fundamentals
- Operational Fundamentals
- Tactical Fundamentals

F
O
R
C
E

L
E
A
D
E
R
S
H
I
P

H
I
S
T
O
R
Y

M
A
N
A
G
E
M
E
N
T



through EAC staff officers. Students complete the AOWC with a deeper understanding of full spectrum operations in the contemporary operating environment, including battlespace appreciation, component roles and responsibilities, shaping, decisive and enabling operations at the tactical level, asymmetric operations, and urban operations.

Four blocks of instruction comprise the 3-month ILE common core: Foundations of Critical Reasoning and Leader Assessment and Development, Strategic Fundamentals, Operational Fundamentals, and Tactical Fundamentals. Three parallel courses are integrated into the instruction: Leadership, History, and Force Management.

A series of exercises are used to evaluate the students' mastery of the concepts taught during the ILE Common Core Course and AOWC. These exercises are conducted at section level; so 64 students do all the planning and execution, as well as manage the opposing forces and white cell for each exercise. The scenario places them in a joint, combined, highly complex environment with numerous opportunities to identify and solve problems.

The benefit here is that instead of waiting for an end-of-year exercise,

students plan and execute multiple operations and receive feedback in order to improve themselves during the 10 months.

AOWC replaces Term II and Term III classes offered in the former CGSOC. It is focused on educating officers as command-capable brigade and battalion level commanders with advanced competencies as staff leaders to serve at all levels up to EAC.

AOWC studies are divided into three blocks of instruction; each block includes an application exercise. Students will demonstrate mastery at LCC, division level, and brigade level operations. This is done on a competitive basis between student groups, providing the opportunity for students to both study and perform in the multiple command and staff roles, as well as in threat force roles. The driving theme is enabling and executing division and brigade fights.

AOWC retains an elective program from the former course to provide the students with opportunities to pursue additional, focused studies.

Instructional Method

Team teaching is the third domain shift differentiating ILE from the former CGSOC. It represents the

“way” in which the school will achieve its “end”—graduates with a warrior ethos who are grounded in warfighting doctrine and who have the technical, tactical, and leadership competencies and skills to be successful in their career field, branch, or functional area.

Each of the teaching teams is made up of 10 instructors with differing areas of expertise: 3 are experts in joint and combined operations, 3 are tactics experts, 1 is a leadership expert, 1 is a historian, and 2 are logisticians. The team is responsible for providing all instruction to their group of 64 students throughout the academic year and exercising oversight during the major exercises at the end of the common-core portion of the course and during each block of AOWC.

Each team member also coaches seven or eight students. In this role, they are responsible for mentoring the students, providing feedback, facilitating, counseling, observing, and assisting them with their professional and personal development.

The team-teaching method is a huge change from CGSOC in previous years. Students know the instructors and, more importantly, the

instructors know the students and consequently are better prepared to provide meaningful developmental counseling. Keeping the students in small groups of 16 to 18 students allows for the best possible instructor-to-student ratio, and allows the team the opportunity to truly know and better develop the students.

So, what do we “old guys” think of ILE? It’s another significant step in the right direction for preparing majors to understand and solve problems in the highly complex operational environment they now face. No longer can they memorize General Defense Plan battle positions at the Fulda Gap and know who and where they will fight.

These field grade officers will be capable of thinking through the most difficult situation, adapting to changes in their operational environment, and ensuring the continued success and freedom of our nation.

We expect it will take time before our officer corps is comfortable with the notion of having no “school solution,” but as we have seen in Afghanistan, Iraq, and other hot spots throughout the world, there is no General Defense Plan, and our enemy is constantly changing, thinking, and adapting.

We have no alternative but to provide our nation with leaders who are capable of meeting these challenges—and ILE is another great step in fulfilling this imperative.

Some will continue to reason ILE is too resource-intensive, or too costly in other ways, or necessitates too many changes in the personnel system. Those and other arguments are quite compelling. But, from our foxhole, until we come up with a more cost-effective system to produce the quality officers our nation will depend upon in the foreseeable future, ILE is another step in the right direction.



Endnote

1. CGSG Mission Statement. See <https://cgsc.leavenworth.army.mil/DAO/ile/mission.asp>.

This article was written by Retired Colonels Neal Bralley, Jim Danley, Dan French, Chuck Soby, and Paul Tiberi—all instructors at the U.S. Army Command and General Staff College, who will teach ILE this coming academic year. Although this article has been submitted to the Army News Service and the TRADOC News Service, it is also being printed in this issue of the Military Intelligence Professional Bulletin because ILE will affect all mid-career Army officers as well as selected officers of the Army Reserve, Army National Guard, Navy, Marine Corps, and Air Force.

Lessons Learned: Task Force Sentinel Freedom OEF/OIF

(Continued from page 16)

leader, and soldier success in combat is operationalizing these imperatives directly from the U.S. Army Intelligence Center with all available assets and energy. We simply have got to move out and get after it.

Task Force Sentinel Freedom’s efforts have not been in isolation. Far from it. The Headquarters, Department of the Army (HQDA) G2 and his staff have been downrange in the

ater and out front solving current and future challenges facing soldiers and units in harm’s way and those going there soon. U.S. Army Forces Command (FORSCOM) and TRADOC are leaning forward on a daily basis supporting and anticipating warfighter’s requirements. Units and soldiers themselves are laser-focused on their missions and responsibilities—we are a nation at war against terrorism and will be for a long time to come. We are a team of teams which must continue to ensure the most accurate and timely intelligence possible makes it to,

stays in front of, and guides the tip of the warfighter’s spear.

ALWAYS OUT FRONT!



Colonel Mike Gearty recently returned from duties on the Coalition Forces Land Component Command C2 staff in Kuwait. He is currently the TRADOC System Manager, All Source Analysis System. Readers may contact him via e-mail at michael.gearty@hua.army.mil and by telephone at (520) 533-4107 or DSN 821-4107.

Sly Fox

ASAS Master Analysts' Support to Information Operations— Communications

by Matthew J. Nunn

This is the second of three articles discussing what the "SlyFox" brings to the Information Operation fight. The first article addressed Information Engineering, and the third will focus on analysis.

"Intelligence without Communications is Useless... Communications without Intelligence is Noise."

—General Alfred M. Grey, USMC

The All-Source Analysis System (ASAS) Master Analyst receives extensive training in Communications Architecture. Communications provides the foundation and backbone for Information Engineering. Without efficient communications, intelligence won't be able to flow from the analysis and control element (ACE). When building the Communications Architecture the Master Analyst considers several factors:

- ❑ Communications must be scaleable to support the volume and bandwidth of the information being received and transmitted.
- ❑ Success will be based on medium- and high-capacity communications.
- ❑ Effective use of communications requires proactive planning and technical knowledge.
- ❑ Intelligence presented and how it is presented must be decided early in the planning process.

Communications Architecture

The process of planning the Communications Architecture begins by the Master Analyst's assessing its three building blocks: The systems,

capacities, and protocols that will be used by the unit; its consumers and what will be required by the type and volume of information received; and the intelligence produced.

Systems

Systems that the Master Analyst has to consider during planning the Communications Architecture are broken down into three basic groups for simplicity—sensors, processors, consumers.

The first group is the sensors. Traditionally there have been a wide variety of sensors providing information into the ACE. These range from extraordinarily simple, to the latest space-age wonder system. An example is the requirement to receive basic SALUTE type reports (size, activity, location, unit, time, equipment) over a telephone or tactical radio, all the way to the latest high-speed, high-volume live imagery feed that could require its own communications pathway and individual workstation.

Second are the processors. Simply, these are any systems located in or in support of the ACE designed primarily to take the incoming data and process it into useable intelligence. Processors include but are not limited to the ASAS-Single Source, ASAS-All Source, ASAS-Remote Workstation (RWS), and ASAS-Light. The Master Analyst will also have to plan for the presence of other non-ASAS systems that might be located within the ACE.

Finally there are the "Consumers." These are systems inside and outside the ACE that will receive the in-

telligence produced by the processors. The range of consumer systems can be broad. It can be a personal computer that receives a graphic intelligence summary, a server that continuously has digital products posted to a web page, an ASAS-Light or other laptop system at brigade or battalion S2s, or even a non-MI system elsewhere in the Corps or Division that doesn't interface well with others. The Master Analyst maintains constant awareness of his consumer's systems, and their ability to receive the products the ACE produces.

Capacities

Capacities are as varied as the systems with which the Analyst Master has to deal. In addition to the raw capacity of the communications medium the ACE will use is the consideration of the portion of that capacity that various data, information, and products will require when moving through and around the ACE. Capacities internal to and external to the ACE vary, and can include those as low as 4.6 Kbps for a simple local area network (LAN) connection to pass text messages between systems; up to 56 Kbps to support multiple types of digital data moving among the ACE network; all the way through a T1 (1.544 Mbps) type circuit that can support multiple high-speed, high-capacity requirements such as video teleconference (VTC), and just about anywhere in between. As important as knowing the capacities of the systems passing information inside and outside the ACE, the Master Analyst must also know the

relative capacity requirements of the products that will be transmitted to various consumers.

Protocols

Protocols are the type of communications that our various systems use to communicate to each other. The right protocol to use is normally considered hand-in-hand with the capacities required by the information being passed. The Master Analyst has to be intimately familiar with the protocols used to communicate between the systems on the network and with the communications servers. Most important to the Master Analyst are the—

- ❑ Transmission Control Protocol/Internet Protocol (TCP/IP) used by the ASAS-Tactical Communications Support Processor (TCSP) which allows transfer of most data types.

- ❑ Digital Data Communications Message Protocol (DDCMP) which supplies serial (point-to-point) connections within the ACE through the Communications Network Server (CNS) 6300.
- ❑ Simple Mail Transfer Protocol (SMTP) used by the ASAS-Secure Messaging and Routing Terminal (SMART) which provides collateral connectivity for the ASAS-RWS and ASAS-Light as well as limited E-mail capability to the ASAS-TCSP.

Final Thought

The ASAS Master Analyst when faced with the vast number of systems utilized within the intelligence community has to maintain the ability to design and implement a broad-based Communications Architecture. While dealing with these

challenges the Master Analyst focuses not only on the needs of the ACE but also on the diverse systems that provide and consume the intelligence produced, that may or may not be 100 percent compatible with the ASAS family of systems. Meeting these challenges will continue to require the Master Analyst to be knowledgeable of his systems, capabilities, and protocols, while keeping in mind the needs of his consumers.



Matt Nunn is the Course Manager and an Instructor for the ASAS Master Analyst Branch. His career has included 13 years as a Signals Intelligence Analyst at multiple echelons and 5 years instructing the ASAS Master Analyst Course and the ASAS Instructor Certification Course. He also has 10 years' experience instructing and using various ASAS systems. Readers may contact Mr. Nunn via E-mail at matthew.nunn@us.army.mil and telephonically at (520) 538-1184 or DSN 879-1184.

Proponent Notes

(Continued from page 67)

officers must manage their careers carefully to ensure that they have sufficient time available to compete for both key leadership and technical jobs at each rank.

BQ for FA 34 Majors. The time requirement for serving in a functional area (FA) 34 coded position for BQ has changed from 30 months to 24 months. This will allow officers who are Career Field Designated (CFD) into FA 34, but not immediately moved, to still have the opportunity to become branch qualified prior to being considered for promotion to LTC.

BQ for FA 34 LTC. The time requirement for serving in an FA 34 coded position (LTC or higher) has been dropped from 48 to 36 months. Again, this change is intended to provide additional time for completion of BQ prior to consideration to COL.

Upcoming Officer Selection Boards. The LTC Command Board

is scheduled to convene in October 2003. Year groups 1984 to 1987 will be considered. Remember, it is imperative to have an updated photo and officer record brief (ORB) prior to the board.

The POC for officers and civilians is Ms. Charlotte Borghardt. Readers may contact her through E-mail at c.borghardt@us.army.mil and by telephone at (520) 533-1188 or DSN 821-1188.

By the time you read this Proponent Note, LTC Harvey Crockett will have assumed the duties as the new Director, OCMI. LTC Crockett was commissioned in 1982 after graduation from Mississippi State University. He has had a variety of tactical assignments from Berlin to Korea and from Fort Hood to Fort Lewis. He has been an S2, S3, XO, ACE Chief, and most recently served as the Commander, 303d MI Bn (OPS), 504th MI Bde, Fort Hood, TX.

In another change, SGM Maurice Mitchell has assumed duties as the

Chief, Enlisted Life Cycle. SGM Mitchell joined the Army in 1983 as a 98J. His past assignments include time spent with the 313th MI Bn, 319th MI Bn, and the 525th MI Bde, XVIII Airborne Corps. After completing the Undergraduate Intelligence Program, Joint MI College (JMIC), he attended the Sergeants Major Academy at Fort Bliss, TX. Readers can contact SGM Mitchell via E-mail at maurice.mitchell@hua.army.mil.



Lieutenant Colonel Eric Fatzinger is the Director, Office of the Chief, Military Intelligence (OCMI). Readers may contact him via E-mail at eric.fatzinger@us.army.mil. Robert C. White, Jr. is the Deputy OCMI; you can reach him via E-mail at bob.whitejr@us.army.mil. Readers may access the OCMI website through the Intelligence Center homepage at <http://usaic.hua.army.mil/> and then link to OCMI by choosing the Training/MI Professionals area. You will be able to find information on issues ranging from enlisted career field overviews to officer, warrant officer, and civilian updates.

TSM Notes

by SFC John L. Girardeau



U.S. Army Photo

Prophet being prepped for sling-load in Afghanistan.

Soldiers like SGT Jedediah Davis and SGT Adriana Hernandez from the 313th MI Battalion made a difference to the convoy they were with during an ambush in Afghanistan by providing continual support with their Prophet system.

—LTG Robert W. Noonan in his Monthly G2 Notes

Operation ENDURING FREEDOM (OEF) has served as a catalyst for accelerating changes in the Army's tactical signals intelligence (SIGINT) and electronic warfare (EW) force. Due to significant capability gaps identified during Task Force (TF) Rakkasan's OEF rotation, the TRADOC System Manager (TSM) for Prophet, in conjunction with the Product Manager (PM) for Prophet, worked with the 313th Military Intelligence Battalion to bolster their existing SIGINT/EW capability. This was accomplished by providing the 313th with Prophet Block I Engineering and Manufacturing Demonstrators (EMDs). The EMD models were provided rather than the production Block I models as the Block I system had not yet entered the production phase. In addition, the Prophet

EMD systems were augmented with additional equipment to further enhance their capabilities due to specific theater requirements. The additional equipment augmentation included the installation of high frequency (HF) extension direction finding (DF) antennas, AN/PRC-150 HF radios with automatic link establishment (ALE) capability, and AR-8200 hand scanners.

According to the 313th soldiers, the systems began making a difference from the moment they hit the ground. Not only was the system technically superior to current systems (such as the AN/TRQ-32(V)2 TEAMMATE and AN/TSQ-138 TRAILBLAZER), its improved mobility enabled the 313th soldiers to better support the infantry soldiers on the ground. Because the system was easily sling-loaded in addition to having roll-on, roll-off capability, the soldiers were able to put the system anywhere on the battlefield at a moment's notice. Because of the system's improved performance, commanders have become more inclined to moving with the initial wave of soldiers rather than the last wave so the system can provide support immediately. In fact, it has become increasingly common to find Prophet systems, like those with the 313th, in the thick of combat providing critical support for situational awareness and force protection.

Based on the lessons learned by the 313th in OEF, a similar but



U.S. Army Photo

Prophet being sling-loaded in Afghanistan.



more ambitious approach was taken to prepare the Army's Military Intelligence units for Operation IRAQI FREEDOM (OIF). The results from both OEF and OIF indicate that we still have a way to go

before tactical SIGINT/EW becomes the force multiplier that it can be. These results are still a vast improvement over past operations, and we appear to be headed in the right direction.

John L. Girardeau is the NCOIC for the TSM Ground Sensors in the TSM-Prophet office and can be contacted via E-mail at john.girardeau@us.army.mil and by telephone at (520) 538-2429 or DSN 879-2429.

Interpreters in Intelligence Operations

(Continued from page 28)

and then adapt doctrine to reality. Our community must also standardize our hiring methodology, streamline our procedures, and recruit a base of linguists to hold on retainer for future operations.

Conclusion

Interpreters provide the critical link between soldiers and the local population. They are part of the team and are truly team players. We need to remember that just as most military members have never communicated through an interpreter, most interpreters have never served in that capacity. They learned the language and culture as a part of growing up. The interpreters are involved in our mission because they have a specialized, mission-essential talent and skill. The faster we learn to work with interpreters, the faster we will accomplish our mission of creating a safe and secure environment during future operations.

2. Interpreters wear U.S. Army uniforms and U.S. flags (flags for Category II and Category III only). Wearing uniforms does not place them in combatant status, and it does help to determine who to protect during hostile activities. The fact that interpreters assist us in mission accomplishment makes them legal targets and increases the commander's responsibility to ensure their safety.
3. All points taken from Interpreters and Interpreter Duties discussed in STP 34-97E24-SM-TG.

john.rovegno@us.army.mil and by telephone at (502) 942-1276.

Linda Hajdari was born in Struga, Macedonia, and moved to the United States after the first grade. She quickly picked up English as her second language. In addition to her regular studies, she attended an Albanian language school on the weekends to maintain command of her native language. She graduated from Rutgers University in New Jersey with a Bachelor of Arts, double majoring in Psychology and Administration of Justice. Immediately after graduation, she was hired to serve as an Albanian interpreter with the U.S. forces in Kosovo. She arrived in Kosovo early in the summer of 1999 and began working as an interpreter assigned to the 101st Military Intelligence Battalion. Linda conducted over 400 missions while assigned to Field HUMINT Teams and has recently moved to become the Interpreter for the Task Force Falcon Commanding General.

Endnotes

1. TRW recently made a policy forbidding interpreters from firing or operating any type of weapon. This policy, while grounded in the intention to keep interpreters from becoming combatants, ignores the fact that these interpreters are part of our teams and could easily be placed in situations where they need weapons skills to protect themselves or their teams. Basic weapons familiarization would also allow interpreters to unload, clear, or disable weapons thus increasing safety for all combatants and noncombatants.

Colonel John Rovegno has served more than 20 years as an intelligence officer throughout the United States, Europe, and the Middle East. He is currently the G2 at the Units of Action (UA) Maneuver Battle Lab at Fort Knox, Kentucky. His assignments include platoon leader, two company commands, S2, the first S2 Observer/Controller at the Combat Maneuver Training Center, Battalion S3 and Executive Officer, Instructor, J2 Operations Officer, and G2. While at U.S. Central Command, he deployed on several operations including VIGILANT WARRIOR, VIGILANT SENTINEL, DESERT STRIKE, and RUGGED NAUTILUS. He joined the 1st Infantry Division in April 1997 as the G2, serving as G2, Task Force Eagle, in Bosnia-Herzegovina through October 1997. He remained as the 1st Infantry Division G2 until February 1999, working extensively in Germany and Macedonia. He took command of the 101st MI Battalion (Air Assault) in February 1999 and deployed with the Battalion as part of the Kosovo Initial Entry Force in June, remaining in Kosovo for just over one year. He is a graduate of the MI Officer Basic and Advanced Courses, Electronic Warfare/Cryptologic Officer Course, Command and General Staff College, Armed Forces Staff College, and the Army War College. He received a Bachelor of Science degree in Business Administration from Shippensburg (PA) University and a Master of Public Administration degree from the University of Missouri. Readers may contact the author via E-mail at

Drita Perezic was born in Italy and reared in New York. She graduated from the Florida Institute of Technology with a Bachelor of Science in Marketing, specializing in International Trade. She spent over ten years working in the fields of marketing, advertising, and public relations. Prior to being hired as an interpreter, Drita served as a Treasury Operations Representative for Salomon Smith Barney. She initially deployed to Tirana, Albania, in May 1999 as part of Task Force Hawk, working with the 165th MI Battalion. She then served as an interpreter for the 10th Special Forces Group, Civil Affairs, and the Joint Implementation Committee. She became the Interpreter for the first Task Force Falcon Commanding General, remaining in that assignment for five Commanding Generals. She recently departed Kosovo after 18 months of service.

MI Heritage

They Also Served:

Virginia Hall, Edmund Jilli, and Elizabeth Friedman

by Katharine W. Schmidli

Every day U.S. soldiers make sacrifices in service to this country. We ask them to be always on watch and frequently to go into harm's way. For this, we as a nation owe them everlasting respect. We must never forget those who give and have given service in defense of our nation.

There were also those who served our nation well but were not soldiers. Some of them were civilians who worked for the Treasury Department, State Department, and the Office of Strategic Services (OSS) and its heir, the Central Intelligence Agency. Here are the stories of three who also served.

Virginia Hall

Virginia Hall served as an intelligence agent during World War II. The French Resistance called her "la dame qui boite," or the "Limping Lady." The Germans called her "Artemis" and put her on the Gestapo's most-wanted list of Allied spies. She had many Allied code names: "Bousey," "Marie Monin," "Germaine," "Diane," and "Camille."

Born in 1906 in Baltimore, Maryland, Virginia Hall was a petite woman who loved outdoor sports and thrived on skiing and hunting. Educated in economics at Radcliff and then Barnard College in New York, she finished her studies in Paris and Vienna. She was also fluent in French, German, and Italian.

In 1930, the U.S. Diplomatic Corps hired her as a clerk where she worked in embassies in Italy, Estonia, and Turkey. During a hunting accident in Turkey, another hunter shot Virginia in the left leg. Doctors fitted her with a wooden leg, which gave her a decided limp for the rest of her life.



When war broke out, Virginia tried to become a Foreign Service Officer, but was turned down because of her wooden leg. In 1941, she proceeded to England where the British Special Operations Executive recruited her. She learned about weapons, communications, and Resistance operations. Her first operation was in Vichy, France, where she established a spy network with the French underground and helped prisoners of war escape. When Germany invaded France, Virginia escaped back to Britain and joined the OSS.

On a dark night in March 1944, Virginia Hall strapped her wooden leg on her side and parachuted back into occupied France. She set up voice and Morse code communications with the Allies and later began to organize Free French Resistance operations and coordinated the rescue and evacuation of downed Allied pilots. The Gestapo never caught her.

Virginia Hall's wartime achievements resulted in the presentation of the Member of the Order of the British Empire by King George VI in 1942 and the Distinguished Service Cross, presented by Major General William Donovan in 1945. The only female civilian to receive the Distinguished Service Cross, Miss Hall wrote, "*Not bad for a girl from Baltimore.*"

The newly formed Central Intelligence Agency welcomed Virginia Hall home to the United States and she continued to serve as one of the agency's first female operations officers until her mandatory retirement in 1966. Virginia Hall continued to live in Maryland until her death in January 1982. Virginia Hall became a member of the Military Intelligence (MI) Corps Hall of Fame in 1988.

Edmund C. Jilli

Edmund C. Jilli, a contemporary of Virginia Hall, served for thirty years in civil service to his nation. He was born in Saint Moritz, Switzerland. He attended school in Zurich, the University College in London, and the City College of New York in New York City before World War II. He was and still is fluent in German, French, English, Italian, and Spanish, with knowledge of at least four additional languages.

Some say Ed Jilli was "born on skis." From 1939 through 1942, he supervised the world-renowned ski and skating facilities at Sun Valley, Idaho. Then in 1943, in support of the war effort, Ed joined the State Department. His first assignments in Ecuador and Honduras were far from the European theater of operation, although he did man-



age to do some skiing in the Andes. By 1945, he was assigned to work for the Air Force in Bad Nauheim, Germany, and the Field Intelligence Agency in Frankfurt, Germany. He later transferred to the G2 Section, Headquarters, U.S. Field Agency at Salzburg, Austria. For the next nine years, he worked with the 430th Army Counterintelligence Corps (CIC) Detachment and with CIC Detachment 35 in Austria.

Mr. Jilli's subsequent assignments included service with the 522d MI Battalion in Munich in 1955-1957 and the Office of the Deputy Chief of

Staff for Intelligence (ODCSI), U.S. European Command (EUCOM), Paris, in 1957-1960. He was an instructor at Fort Holabird, Maryland, in 1960-1961; served with the G2 Section, U.S. Army Southern Command (USARSO), Panama, in 1961-1965; the 513th and 66th MI Groups in Frankfurt and Munich from 1965 to 1971.

His last formal position was as an instructor at the U.S. Army Intelligence School at Fort Huachuca, Arizona, in 1971-1973. He taught the Offensive Counterintelligence Operations Course, also known as Clandestine Operations. Ed Jilli retired from Civil Service in 1973, but continued to contract with the State Department as an interpreter and escort for foreign dignitaries visiting the United States. He was inducted into the MI Hall of Fame in 1988.

Elizabeth Friedman

The National Security Agency's Friedman Auditorium at Fort Meade, Maryland, and Friedman Hall at Fort Huachuca are **not** named after Elizabeth Friedman. Instead they memorialize her husband William F. Friedman, the "father of U.S. cryptanalysis." A preeminent cryptanalyst, William Friedman is noted for his cryptologic publications and for his team's solving the Japanese PURPLE code in 1940 and 1941. He was a 1988 inductee into the MI Corps Hall of Fame.

His wife Elizabeth Friedman was a cryptologist in her own right. During World War I, they both taught cryptology to Army officers. From the late 1920s through the 1930s, the Federal Bureau of Investigation (FBI) was concerned by the increased use of cryptography by criminal smugglers. Employed by the Treasury Department, Elizabeth Friedman broke the complicated codes of international and domestic smuggling rings. With no underlying knowledge of Chinese Mandarin, she deciphered encrypted communications between opium smugglers and broke the codes of West Coast Rum Runners during Prohibition.

Final Thoughts

There are many more examples of civilian intelligence professionals in service to our country from the Revolutionary War through the Vietnam War and beyond. They also served—silent civilian warriors in defense of our freedom!



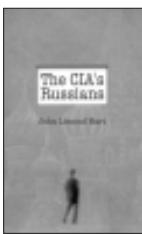
Editors Note: The photographs of Ms. Hall and Mr. Jilli have been electronically modified to improve their clarity.

Kate Schmidli is the curator for the U.S. Army Military Intelligence Museum at Fort Huachuca, Arizona and a retired MI Soldier. The museum is open seven days per week, from 9:00 to 4:00 weekdays and from 1:00 to 4:00 on weekends. Readers may contact her via E-mail at katherine.schmidli@us.army.mil and telephonically at (520) 533-1107 or DSN 821-1107.

Security Releases Required With Your Articles

The **Military Intelligence Professional Bulletin** always welcomes your professional contributions! **MIPB** does require a release signed by your local security officer or SSO stating that your article and the accompanying graphics are "unclassified, nonsensitive, and releasable in the public domain." The release should include your name, the title of the article, and contact information for the person who signs the release. We must have a signed copy of the security release either mailed or faxed to us. If your installation or agency requires you to obtain a public affairs release as well, please do so.

Professional Reader



By John Limond Hart
(United States Naval Institute Press, 2003), 264 pages, \$28.95, ISBN: 1-59114-352-7.

John Hart was a career Field Operator and Manager for the Central Intelligence Agency from 1948-76). While assigned to Central Intelligence Agency (CIA) Headquarters, he ostensibly became so "intrigued" with the reasons behind a handful of "high-level" Cold War defections that he, with the permission of CIA Director Richard Helms, took a year to attempt to locate common personality denominators.

In his Prologue, Mr. Hart provides background color to the times, The Cold War, discussing the U.S. attempts to roll back the Iron Curtain and some of the professional challenges facing the CIA "Field Operator." He discusses challenges such as paper mills and fabrications, the absence of agents in the East (Remember Korea?), spies versus defectors, and he ends by providing an insight into "Cultural Differences" and "the Matter of Motivation."

Chapters One through Four outline the CIA's involvement with four Soviet men who, between 1953 and 1962, acted as traitors to their country by providing information to the CIA. Pyotr Popov (1953-1958) was a Major in the Soviet Army; Oleg Penkovsky (1961-1962), a Soviet Colonel (later transferred to the GRU (Military Intelligence)); and Yuri Nosenko (1962- defected in 1964), a Captain in the KGB (State Security); and "Mikhail" (Jan-Apr (?) 1958), an agent with the GRU.

Whoa Nellie, that's only four guys! What's going on here? The CIA has only four Russians? At \$28.95 for the

The CIA's Russians

book, that's \$7.24 per Russian. That's all of the CIA's "Russians"? I truly hope that if there is a Hell it has a place for the folks who title books.

The chapters on Popov and Penkovsky make perfectly good sense. Between the two, they represent perhaps the two greatest spy coups ever perpetrated against the USSR by the U.S. Chapter Three, the piece on Nosenko, describes perhaps the greatest profile screw-up ever perpetrated by the CIA; they locked the man up for three years and two months on the presumption that he was a plant. No evidence, just a presumption. Eventually he was released and proved of some value.

Then there's Chapter Four, an account of the defection of a GRU officer named only "Mikhail." The CIA actually validated little of his background and he provided little significant information. Hart raises the question "why did the CIA waste time on him?" Perhaps a more germane question is, "Why did Hart waste time on him?" Maybe a better question would be, "Is this the best of the lot? Security notwithstanding, does the CIA's "Russians" now consist of only three men?" The Mikhail case was an example of those Wackos with whom field officers must from time to time confront.....I suppose. The price per Russian just hit \$9.65.

Chapter Five, the "Motivation" piece, provides a fair personality profile for Popov, Penkovsky, and Nosenko but pretty much presents Mikhail, like many of those who engage in the spy trade, "doing so for selfish and shallow reasons." For one-fourth the price of the book, I learned this little gem!

At this point in the book, the vast body of psychological data available to the CIA is notably absent. The

rather scant four-man study group receives an occasional plus-up with comments about some other heretofore unidentified Russian only to have the conclusion qualified with exceptions. Mr. Hart toys with such phrases as: "Resolution of psychological conflict through treachery.....an alternative way of resolving innertension....while bringing enough money to finance an more agreeable double life. Perhaps a sub-category sociopathic or psychopathic personality."

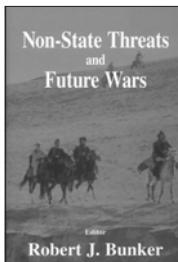
In an Epilogue, Mr. Hart describes Soviets he met in diplomatic circles and ironically none match as the personalities described. Of course, he probably met more than three *diplomats*.

The CIA's Russians is articulate, and quite easy to read; but there are a few speed bumps. While the chapters on Popov and Penkovsky (spelled "Penkovskiy," Avon Books, 1965 ed.) are informative, the chapter on Nosenko smacks a great deal of airing the dirty linen. Perhaps the Nosenko case was just the worse example of the CIA's work Mr. Hart could actually share.

All in all, *The CIA's Russians* (All Three of Them) provided a look (a very brief look) into the actions of a small (very small) population during a tense, confrontational era. However, I'm left wondering how anyone draws a psychological conclusion from a population of three? I'm thinking this book may have had more meat, prior to the CIA pre-publication review. Look for the book on Amazon.com, you can get it for about \$6 a Russian.



Dick Cameron, MW5 (Ret)
Colorado Springs, Colorado



edited by Robert J. Bunker (Portland, Oregon: Frank Cass and Company Limited, January 2003), 184 pages, \$24.99, ISBN: 07146 5374 8 (cloth) ISBN: 07146 8308 6 (paper)

Non-State Threats and Future Wars [edited by Robert J. Bunker] brings together a world-class team of defense scholars, military thinkers like Martin van Creveld and Ralph Peters, and law-enforcement specialists to discuss issues that are truly post-Soviet: [the changing nature of warfare, decentralized intelligence structures, the continuing blur between law-enforcement and military operations, the use of mercenaries, nonlethal weapons, and preparation for intense urban operations.] **Non-State Threats and Future Wars**, like most national security study-related books written in the last ten years or so, starts off with the proverbial introductory phrase “since the collapse of the Soviet Union.” However, unlike most books on the national security studies market, **Non-State Threats and Futures Wars** goes beyond most so-called “post-Soviet ideas” like adding a new kind of sensor package to a tank and calling that an innovation fit for the new battlespace. In fact, most of the authors who contributed to this book would question the utility of the main battle tank entirely.

T. Lindsay Moore’s article “Fourth Epochal War” questions the utility

of the military concepts of “exhaustion” and “wars of density,” which he defines as antiquated concepts of warfare unable to adapt to the realities of the new battlefield. Moore draws upon the lessons of history to demonstrate his point. Arguing by analogy, Moore suggests that “current weapons of efficiency” (like the main battle tank, for example) on the post-modern battlefield peppered with non-state terrorist networks among other things, is analogous to the medieval knights of old. They were riddled with arrows at Crécy in 1346 by English long-bow archers who not only were more mobile than the heavy knights but also refused to fight on the French knights’ chivalrous level. The medieval knights’ chivalrous code of combat and main armaments failed to defeat the new enemy just as the United States could fail to defeat the new enemies of the 21st century (criminal-soldiers, terrorists, warlords, and drug dealers) if the United States does not learn from the past and adopt new tactics, operations, and strategies that address the new strategic environment; this is very different from our current nation-state-based, force-on-force, traditional strategic model.

One of the overarching themes of **Non-State Threats and Future Wars** is that networked organizational structures are more apt to deal with post-modern security threats than are the traditional bureaucratic hierarchies of nation-states. The au-

Non-State Threats and Future Wars

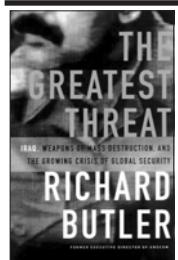
thors’ writing specifically on this subject understand that the nation-state and its concomitant bureaucratic hierarchies will remain the dominant form for political and social organization for many decades to come. However, the authors suggest that the two organizational forms can coexist: they believe that we can and must graft some sort of decentralized network that spans military, intelligence, law enforcement, and emergency services upon related traditional hierarchies to move quickly through Colonel John R. Boyd’s famous OODA (Observe, Orient, Decide, Act) loop, which is crucial in a security environment loaded with non-state actors.

The days when military and law-enforcement operations were mutually exclusive are over. Military and national intelligence agencies can no longer “hoard” their respective intelligence and must act in accord with law enforcement to combat terrorism that will most likely take place in our backyards. We will not always fight the wars of the future with the military “over there.” Military and intelligence officers should read this book because it paints a template for future conflict in an “out of the box” context. Remember, a little out-of-the-box thinking can and usually does go a long way!



Christian K. Rasmussen

Alexandria, Virginia



by Richard Butler (New York: Public Affairs, 2000), 262 pages, \$14.00, ISBN 1-58648-039-1

The Greatest Threat provides a chronological look at the attempts by the United Nations (U.N.) Secu-

rity Council’s appointed commission to document and account for the extended-range missiles and the manufacturing and production of chemical, biological, and nuclear weapons within Iraq. Despite the fact that the underlying theme of this book is arms control, additional dialog

The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Growing Crisis of Global Security

helps to reveal the inner workings of the diplomatic community. From Iraq’s point of view, they simply want embargos lifted that the United Nations ratified under *U.N. Resolution 661, Iraqi Sanctions* (6 August 1990). Understandably, these sanctions were put in place following

Iraq's unprovoked invasion of Kuwait in 1990.

As my reading progressed, I gained a greater understanding of the author's intent in addressing the unique threat that weapons of mass destruction (WMD) pose. The author addresses not only the failure of United Nations Special Commission (UNSCOM), the U.N.-created special commission involved in the disarmament process in Iraq, but ultimately the U.N. Security Council for failing to maintain authority over the entire disarmament process, clearly a threat to global security. I found myself seeking but not finding any framework that clearly defined the role of UNSCOM (as authorized by the Security Council) to control fully the disarmament process and ensure Iraq's compliance with international law. Reading this book made me wonder if the path we walk to maintain global security is not simply a political game of hiding the facts, turning the other cheek, and hoping the problem goes away.

Following the Gulf War, *U.N. Resolution 687* on implementation of Iraq inspections (adopted 3 April 1991) established the terms for a cease fire; under this Resolution, the U.N. directed Iraq to destroy all of its stockpiles of chemical and biological weapons including all ballistic missiles with ranges over 150 kilometers. The Resolution also prevents Iraq from acquiring

or developing nuclear weapons and created the special commission, UNSCOM, to inspect Iraqi sites to ensure compliance. Currently, the U.N. has failed in its attempts to disarm Saddam Hussein; his regime maintains an undisclosed quantity of WMD following the aftermath of the 1991 Persian Gulf War.

Richard Butler was the head of the UNSCOM-led inspections to disarm Iraq. Mr. Butler has a robust background in arms control and disarmament dealings as they pertain to global security and is a professional diplomat. As a result of his impressive background, Mr. Butler does an excellent job of bringing to light the facts that he and his staff uncovered during their inspection period. His argument is that undeniably we cannot assume that Iraq, under Saddam Hussein's direction, has never developed long-range weapons, missiles with the capability to deliver chemical and even biological agents, or that they destroyed these weapons as otherwise declared but rather concealed them for future deployment against enemies of Iraq.

This book can help us to draw relevant conclusions surrounding the current state of affairs in this region. It enhanced my perspective of the political dealings that manifest around the military community. Working as intelligence professionals, if reading about things like

political corruption, non-stop negotiations to disarm a rogue power, and underlying rhetoric from certain members of the international community does not excite you, then maybe deceptive conduct by permanent members of the Security Council, proof of Iraq weaponizing "VX" chemical agents, and the existence of known contaminated areas throughout that region will.

Lastly, a common theme throughout the book is that Iraq has shown belligerent and aggressive behavior toward the United States and our allies since the 1991 Gulf War campaign limited Iraq's reign of terror on its neighboring states. What can we take from this refusal to cooperate? The question that concerns all of us is: Will Iraq unleash weapons of mass destruction? It is correct to assume that the threat from the extended-range missiles supports our worst-case scenario in which Saddam Hussein initiates an Arab-led attack using these WMD against Israel and draws all into a catastrophic situation. I can draw only one conclusion from reading this book: Iraq maintains this capability and will certainly use these weapons associated with chemical, biological, and nuclear-capable delivery systems to eradicate all antagonists.

Douglas Thompson
Fort Huachuca, Arizona



MIPB Website Address

The **Military Intelligence Professional Bulletin** will be located within the Intelligence Center on the portal (ICON) which is located at <https://iconportal.hua.army.mil>. Our old address (which was <http://138.27.35.32/mipb/mipbhome/welcome.htm>) is no longer available. While we transition to the new automated website, **MIPB** will not post the issues from April-June 2000 through January-March 2003. However, readers can contact del.stewart@us.army.mil or mipb@hua.army.mil about those issues in the interim period.



Contact Information and Submissions



This is your magazine and we need your support in writing articles for publication. When writing an article, select a topic relevant to the Military Intelligence community; it could be historical or about current operations and exercises, equipment, TTPs, or training. Explain lessons learned or write an essay-type thought-provoking article. Short "quick tips" on better use of equipment, personnel, or methods of problem-solving and articles from "hot spots" are always welcome. Seek to 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 explain how a new piece of technology will change the way we operate.

Maintain the active voice as much as possible. Make your point. Avoid writing about internal organizational administration. If your topic is a new piece of technology, tell the readers why it is important, how it works better, and how it will affect them. Avoid lengthy descriptions of who approved it, quotations from senior leaders describing how good it is, or reports your organization filed regarding the system, etc. Note: Mailings become the property of **MIPB** and may be released to other government agencies or non-profit organizations for republication upon request.

The **MIPB** staff will edit the articles and put them in a style and format appropriate for the magazine. You can send articles, graphics, and photographs via E-mail to **mipb@hua.army.mil** or **del.stewart@us.army.mil** and **liz.mcgovern@us.army.mil** or mail (with a soft copy on disk) to ATTN: ATZS-FDT-M, Bldg 61730, Room 105, U.S. Army Intelligence Center and Fort Huachuca, 550 Cibeque Street, Fort Huachuca, AZ 85613-7017. (Please do not use special document templates and attach the graphics separately.) We can

accept articles in Microsoft Office 2000, Word 7.0, and ASCII; we need the graphics in Adobe, tif, jpg, Corel, or PowerPoint (in order of preference). Please include with your article:

- A cover letter with your work and home E-mail addresses, work telephone number, and a comment stating your desire to have the article published.
- A release signed by your local security officer or SSO stating that your article is unclassified, non-sensitive, and releasable in the public domain (see page 66).
- Pictures, graphics, and crests/logos with adequate descriptions. Submit clear "action" photos that illustrate your article with captions for the photos (the who, what, where, when, why, and how); the photographer credits; and include the author's name on photos. Please do not embed graphics in the article 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 position, related assignments, relevant civilian degrees (degree, school, major), and any special qualifications. (Please indicate whether we can print your telephone number and your E-mail address with the biography.)

We cannot guarantee we will publish all submitted articles but will send you a message acknowledging its receipt. We may notify you again when we get ready to publish it. Please inform us of any changes in contact information as it can take a year or more before we publish some articles.

If you have any questions, please call (520) 533-9968 (DSN 821) or (520) 538-1005 (DSN 879).



ASAS Contributions to Operation IRAQI FREEDOM

(Continued from page 30)

data sharing between higher and lower echelons worked exceptionally well. Although it often appeared we were being slowed by the system's capabilities, in reality data was being transferred faster and timelier than ever before. Personally, I believe expectations were placed so high they could

not be reached. This is not necessarily a bad thing. I agree the bar should be high and, as it comes in view, raised even higher. In the final analysis, all I needed to hear was a subordinate command say, "Thanks for the info."



Michael Joseph Gaynor's current position is the ASAS Database Manager for

the 513th Military Intelligence Brigade, Fort Gordon, GA. Mr. Gaynor has served in this position since becoming a contractor for General Dynamics in 1998, thus encompassing both Operation ENDURING FREEDOM and Operation IRAQI FREEDOM. Previous assignments include Order of Battle technician at the 513th MI Bde from 1994 to 1998. He has served in numerous intelligence positions ranging from Battalion to Army level.

104th Military Intelligence Battalion



DISTINCTIVE UNIT INSIGNIA

Description: A Silver color metal and enamel device 1-1/8 inches (2.86 cm) in height overall consisting of a shield blazoned: Azure (oriental blue) an eagle's head Proper in front of two swords in saltire Argent hilted Or and in chief a lightning flash fesswise of the like. Attached below the shield a Silver scroll inscribed "WATCHFUL AND READY" in Black letters.

Symbolism: Oriental blue and silver gray are the colors associated with Military Intelligence. The crossed swords attest to the unit's readiness; the eagle, wide-eyed and alert, is symbolic of watchfulness. The bolt of lightning above refers to the unit's electronic warfare capability; altogether the symbols express the words of the motto and the unit's basic mission and responsibility.

Background: The distinctive unit insignia was approved on 12 May 1981.

Motto: WATCHFUL AND READY

Constituted 16 September 1980 in the Regular Army as the 104th Military Intelligence (MI) Battalion (BN), assigned to the 4th Infantry Division, and activated at Fort Carson, CO (374th Army Security Agency [ASA] Company). Constituted 21 November 1963 in the Regular Army as Company C, 303d ASA BN; Activated 20 December 1963 at Fort Lewis, WA; Reorganized and redesignated 15 October 1966 as the 374th ASA Company; Inactivated 30 June 1972 at Fort Carson, CO; Activated 21 December 1977 at Fort Carson, CO; Inactivated 15 December 1995 at Fort Carson, CO; and Activated 16 January 1996 at Fort Hood, TX.

4th MI Company concurrently reorganized and redesignated as Companies A and B. Constituted 12 July 1944 in the Army of the United States as the 4th Counter Intelligence Corps Detachment; Activated 6 August 1944 in France with personnel from provisional Counter Intelligence Corps detachment attached to the 4th Infantry Division; Inactivated 23 February 1946 at Camp Butner, NC; Activated 30 November 1946 in Germany; Inactivated 20 April 1947 in Germany; Allotted 5 January 1949 to the Regular Army; Activated 31 January 1949 at Fort Ord, CA; Reorganized and redesignated 25 January 1958 as the 4th MI Detachment; Reorganized and redesignated 26 December 1969 as the 4th MI Company; and Assigned 21 July 1978 to the 4th Infantry Division.



COAT OF ARMS

Blazon:

Shield: Azure (oriental blue) an eagle's head Proper in front of two swords in saltire Argent hilted Or and in chief a lightning flash fesswise of the like.

Crest: None.

Symbolism: Oriental blue and silver gray are the colors associated with Military Intelligence. The crossed swords attest to the unit's readiness; the eagle, wide-eyed and alert, is symbolic of watchfulness. The bolt of lightning above refers to the unit's electronic warfare capability; altogether the symbols express the words of the motto and the unit's basic mission and responsibility.

Background: The coat of arms was approved on 26 February 1981.

NOTE: Only combat-proven units are authorized a Coat of Arms in coordination with

Campaign Participation Credits and Decorations

Company A entitled to: VIETNAM: Counteroffensive, Phases II through VI; Tet 69/Counteroffensive; Summer-Fall 1969; Winter-Spring 1970; Sanctuary Counteroffensive; Counteroffensive, Phase VII.

Company B entitled to: WORLD WAR II - EAME: Normandy (with arrowhead); Northern France; Rhineland; Ardennes-Alsace; Central Europe.

VIETNAM: Counteroffensive, Phases II through VI; Tet 69/Counteroffensive; Summer-Fall 1969; Winter-Spring 1970; Sanctuary Counteroffensive; Counteroffensive, Phase VII.

Company A entitled to: Meritorious Unit Commendation (Army) for VIETNAM 1967/1968/1969/1970

Army Superior Unit Award for 1996-1997; Republic of Vietnam Cross of Gallantry with Palm for VIETNAM 1967-1969/1969-1970; Republic of Vietnam Civil Action Honor Medal, First Class for VIETNAM 1967-1969.

Company B entitled to: Meritorious Unit Commendation (Army) for VIETNAM 1968-1969; Belgian Fourragere 1940; Cited in the Order of the Day of the Belgian Army for action in Belgium and Ardennes; Republic of Vietnam Cross of Gallantry with Palm for VIETNAM 1968-1969; Republic of Vietnam Civil Action Honor Medal, First Class for VIETNAM 1968-1969.

104th Military Intelligence Battalion is now serving in Operation IRAQI FREEDOM.

WATCHFUL AND READY!

ATTN ATZS-FDT-M (12)
USAIC AND FORT HUACHUCA
550 CIBEQUE STREET
FORT HUACHUCA AZ 85613-7017

BULK RATE
U.S. POSTAGE & FEES PAID
NIAGARA FALLS, NY 14304
PERMIT NO. 300



Now...



and then...

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

PIN: 081083-000