MIPB

Military Intelligence Professional Bulletin

July-September
2002
PB 34-02-3

Battlefield Visualization and Presentation

From the Editor

Like the surprise attack on Pearl Harbor some 60 years ago, the devastating attacks on the World Trade Center and Pentagon 11 September 2001 jolted U.S. citizens out of their complacency and attitude that "*it can't happen here*." For those of us living in both 1941 and 2001, no longer was the war "*over there*." Both attacks struck the core of the nation's economic, military, and political institutions and both would leave an indelible mark on the citizens of the United States.

The shocking and tragic events of September 11 proved to be but the tip of the iceberg. On 8 October 2001, the President signed **Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council**, which established the Office of Homeland Security (OHS). Homeland Security (HLS) consists of two broad mission areas: Homeland Defense (HLD) and Domestic Support. Of these, the Department of Defense (DOD) serves as the executive agent for HLD with support from other federal and state agencies while the Federal Emergency Management Agency (FEMA) serves as an executive agency for Domestic Support issues with the support of DOD and other agencies.

The OHS has the primary mission of developing, coordinating, and implementing a comprehensive national strategy to secure the United States from terrorist threats or attacks. Efforts to execute **Executive Order 13228** have affected nearly every aspect of our daily lives. We are still feeling these impacts on Wall Street, Pennsylvania Avenue, and Rodeo Drive, not only with regard to increased security but also with the cost of the Global War on Terrorism that began with the attacks in New York City and Washington D.C.

Today U.S. citizens live with roadblocks and safety zones installed around our government buildings and increased security in our cities and airports and seaports. Additionally, we have seen our military forces and those of our allies dispatched to Afghanistan. This movement of troops, the subsequent operations, and the successes of these military forces have for the moment allowed the United States and her allies to regain the initiative. There we continue to push and force Al Qaeda from its caves and safe houses. We have taken the fight to the enemy and since October 2001 also have moved U.S. forces into Pakistan, the Philippines, and other locations. Additional deployments will follow as the War on Terrorism continues, and it will go on for some time.

This edition of the ***Military Intelligence Professional Bulletin (MIPB)*** focuses on many aspects of HLS. As President George W. Bush said during a speech at the Citadel, "*We have to think differently. The enemy who appeared on September eleventh seeks to avoid our strengths and constantly searches for our weaknesses so America is required once again to change the way our military thinks and fights. The enemies worldwide got a chance to see the new American military on October 7 [2001]. Our military cannot and will not be evaded*."

In such a diverse and dynamic society as ours, HLS issues, especially those addressing the *USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act)* and Intelligence Oversight issues, remain controversial. ***MIPB*** serves as a conduit between the Intelligence Center and MI professionals and as such has sought input from a variety of sources regarding Homeland Security. The articles submitted do not necessarily reflect the official policy or position of the U.S. Army, Department of Defense, or the U.S. Government.

Regarding the articles in this issue of ***MIPB,*** although each writer may not specifically refer to the orders, regulations, and policies listed below, all intelligence activities must adhere to Intelligence Oversight policy. **Executive Order 12333**, **United States Intelligence Activities**, and the Crimes Reporting Memorandum of Understanding between the Department of Justice and Intelligence Community members stipulate that certain activities of intelligence components that affect U.S. persons be governed by

(Continued on page 18)

Michael P. Ley

Michael P. Ley

MILITARY INTELLIGENCE
Professional Bulletin

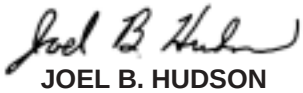
ALWAYS OUT FRONT

PB 34-02-3
Volume 28 Number 3
July-September 2002

FEATURES

DEPARTMENTS

By order of the Secretary of the Army:
Official:



JOEL B. HUDSON
Administrative Assistant to the Secretary of the Army
0210102

ERIC K. SHINSEKI
General, United States Army
Chief of Staff

Always Out Front

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

Much has been said and written about the events and emotions of 11 September 2001. Allow me to reflect personally about that day. September 11, 2001, was the day I took command of the U.S. Army Intelligence Center and Fort Huachuca (USAIC&FH). We honored Major General John D. Thomas, Jr., my predecessor, for his wonderful career of selfless service as a soldier. I thanked the Army leadership for placing their trust and confidence in my family and me with the responsibilities of command of our nation's most precious resource, her sons and daughters in uniform. Finally, I challenged our soldiers and civilians to prepare themselves for the days ahead…to whom much is given, much is expected. Our soldiers receive the best training in the world; our nation expects us to step forward and do what is required. As we all learned just minutes before the ceremony, our nation was under attack. It was the United States' first "home game" since the Civil War. Things were now different. Little did I know 26 years ago that the training I received as a Second Lieutenant at Fort Huachuca would provide the skills necessary to accept the burden of that day.

The change-of-command ceremony with Major General Thomas took place at 0800 on Brown Parade Field. Earlier in the morning, I was in the guesthouse and, like every soldier, was polishing my boots and squaring away my uniform when my daughter called me to the television. My jaw nearly hit the floor. The top floors of one of the World Trade Center buildings was a mass of black smoke and flame. The initial reports were somewhat confusing. An aircraft, believed to be a passenger jet, had apparently slammed into the building. It was a clear, bright morning in New York and I wrestled to grasp how such a collision could occur. I could only think this was no accident. This was a deliberate attack, but even while thinking through the possibilities, I followed the flight of the second jet through completion of its own horrible journey. There were no doubts now, our country was under attack. Listening to the news of the Pentagon attack and the crash of yet another passenger jet in Pennsylvania, I quickly finished dressing. As I walked toward Brown Parade Field with my wife Marty and our youngest daughter Claire, I reflected for a moment how my father and his generation had absorbed the news of the attack on Pearl Harbor some sixty years before.

There was, however, little time for reflection. Our nation was under attack by an enemy who was not known but whose intentions were clear…the destruction of our way of life. I had a job to do. There were soldiers in formation who awoke that morning to a country at peace and within the span of twenty minutes, found her at war. Looking back on it now, I admit that even though I had 26 years of service under my belt, I was surprised at the extent of how much my training and preparation took over during the next 48 critical hours.

At Brown Parade Field, I could see the same feeling in Major General Thomas' eyes. Both of us were well schooled in the lessons of Pearl Harbor, both of us realized there had been an intelligence breakdown, and both of us realized there was a new war to fight. Following an abbreviated change of command ceremony, I spoke to the audience, all by now aware of the situation. Observing the mostly young faces, I could see a mix of worry, horror, and grim determination as they mentally steeled themselves for what they knew was coming. Those twenty minutes between the first and last suicide attacks had forever changed their world.

The speech I had written and was prepared to give was now terribly obsolete. Like the soldiers, my world had changed in those same twenty terrible minutes. Like all the Soldiers, Sailors, Airmen, Marines, and Civilians present that morning, I was unconsciously shifting into another gear, one that could only be addressed by my years of training. The United States had been challenged. Because our nation has the best trained and equipped military force in the

(Continued on page 4)

CSM Forum

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

This past March, we held our CSM/SGM Military Intelligence Worldwide Conference. The conference was a great success.

Highlighting the week was our recognition of Specialist Ario Sanchez-Padilla, 75th Ranger Regiment (Infantry) as the Second Annual Doug Russell award recipient. (Presented during the conference each year, this award goes to a soldier (E1 through E5) who has made a significant contribution to military intelligence.) At the Ice Breaker on the first night of the conference, we invited our great retired MI SGMs/CSMs, which brought together the past, present, and future of our NCO leadership. We, the MI Sergeants Major, want to thank the sponsors for making our Ice Breaker so successful—we are fortunate to have sponsors like them here in Sierra Vista, Arizona, embracing Fort Huachuca and bringing the civilians and military together into "A Community of One," a true partnership. Also, special thanks from Brigadier General John Marks and myself to all of the Sergeants Major for the donations to the MI Museum and new memberships for the MI Corps Association (MICA). We contributed more than $5,000 to the Museum and MICA.

We all need to start thinking about next year's conference; if there are any briefings, issues, or speakers you would like for next year's conference, let me know. My E-mail address is lawrence.haubrich@hua.army.mil. The basis of the success of our conference reflects what we, as the senior noncommissioned officers of Military Intelligence, want to accomplish.

During the past three months, I visited some of our terrific MI soldiers. I spent a day with the 260th MI Battalion (Linguist), Florida Army National Guard, in Miami. This Battalion not only integrates Intelligence and language expertise but also has an active role in the Florida Army National Guard Counternarcotics Program. Since the attacks on 11 September 2001, the 260th MI Battalion has provided continued augmentation support to the U.S. Coast Guard for Operation SAFE HARBOR (seaport security). While in Florida, I also visited Pensacola where I talked with many of the soldiers in the 98K (Signals Collection/Identification Analyst) initial entry training (IET) classes and the cadre which are setting these great young soldiers up for success. The cadre briefed and took me through the material the 98K soldiers learn at Pensacola. The bottom line is that what these fine young soldiers learn in 98K IET hurts my head.

Having never been to Korea or Japan, I was very excited to have the opportunity to visit the MI soldiers there. In Korea, I visited the U.S. Forces-Korea MI unit, the 501st MI Brigade, and attended their 2002 Military Intelligence Ball. This year's theme for the MI Ball, "Yesterday-Today-Tomorrow: 50 Years of Combined Intelligence," paid tribute to the intelligence partnership between the Republic of Korea and the United States. Their MI Ball was full of camaraderie, fun, and friendship among many individuals associated with the intelligence community on the Korean Peninsula. The Korea Chapter of MICA did a wonderful job hosting this significant event. The MI soldiers in Korea are truly "READY TO FIGHT TONIGHT."

In Japan, I visited U.S. Forces-Japan units and the 500th MI Group. While visiting the MI soldiers at Camp Zama and Misawa, I had an office call with Colonel Mitzell and the Superintendent of the site located on Misawa. Both of them spoke very highly of the "Army soldiers," our MI soldiers assigned to the 403d MI Detachment. They shared with me the added value our MI soldiers bring not only in the intelligence field but also to the leadership and Army values that they bring to the joint environment as well. Our MI soldiers are doing great things in the joint environment.

I want to personally thank all of those Military Intelligence soldiers from their respective units I visited for teaching me "their jobs." I am always a student; I learned from you, and all of you taught me well. Thank you!

As always, let's take care of each other and our families. You train hard, you die hard; you train easy, die easy. Peace needs protection.

ALWAYS OUT FRONT!

(Continued from page 2)

world, we, like our fathers at Pearl Harbor, would recover. We would strike back at our enemies, and we would win. Even as I said these words, I realized that, our inevitable victory would not be without cost: cost on both the military and home fronts. As we all learn, our freedom is not free.

My short speech that morning reflected the challenge to our form of government and the very values on which our government was established. I said that to meet the challenges in the days ahead, we had to rely on our training, our years of preparation, our leadership, and our technological enablers. This is the first war of the 21st century. Meeting these new challenges is not an easy task. The Global War on Terrorism will be long and hard-fought. Our soldiers will face asymmetric threats in locations that were not among the highest priorities before that fateful morning.

The arsenal of intelligence skills we need to win are mostly adaptive techniques to our most fundamental skills. I believe these skills fall across the scope of our core competencies and once again validate these competencies. If we are technically proficient we will excel. A few skills and techniques I would like to highlight include—

- ❑ A thorough understanding of the laws, directives, and regulations governing collection on U.S. persons and the skill to make these provisions work for our mission.
- ❑ Maximizing every antiterrorism and force protection (AT/FP) process, procedure, and product through the timely and effective integration of foreign intelligence and predictive intelligence techniques.
- ❑ Carefully working with other U.S. federal, state, and local agencies so that we are truly acting in a partnership rather than occasional coordination.
- ❑ Adapting intelligence preparation of the battlefield, indications and warning, situation development, and intelligence support to targeting to meet our units' consideration for AT/FP and Homeland Security (HLS).
- ❑ Carefully using interrogation techniques and open-source information to "round out" AT/FP and HLS.

We were surprised that September morning, but not anymore. Protecting not only our homeland but also our forces has new and personal meaning for each of us. We are not waiting but are taking the initiative—we are taking the war to our enemy. Our forces have already defeated some of the most feared terrorists in the world. The fighting in Afghanistan continues but we are also assisting in the effort to defeat terrorist groups in other parts of the globe. The terrorist threat is not local nor regional but threatens all of mankind. With our friends and allies, we are meeting the challenges. As our President said, "*we will not falter and we will not fail*."

Finally, in light of the events and challenges posed by the attacks on September 11, there is now more emphasis than ever on my words from the last issue of ***MIPB***. I wrote, "*You have received the best training; you are led by the best NCOs and officers in uniform; you are enabled by unprecedented technologies. You will perform. We expect much of you*." Our nation needs you now more than ever. Stay focused on the task at hand. Run hard, run fast, run with your eyes wide open. You are the best.

"I Got It"

Annual ATCAE Conference 23-27 September 2002: Tactical Operations in the War on Terror

The Army Technical Control and Analysis Element (ATCAE) will host its fourteenth annual conference at Fort Meade, Maryland, from 23 through 27 September 2002. This event is open to properly cleared signals intelligence and electronic warfare professionals from the U.S. Army and our sister Services, and national and allied organizations involved in operations with and support to tactical SIGINT/EW units. The theme of this year's conference is "Tactical Operations in the War on Terror."

The annual ATCAE conference provides an opportunity to learn about new techniques and technologies, and for units to share operational lessons learned. Details of the conference agenda and procedures for participation will be available through formal messages and on the ATCAE INTELINK website. You may address any questions about the conference to CW5 Wallace Price, ATCAE Senior Technical Advisor, via E-mail at wsprice@nsa.ic.gov and by telephone at (301) 688-6900 or DSN 644-6900 (STU III).

This issue of ***MIPB*** focuses on antiterrorism, force protection, and Homeland Security. Although each writer may not specifically refer to the orders, regulations, and policies below, all intelligence activities must adhere to intelligence oversight policy.

Executive Order 12333, **United States Intelligence Activities**, stipulates that certain activities of intelligence components that affect U.S. persons be governed by procedures issued by the agency head and approved by the Attorney General. **AR 381-10**, **U.S. Army Intelligence Activities**, establishes the responsibility for intelligence activities concerning U.S. persons, includes guidance on the conduct of intrusive intelligence collection techniques, and provides reporting procedures for certain federal crimes. **AR 381-10** implements **Executive Order 12333**, the Crimes Reporting Memorandum of Understanding between the Department of Justice and Intelligence Community members, **Department of Defense (DOD) Directive 5240.1**, **DOD Regulation 5240.1-R**, and **DOD Instruction 5240.4**. These regulations apply to the Active Army, the U.S. Army National Guard, and the U.S. Army Reserve. They apply to Army intelligence components and non-intelligence components conducting intelligence activities.

Lieutenant General Robert W. Noonan, Jr., signed a memorandum, Subject: Collecting Information on U.S. Persons, on 5 November 2001. In the memorandum, LTG Noonan offered the following guidance:

a. Contrary to popular belief, there is no absolute ban on intelligence components collecting U.S. person information. That collection, rather, is regulated by **EO 12333** and implementing policy in **DOD 5240.1-R** and **AR 381-10.**

b. Intelligence components may collect U.S. person information when the component has the mission (or "function") to do so, and the information falls within one of the categories listed in **DOD 5240.1-R** and **AR 381-10**.

LTG Noonan also explained that "MI may receive information from anyone, anytime. If the information is U.S. person information, MI may retain that information if it meets the two-part test discussed in paragraph b, above."

As each article discusses intelligence collection to support antiterrorism, force protection, and Homeland Security, active adherence to intelligence oversight policy is occurring, although the author may not specifically cite or caveat that fact.

Homeland Security: An Intelligence Oversight Perspective

by Regan K. Smith

Since September 11, the United States' Legislative and Executive Branches have been grappling with how to determine and respond to threats to the United States' sovereign territory. Congress passed the *USA PATRIOT Act*.[1] The President established the Office of Homeland Security. The Secretary of Defense established a Department of Defense (DOD) Homeland Security Office. The Army is wargaming and evaluating its requirements. To date, however, the only guidance actually documented was the *PATRIOT Act*. This article reviews intelligence oversight in light of recent events, and provides Military Intelligence (MI) professionals food for thought as the Homeland Security (HLS) process evolves.

USA PATRIOT Act of 2001

The *PATRIOT Act* requires the Attorney General to write implementing guidelines. As of this writing, the Attorney General's office has not yet promulgated those guidelines; they will not apply to MI until DOD implements any relevant portions of that guidance. The *PATRIOT Act* did not alter, in any manner, the DOD criminal investigative or counterintelligence (CI) jurisdictions established in the current DOD and Department of Justice (DOJ) delimitations agreements. See Figure 1 for those few areas impacting the Intelligence Community (IC).

The *Act* allows law enforcement to share certain information, such as grand jury information, with the Intelligence Community—information to which the IC previously had no access. In turn, the Director of Central Intelligence, working with the Attorney General, must develop and implement a means of sharing IC information with the law enforcement community in ways that get the information to an actionable agency, yet still does not endanger intelligence sources and methods. How both communities will accomplish this is not known.

Intelligence Oversight Changes

So what does this mean for intelligence oversight? It means that the

The *PATRIOT Act* did not fundamentally alter the framework under which DOD conducts intelligence activities—the *Act* primarily affected the law enforcement community. All the current laws and regulations remain in effect for intelligence components.

Section 203. Broadens the law enforcement community's ability to share information unearthed in criminal investigations.

Grand Jury Information. Section 203(a) allows law enforcement officials to share previously unattainable Grand Jury information with any intelligence, national security, or national defense official when the information is of foreign or counterintelligence value.

Wiretap Information. Section 203(b) allows federal officials acting pursuant to a warrant obtained under the wiretap statute to share foreign and counterintelligence discovered pursuant to that warrant with appropriate law enforcement and intelligence officials.

Foreign Intelligence Generally. Section 203(d) authorizes sharing foreign intelligence obtained during criminal investigations with the appropriate federal officials (including intelligence), notwithstanding any other provision of law.

Section 206. Amends the *Foreign Intelligence Surveillance Act* (FISA) of 1978 to allow "roving" wiretaps for intelligence purposes. Previously, each FISA warrant focused on the specific telephone lines or computer addresses to be monitored. This change allows the monitoring of individuals, regardless of what phone or computer they use.

Section 207. Extends the period of surveillance of "agents of a foreign power" and for physical searches.

Section 216. Amends the Pen Register/Trap and Trace statute to make warrants issued under the statute effective nationwide. Before this change, investigators had to apply for a new warrant in each jurisdiction they entered. This section also explicitly extends the PR/TT statute to Internet communications (although in practice, it already applied).

Sections 217 and 1003. Amends the definition of "electronic surveillance" to allow monitoring of computer trespassers without a warrant, providing the system owner has consented and the monitoring is pursuant to a lawful investigation.

Section 504. Allows federal officers conducting FISA electronic surveillance and physical searches to consult and share information with law enforcement officers to prevent terrorist attacks and clandestine intelligence activities.

Section 905. Requires federal law enforcement officials, in accordance with guidelines to be developed by the Attorney General, to disclose expeditiously to the Director of Central Intelligence any foreign intelligence unearthed in the course of a criminal investigation.

Sunset Provision. Most changes in Title II sunset on 31 December 2005. The sunset provision does not apply to the amendments in sections 203(a) and 216.

Figure 1. Impact of the *USA PATRIOT Act* of 2001 on DOD Intelligence Activities.
(Courtesy of the Office of the Assistant to the Secretary of Defense for Intelligence Oversight.)

DOD and Army policies predating the *PATRIOT Act* remain in effect (**DOD 5240.1-R**, **Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons**, and **AR 381-10**, **U.S. Army Intelligence Activities**). (MI has no more and no less authority to collect, retain, and disseminate domestic U.S. person information, without a connection to foreign powers or international terrorism, than it did before the *Act*).

What has changed is a realization that information stovepipes are hindering the United States from determining what the normal internal baseline is, how to tell when a situation changes from the norm, and what that might mean. Does information indicate another terrorist attack is in preoperational planning? Is an attack imminent? Was it just ordinary crime or ordinary daily activity in that region? We literally do not know what we do not know. At DOD and the Joint Staff (and yes, Headquarters, Department of the Army [HQDA]) levels, they are now questioning whether we all have too strictly interpreted intelligence and law enforcement oversight, limiting our baseline knowledge within the United States and, if so, what changes are necessary.

Meanwhile, there is an immediate requirement to fuse information from the IC; federal, state, and local law enforcement; and other local entities at various levels into as accurate an analysis of potential or actual threats as possible. **AR 525-13**, **Antiterrorism**, dated January 2002, covers this in detail. It is here that things become very confusing in the Army.

In a nutshell, the same old rules apply for MI. Military intelligence still is not and will not be the "database central" for all "threat" data held inside the Army ("threat" appears to change definitions according to location and who requested it for a particular type

of information). **AR 525-13** clearly states that the force protection (FP) focal point lies with the G3 or equivalent, not in the G2. The fusion process, combining police intelligence, criminal intelligence, and MI into an FP product, is not a provost marshal, U.S. Army Criminal Investigations Command (USACIDC), or MI function. It is a force protection office function.

Rules Applicable to HLS Collection and Dissemination

While most Army elements can task-organize as needed, certain rules apply no matter where a command places its FP office. For example, suppose a continental United States (CONUS) installation has designated its fusion point as a "Force Protection Analyst" (FPA) position? Contrary to **AR 525-13**, that position was in the installation or corps G2 shop. That individual has the responsibility (assigned function) of fusing and analyzing information, but the disseminated product is **not** an intelligence product. Merely locating within the G2 shop does not constitute a functional assignment to the G2. The G2 shop may simply have all the communication "pipes" necessary for the FPA to do his work.

This FPA must receive information from many sources including:

- ❑ Provost marshal, USACIDC, and 902d MI Group local offices (and through these three, local civilian officials).
- ❑ Army G3 Antiterrorism Operations and Intelligence Cell's daily FP summary.
- ❑ Engineer data.
- ❑ Finished IC and local G2 products.
- ❑ FP offices in nearby DOD facilities.

The FPA then determines which information meets the "so what" criteria of applicability to his customers. Only that information goes into his FP analytical products, which are filed as FP products, under MARKS (Modern Army Recordkeeping System) file number 525. When the FPA briefs the information, it is an FP assessment briefing—no G2 logos, no presentation as an intelligence briefing, nothing that will give the customer the impression that this is an MI product.

Now, what does the "so what" criteria mean to that FPA's supporting MI shop? In a current example—combined and sanitized to obscure actual identities—several organizations recently downloaded a public media report about a militia group in a remote area of the country. This group had claimed it would attack state officials, who would then call up the National Guard. The group would attack the National Guard, thereby bringing on a general revolution against the federal government. This report appeared in several FP daily summaries. Organizations then copied and pasted it into any number of intelligence products, without ever showing a connection to the organization publishing it.

One command stated it had to know about the information because it was responsible for FP, and the militia was a threat to the National Guard. Let us dissect two facets to this claim.

"*The command is responsible for force protection*." Whose force protection? The nation's? No, that responsibility belongs to far more than one Army element. The Army's force protection? No, every Army commander is responsible for his own FP, and installation commanders are responsible for installation FP. The command's force protection? No, the command has no assets whatever in the state where the group resides.

"*The group is a threat to the National Guard*." When asked if the command had actually passed the information to the National Guard, however, the answer was "*no*." When asked if the command had considered that the state Adjutant General was already well aware of this militia group and its threats, it had not occurred to the command. When asked if the command had considered that the federal, state, and local law enforcement agencies—in whose jurisdiction the group was—were already well aware of and acting upon the information, the answer was "no."

While it might have been an interesting news item, it did not meet the "so what" criteria—basically, it was useless for military purposes.

- ❑ Impact on current or future command operations.
- ❑ Present an imminent threat to command personnel or materiel.
- ❑ Show a modus operandi of an international terrorist organization.
- ❑ Present a link to other activity that together could have shown a link to foreign powers or international terrorists.

It also resulted in several questionable intelligence activity reports, because some commands could not differentiate between an MI product and a fused FP product, or even what was actually relevant to the command.

At the present time, the fusion process seems to be little more than laundry lists of incidents. While it might be interesting reading, it offers nothing more than raw historical reports, and it led another command into **AR 381-10** difficulties.

(Also sanitized) This command's G2 shop started publishing "intelligence summaries" right after 11 September 2001. With good reason, many of its subordinate elements were nervous, and reported every suspicious incident immediately. They did not always report when they resolved an incident locally. The G2's intent was to alert subordinate elements to be on the lookout for similar suspicious activities at their locations, so that the command could determine if there was a pattern that could indicate terrorist pre-operational activity.

The "intelligence summary" was not actually an intelligence summary (INTSUM), as outlined in joint and Army doctrine. It was a mixture of law enforcement, physical security, security countermeasures, and MI informa-

tion. It had contained raw, unevaluated information, often with U.S. person information included—not only the suspect individual's identity but also the U.S. person who reported the information. The command did not publish any pattern analysis or clearly explain why this was MI information. It was a good start toward a fused FP product with security awareness training included, but the command was treating it like an MI product.

Because the command published raw incidents upon receipt, instead of waiting until the local element could resolve them or advise that they still were suspicious, the overall command may have had an inaccurate baseline of actual suspicious activity. If the subordinate element could quickly resolve it—such as a local who routinely entered the installation to fish, had done so for years, and whose presence was only now reported because he did not enter through the main gate—the incident should never have gone into a database, no matter whose database it was. There was no example for which other command elements should "be on the lookout," and no reason whatever to publish this U.S. person's identity. An analyst's assessment of reporting a U.S. person's likely credibility may have been useful, but there was no reason to identify the reporting person by name.

Avoiding Violations

How can your unit avoid an inadvertent violation of **AR 381-10**? Before incorporating information from another entity into your intelligence products, consider these questions:

- ❑ Was the product already disseminated to a large audience? The Army G3 Daily Force Protection Message, a fused intelligence and law enforcement product, goes to thousands of recipients worldwide, Army and non-Army. What value do you add by repeating it in an intelligence product? Could a repeat cause false confirmation or circular reporting? Could you violate **AR 381-10** by incorporating information not within your assigned intelligence mission?
- ❑ Is the information directly related to your assigned function, or is it simply interesting? You are not the news media. Stick to your assigned functions and areas of responsibility.
- ❑ Are you reporting incidents without any analysis? Can you link this and other incidents to clearly show a foreign modus operandi, a trend, or another indicator of international terrorist pre-operational activity? If so, report that analytical linkage. If not, what value are you adding?
- ❑ Is the U.S. person identification absolutely required for a full understanding of the reported incident or trend? If not, delete it. Remember, just because a non-Army agency reported it in an intelligence product, that does not mean you can copy and paste with impunity. The Army does not assign to MI the Army responsibility for physical security and law enforcement—if it is not within MI's assigned functions, simply pass it to the appropriate office for incorporation into their products.

Both DCS G2 memorandums, from Lieutenant General Robert W. Noonan, Jr., in 2001, and from LTG Claudia Kennedy in 1999, are still current (see page 9). Go to http://www.dami.army.pentagon.mil, click on *Projects*, then *Intel Oversight*, then *What's New*. Between those memos, the site's Frequently Asked Questions, and the current **AR 525-13**, you can chart who is responsible for what in Army FP, what the MI slice is at your level, and what products you need to produce.

As long as you can clearly articulate what your assigned MI function is (foreign threats and international terrorism), and why that U.S. person information is necessary to accomplish that assigned mission, you should be fine. Not knowing exactly what your MI job is gets one off track and into **AR 381-10** "hot water." Worse than that, getting off track can cause people to become overly concerned about nothing—wasting time, effort, and assets that they could have directed toward developing an accurate baseline of the local norm. From this, an FP information-fusion point could analyze the "spikes" out of the norm thus showing something requiring a response.

Concluding Thoughts

Homeland Security will continue to evolve, and changes in intelligence oversight may possibly occur. However, do not assume that MI now has "free rein" to gather information about the domestic activities of U.S. persons, lacking that foreign connection. Army MI slid down that slippery slope in the 1960s and 1970s. We will not make that mistake again. Stay calm, focus on what you are already authorized to do at your level, and let the decision makers document what changes they will allow within the IC.

Until then, if you still have questions or concerns that the intelligence oversight web pages do not seem to cover, please contact us at HQDA. We are watching closely for intelligence oversight interpretation changes outside the Army and reevaluating our own internal interpretation. Your concerns or inputs may well help us in the ongoing revision of **AR 381-10**.

Endnote

1. President George W. Bush signed the *USA PATRIOT Act (USAPA)* on 31 October 2001. The actual title of the *Act* passed by Congress is *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act*.

Regan Smith is the Intelligence Oversight Policy Proponent and a Counterintelligence (CI) Specialist in the Deputy Chief of Staff G2, HQDA. For 26 years, she has served in active, Reserve, and civilian positions in MI and military police (MP) units at all echelons. Readers may contact the author via E-mail at regan.smith@hqda.army.mil or through the "contact us" button at the Intelligence Oversight web page.

Intelligence Oversight Guidance From G2/DCSINT

This issue of the ***Military Intelligence Professional Bulletin*** features a number of articles discussing many aspects of Homeland Security, Homeland Defense, and Force Protection (FP). The following are guidance letters from the current Deputy Chief of Staff G2 and former Deputy Chief of Staff for Intelligence discussing information collection on U.S. persons and intelligence support to FP in the continental United States. The former is an extract of the reprint from the January-March 2002 issue of ***MIPB***.

Collecting Information on U.S. Persons

From Lieutenant General Robert W. Noonan, Jr., U.S. Army Deputy Chief of Staff G2, Memorandum, Subject: Collecting Information on U.S. Persons, dated 5 November 2001.

Many of the perpetrators of the attacks of 11 September 2001 lived for some time in the United States. There is evidence that some of their accomplices and supporters may have been U.S. persons, as that term is defined in **Executive Order (EO) 12333, United States Intelligence Activities**. This has caused concern in the field regarding the Military Intelligence (MI) Corps' collection authority. With that in mind, I offer the following guidance:

a. Contrary to popular belief, there is no absolute ban on intelligence components collecting U.S. person information. That collection, rather, is regulated by **EO 12333** and implementing policy in **DOD Directive 5240.1-R, Procedures Governing the Activities of DOD Components That Affect United States Persons**, and **AR 381-10, U.S. Army Intelligence Activities**.

b. Intelligence components may collect U.S. person information when the component has the mission (or "function") to do so, and the information falls within one of the categories listed in **DOD 5240.1-R** and **AR 381-10**. The two most important categories for present purposes are "foreign intelligence" and "counterintelligence." Both categories allow collection regarding U.S. persons reasonably believed to be engaged, or about to engage, in international terrorist activities. Within the United States, those activities must have a significant connection with a foreign power, organization, or person (e.g., a foreign-based terrorist group).

EO 12333 provides that—

timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence possible.

That said, my staff has received reports from the field of well-intentioned MI personnel declining to receive reports from local law enforcement authorities, solely because the reports contain U.S. person information. MI may receive information from anyone, anytime. If the information is U.S. person information, MI may retain that information if it meets the two-part test discussed in paragraph b, above. If the information received pertains solely to the functions of other DOD components, or agencies outside DOD, MI may transmit or deliver it to the appropriate recipients, per Procedure 4, **AR 381-10**. Remember, merely receiving information does not constitute "collection" under **AR 381-10**; collection entails receiving "for use." Army intelligence may always receive information, if only to determine its intelligence value and whether it can be collected, retained, or disseminated in accordance with governing policy.

Military Intelligence must collect all available information regarding international terrorists who threaten the United States, and its interests, including those responsible for planning, authorizing, committing, or aiding the terrorist attacks of 11 September 2001. We will do so—as **EO 12333** directs—

in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law, and respectful of the principles upon which the United States was founded.

Policy Guidance for Intelligence Support to Force Protection in CONUS

From Lieutenant General Claudia J. Kennedy, Previous Deputy Chief of Staff for Intelligence, Memorandum, Subject: Collecting Information on U.S. Persons, dated 19 February 1999.

AR 381-10, U.S. Army Intelligence Activities, governs Military Intelligence (MI) activities that affect United States persons, and states that authority to employ certain collection techniques is limited to that necessary to perform functions assigned to the intelligence component. **AR 381-12, Subversion and Espionage Directed Against the Army (SAEDA); AR 381-20, The Army Counterintelligence Program;** and **AR 525-13, Antiterrorism/Force Protection (AT/FP): Security of Personnel, Information, and Critical Resources**—more specific functions and responsibilities for intelligence support to force protection. DOD message,

(Continued on page 45)

Defining Homeland Security

by Lieutenant Colonel Patrick Kelly, III

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

Any appreciation of the role of intelligence relative to Homeland Security (HLS) begins with definitional issues. An examination of intelligence definitions will follow shortly, but the discourse must begin with the many definitional issues associated with HLS. The current administration is heavily engaged in the development of a National Security Strategy. Without this published document from the White House, we must extrapolate the HLS role within the national security from published remarks of President Bush and his staff as well as a review of the source documents of the previous Clinton Administration.

The President has spoken on numerous occasions since 11 September 2001 on the requirement to defend the homeland from terrorist attacks, most notably during his two addresses to Congress including his January 2002 State of the Union message. Additionally, **Executive Order 13228, Establishing the Office of Homeland Security and the Homeland Security Council**, signed on 8 October 2001, established the Office of Homeland Security. *"The mission of the Office [of Homeland Security] shall be to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."*[1] Headed by former Governor Tom Ridge, this organization has the unenviable requirement to stand up authorities and procedures while simultaneously prosecuting a complex campaign. There is every expectation that the National Security Strategy (NSS) will generate a companion National Homeland Security Strategy document. This strategy will join the National Military Strategy, the National Economic Strategy, and the National Foreign Policy Strategy in describing application of the elements of national power by the United States.

The requirements and strategy for HLS have been under development for some time. For the last half dozen years, numerous attempts wrestled with the issues of homeland defense (HLD) and HLS. The concepts codified in the National Security Strategy of 1996 were still discrete and described as counterterrorism (CT), fighting drug trafficking, and other missions. President Clinton introduced the requirements stating—

> *At the same time, the challenges to the security of our citizens, our borders and our democratic institutions from destructive forces such as terrorists and drug traffickers [are] greater today because of access to modern technology. Cooperation, both within our government and with other nations, is vital in combating these groups that traffic in organized violence. …Countering terrorism effectively requires close, day-to-day coordination among Executive Branch agencies.*[2]

By May 1997, the NSS outlined the requirements to protect against transnational threats that included terrorism, drug trafficking, international organized crime, and environmental and security concerns.

> *Combating these dangers which range from terrorism, international crime, and trafficking in drugs and illegal arms, to environmental damage and intrusions in our critical information infrastructures requires far-reaching cooperation among the agencies of our government as well as with other nations.*[3]

Throughout 1998 and 1999, the National Security Strategy continued to refine the HLS requirements. The maturation is clear in **A National Security Strategy For A New Century** from December 1999. In addition to a listing of transnational threats to the nation, the strategy clearly outlines components of the homeland defense. Although not quite a definition, these capabilities describe the requirements of HLD including national missile defense, countering foreign intelligence collection, domestic preparedness against weapons of mass destruction (WMDs), critical infrastructure protection, and national security emergency preparedness.

> *Adversaries may be tempted to use long-range ballistic missiles or unconventional tools, such as WMDs, financial destabilization, or information attacks, to threaten our citizens and critical national infrastructures at home. The United States will act to deter or prevent such attacks, and if attacks occur despite those efforts, will be prepared to defend against them, limit the damage they cause, and respond effectively against the perpetrators. At home, we will forge an effective partnership of Federal, state and local government agencies, industry, and other private sector organizations.*[4]

The culmination of the years of hard work and attention by the Clinton Administration to homeland security is their capstone strategy document, **A National Security Strategy for a Global Age,** published in December 2000. It states—

> *Emerging threats to our homeland by both state and non-state actors may be more likely in the future as our potential adversaries strike against vulnerable civilian targets in the United States to avoid direct confrontation with our*

military forces. Such acts represent a new dimension of asymmetric threats to our national security. Easier access to the critical technical expertise and technologies enables both state and non-state actors to harness increasingly destructive power with greater ease. In response to such threats, the United States has embarked on a comprehensive strategy to prevent, deter, disrupt, and when necessary, effectively respond to the myriad of threats to our homeland that we will face.[5]

Seven mission areas associated with protecting the homeland, combating terrorism, and fighting drug trafficking and other international crime join the five previously outlined areas: national missile defense, countering foreign intelligence collection, domestic preparedness against WMDs, critical infrastructure protection, and national security emergency preparedness. Even though it is not available on the White House homepage, this document remains the published national security of the United States; in fact, it became obsolete and politically irrelevant even upon publication. The bitter Bush-Gore presidential election and the Bush repudiation of the Clinton engagement strategy of "Shape, Respond, Prepare" doomed this strategic document.

The Clinton Administration outlined a broad concept of HLD while debating the delineation of a detailed definition. The U.S. Army initiated its parallel planning and began ongoing internal and external discussion of the roles, missions, responsibilities, and requirements of the Army for homeland defense. The first major contribution to the dialogue was the May 1999 U.S. Army Training and Doctrine Command (TRADOC) White Paper *Supporting Homeland Defense*. The doctrinal review of the HLD mission began with a postulated definition.

Doctrine must refine and codify the definition of homeland defense consistent with practice, policy, and National Command Authorities' emphasis. Currently, the Department of Defense (DOD) provides no official definition of homeland defense; therefore, the following is proposed. Homeland defense is protecting our territory, population and critical infrastructure at home by deterring and defending against foreign and domestic threats; supporting civil authorities for crisis and consequence management; and helping to ensure the availability, integrity, survivability, and adequacy of critical national assets.[6]

With the definitional framework established, the TRADOC White Paper outlined broad categories or mission areas for the U.S. Army.

The Army's role in homeland defense will fall into the following broad categories: force protection, support to crisis management, support to consequence management, protection of critical assets, support to counterterrorism, deterrence and defense against strategic attack, and [military assistance to civil authorities] MACA missions. Doctrine must expand, revise, or develop new guidelines to address each of these categories.[7]

Although superseded in subsequent doctrinal and definitional discussions, the definition and categories shaped the HLD debate within the DOD.

Always careful to defer to administration and departmental sensitivities about the evolving HLD mission areas, the Army continued its staff planning. The most obvious indicator of the political sensitivities associated with the undefined mission area was the migration of the concept in the winter of 2000 from "homeland defense" to "homeland security." In response to civil libertarian and bureaucratic concerns with the DOD's role in the evolving mission areas, Deputy Secretary of Defense John Hamre introduced the concept of "homeland security." Since its introduction, this concept has been used interchangeably with homeland defense without the necessary definitional clarity. On 10 September 2001, the Army published the coordinating draft of the Army Homeland Security (HLS) Strategic Planning Guidance.

The purpose of this document is to promulgate strategic planning guidance for the Army to support an Army HLS assessment and the continuing development of the Army role, missions, and functions associated with HLS. The Strategic Planning Guidance is designed to define the scope of operations, identify critical operational nodes, and provide a baseline for implementing the necessary processes, programs and systems to ensure it is capable of effectively and efficiently supporting HLS requirements.[8]

Included within the strategic planning guidance is a revised HLS definition modified from the original TRADOC HLD definition.

Homeland security is those active and passive measures taken to protect the population, area, and infrastructure of the United States, its possessions, and territories by: deterring, defending against, and mitigating the effects of threats, disasters, and attacks; supporting civil authorities in crisis and consequence management; and helping to ensure the availability, integrity, survivability, and adequacy of critical national assets.[9]

From this definition, the Army promulgated two broad mission areas and seven specific operations. Additionally the document outlined four tasks (deterrence, defense, crisis management, and consequence management) performed both before and after an incident.

Homeland Security consists of two broad mission areas, ***Homeland Defense*** *and* ***Domestic Support****, with distinct types of operations. This categorization derives from the definition for HLS and a review of previously published policy, guidance, and directives.*

❑ ***Homeland Defense*** *missions respond to the actions of a hostile or unwelcome force intruding on or attacking targets on U.S. sovereign territory. The missions associated with Homeland Defense include support [against] the following types of threats: Missile Attack; Air, Land, and/or Sea Sovereignty Incursion, Weapons of Mass Destruction Attack, and Cyber Attack.*

❑ ***Domestic Support*** *missions are conducted in reaction to or anticipation of a major disaster; act of civil disobedience, or to assist with a national-level event. The missions associated with domestic support include support to the following areas: Disasters, Civil Disorder, and Special Events.*[10]

The influence of the TRADOC and Army doctrinal work is evident in the current Joint Staff and Office of the Secretary of Defense definitions of HLS. In January 2002, the Joint Staff approved the following definitions:

Homeland Security: The preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggressions directed towards U.S. territory, sovereignty, domestic population, and infrastructure; as well as crisis management, consequence management, and other domestic civil support. Also called "HLS". See also homeland defense and civil support.

Homeland Defense: The protection of U.S. territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also called "HLD". See also homeland security and civil support.

Civil Support: Department of Defense support to U.S. civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called "CS". See also homeland security and homeland defense.[11]

The DOD's final codification of the four-year debate on HLS definitions is not yet finished. The Office of the Secretary of Defense (OSD) is an active participant in the development of the National Security Strategy and responsible for the National Military Strategy that will codify the Services' position. Without these two documents, we must infer the Army's position from other work. The Unified Command Plan (UCP) and the **Quadrennial Defense Review** (**QDR**) are two primary indicators of the Army's commitment to homeland security. Also not yet completed and classified, the Unified Command Plan might not normally provide public insight into such a critical issue; however, this year's efforts clearly indicate HLS activity. Recently the Secretary of Defense announced the formation of a tenth Unified Command, called U.S. Northern Command or NORTHCOM. With geographic responsibility for North America, this command will potentially be responsible for all coordination of homeland security missions, especially the interagency process with federal, state, and local officials.

A less tumultuous indicator of the OSD position on HLS is the **QDR**. Abandoning the Clinton strategy of engagement, the Rumsfeld Defense Department—

developed a new strategic framework to defend the nation and secure a viable peace. This framework is built around four defense policy goals: assuring allies and friends; dissuading future military competition; deterring threats and coercion against U.S. interests; and if deterrence fails, decisively defeating any adversary. [12]

Focusing on defending the United States and projecting U.S. military power, the defense strategy clearly states,

…defending the Nation from attack is the foundation of strategy…. Therefore, the defense strategy restores the emphasis once placed on defending the United States and its land, sea, air, and space approaches. It is essential to safeguard the Nation's way of life, its political institutions, and the source of its capacity to project decisive military power overseas.[13]

A new force-sizing construct emphasized up front the forces necessary to defend the United States and places *"new emphasis on the unique operational demands associated with the defense of the United States and restores the defense of the United States as the Department's primary mission."* [14]

The highest priority of the U.S. military is to defend the Nation from all enemies. The United States will maintain sufficient military forces to protect the U.S. domestic population, its territory, and its critical defense-related infrastructure against attacks emanating from outside U.S. borders, as appropriate under U.S. law. U.S. forces will provide strategic deterrence and air and missile defense and uphold U.S. commitments under NORAD [North American Aerospace Defense Command]. In addition, DOD components have the responsibility, as specified in U.S. law, to support U.S. civil authorities as directed in managing the consequences of natural and man-made disasters and CBRNE-related [chemical, biological, radiological, nuclear material, and high-yield explosives] events on U.S. territory. Finally, the U.S. military will be prepared to respond in a decisive manner to acts of international terrorism committed on U.S. territory or the territory of an ally.[15]

Recognizing shortfalls, the **QDR** assessment continues:

Ensuring the safety of America's citizens at home can only be achieved through effective cooperation among the many federal departments and agencies and state and local governments that have homeland security responsi-

bilities. It is clear that the roles, missions, and responsibilities of the many organizations and agencies involved in national preparedness must be clearly delineated through an integrated interagency process. The Office of Homeland Security, which is responsible for overseeing and coordinating a comprehensive national strategy to safeguard the United States against terrorism and respond to any attacks that may come, will lead this important process.[16]

Concluding with statements tinged with bureaucratic angst and the raw emotion of survivors of the Pentagon attack, the **QDR** paradigm shift embraces a next step not quite achieved by the Clinton national security team.

It was clear from the diverse set of agencies involved in responding to the 11 September 2001 terror attacks on the World Trade Center and the Pentagon that the Department of Defense does not and cannot have the sole responsibility for homeland security. DOD must institutionalize definitions of homeland security, homeland defense, and civil support and address command relationships and responsibilities within the Defense Department. This will allow the Defense Department to identify and assign homeland security roles and missions as well as examine resource implications. DOD must be committed to working through an integrated interagency process, which in turn will provide the means to determine force requirements and necessary resources to meet our homeland security requirements. DOD must bolster its ability to work with the organizations involved in homeland security to prevent, protect against, and respond to threats to the territorial United States. In particular, the Defense Department will place new emphasis upon [counterterrorism] training across federal, state, and local first responders, drawing on the capabilities of the Reserve and National Guard. Integration of protection mechanisms (e.g., counterintelligence, security, infrastructure protection, and information assurance) will be a key component. In particular, the United States must enhance its capabilities to protect its critical infrastructure, especially infrastructure that supports oil and gas transportation and storage, information and communications, banking and finance, electrical power, transportation, water supply, [and] emergency and government services. [17]

The **QDR** report of 30 September 2001 is one of the first official documents the Bush Administration published specifically addressing HLS. Outlining a new defense strategy and anticipating a new NSS, they wrote, debated and revised this document before the events of 11 September 2001 with only a coda of acknowledgement that the future was upon us sooner than anticipated. In many ways, the **QDR** assessment of HLS derives from the last published Clinton NSS. When correlated, six of the Clinton seven mission areas protecting the homeland are in the **QDR** assessment. Only fighting drug trafficking and other international crime, not specifically a Defense Department mission anyway, is missing from the priority HLS missions. As witnessed during the first six months of the Global War on Terrorism, and the President's January 2002 State of the Union message—in which he said, *"Stricter border enforcement will help combat illegal drugs"*[18]—this mission area may yet also survive as a component of HLS since it is so closely intertwined with combating terrorism.

As admitted by the **QDR** report, we need definitions for HLS. In fact, neither Congress nor the Executive Branch has defined HLS. Congressional deference to the Executive Branch's responsibilities is evident, though not absolute, throughout the debate on HLS. Congress did take the opportunity to enter the debate through *The National Homeland Security Act of 2001* (House Resolution 1158), sponsored by Representative Mack Thornberry (Republican-Texas) and the *National Homeland Security Strategy Act of 2001 (*House Resolution 1292). This proposed bill, introduced in March 2001 by Representative Ike Skelton (Democrat-Missouri), defines HLS as,

the protection of the territory, critical infrastructures, and citizens of the United States by Federal, state, and local government entities from threat or use of chemical, biological, radiological, nuclear, cyber or conventional weapons by military or other means.[19]

This broadly scoped definition indicates Congress' central concern with WMDs.

The scope of WMD in this proposed legislation is expanded with the addition of "conventional weapons" and falls more in line with the Title 18 [Crimes and Criminal Procedures] of The United States Code definition of WMD and the acronym CBRNE. Also apparently excluded from this definition as a part of HLS is the element of natural disasters as defined in the Stafford Act and Title 10 [Armed Forces], USC.[20]

Following the events of 11 September 2001, congressional attention to the homeland security debate has manifested in a number of resolutions, task forces, and bills. Most germane to the issue of defining Homeland Security and intelligence support to HLS are the *USA PATRIOT Act of 2002*[21] and the *Intelligence Authorization Act* for Fiscal Year 2002.

President Bush created the Office of Homeland Security on 8 October 2001 in response to the terrorist events of 11 September 2001, as well as in response to the recommendations contained within bills like the *Homeland Security Strategy Act of 2001* and reports from influential commissions such as the Report from the United

States Commission on National Security/21st century (also known as the Hart-Rudman Commission) and The Commission on Counter-Terrorism (also known as the Gilmore Commission). Earlier, in May 2001, responding to congressional and commission recommendations, the President designated Vice President Dick Chaney to lead the domestic preparedness effort as outlined in a statement on "Domestic Preparedness Against Weapons of Mass Destruction." The events of September 11 greatly accelerated the administration focus on HLS.

The President is committed to a clear articulation of a national strategy for HLS, the mission given to the Office of Homeland Security. Functions have been codified as *"coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to and recover from terrorist attacks within the United States."* [22] The timeline pronounced in the President's statement on "Securing the Homeland, Strengthening the Nation" is this year. Declaring HLS *"A New National Calling,"* the President's commitment is steadfast:

> *The higher priority we all now attach to homeland security has already begun to ripple through the land. The Government of the United States has no more important mission than fighting terrorism overseas and securing the homeland from future terrorist attacks. This effort will involve major new programs and significant reforms by the Federal government. But it will also involve new or expanded efforts by State and local governments, private industry, non-governmental organizations, and citizens. By working together, we will make our homeland more secure.*[23]

In his State of the Union speech, President Bush declared: *"My budget nearly doubles funding for a sustained strategy of homeland security, focused on four key areas: bioterrorism, emergency response, airport and border security, and improved intelligence."*[24] These four areas are an immediate budgetary focus; the President also promises *"the strategy will be comprehensive. It will encompass the full range of HLS activities and will set priorities among them."* [25]

Here then is a presidential directive for a comprehensive, holistic strategy for Homeland Security promising challenges *"of monumental scale and complexity"* requiring a long-term, national (not just Federal) opportunistic, objective-oriented, multiyear budgeted plan.[26] With the publication of the National Strategy for Homeland Security, we will almost certainly obtain a definitive definition of Homeland Security. When published, it is almost certain that Intelligence will remain integral to the strategy.

Endnotes

1. George W. Bush, **Executive Order 13228**, **Establishing the Office of Homeland Security and the Homeland Security Council** (Washington, D.C.: The White House, 8 October 2001), page 1.
2. William J. Clinton, **A National Security Strategy of Engagement and Enlargement** (Washington, D.C.: The White House, February 1996), pages 19-20. See the electronic copy of the 1996 National Security Strategy at http://www.fas.org/spp/military/docops/national/1996stra.htm.
3. William J. Clinton, **A National Security Strategy for a New Century** (Washington, D.C.: The White House, May 1997), page 13. The electronic copy of the 1997 National Security Startegy is at http://clinton2.nara.gov/WH/EOP/NSC/Strategy/.
4. William J. Clinton, **A National Security Strategy for a New Century** (Washington, D.C.: The White House, December 1999), page 16. An electronic copy of the 1999 National Security Strategy is at http://Clinton4.nara.gov/media/pdf/nssr-1229.pdf.
5. William J. Clinton, **A National Security for a Global Age** (Washington, D.C.: The White House, December 2000), page 20.
6. Department of the Army, U.S. Army Training and Doctrine Command (TRADOC), *Supporting Homeland Defense*, White Paper (Norfolk, Virginia: U.S. Department of the Army, May 1999, page 1.
7. Ibid., page 4.
8. Department of the Army, **Army Homeland Security (HLS) Strategic Planning Guidance** (Washington, D.C.: Department of the Army, 10 September 2001), pages 1 and 2.
9. Ibid. page 6.
10. Ibid.
11. Department of the Army, "JCS Approved HLS Definitions," briefing slide from the Army G8 Deputy Chief of Staff for Programs, Headquarters, Department of the Army, 14 February 2002.
12. Department of Defense, **Quadrennial Defense Review** (Washington, D.C.: Department of Defense, 30 September 2001), page 11.
13. Ibid., page 14.
14. Ibid., page 17
15. Ibid., page 18.
16. Ibid.
17. Ibid., pages 19 and 20.
18. George W. Bush, "The President's State of the Union Address" (Washington, D.C.: The United States Capitol, 29 January 2002). The text of the President's State of the Union speech is at http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html.
19. **Army HLS Strategic Planning Guidance**, page 9.
20. Ibid.
21. The full name of the *Act* is *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act*.
22. **Executive Order 13228,** page 1.
23. George W. Bush, **Securing the Homeland, Strengthening the Nation** (Washington, D.C.: The White House, February 2002), page 3. The President's homeland security policy and budget priorities statement is at http://www.whitehouse.gov/homeland/homeland_security_book.html.
24. "State of the Union."
25. Bush, **Securing the Homeland, Strengthening the Nation**, page 6.
26. Ibid. The criteria listed are from the President's highlighted plan for a National Strategy for Homeland Security. The complete list is on pages 6 and 7.

Lieutenant Colonel (P) Patrick Kelly, III, is the 2002 U.S. Army Fellow at the Center for Strategic Studies (CSIS). His most recent assignment was as the Chief, Force Planning and Interrogation Team, Army War Plans Division, Headquarters, Department of the Army. His prior assignment was Senior Intelligence Officer (G2), 1st Calvary Division, including one year as the senior intelligence officer of Task Force Eagle and the MultiNational Division-North (MND-N) of the Stabilization Force (SFOR) in Bosnia-Herzegovina. LTC Kelly's fellowship research project is Intelligence Support to Homeland Security. Readers can reach him via E-mail at pkelly@csis.org and by telephone at (202) 775-3288.

The 902d Military Intelligence Group and Homeland Security

by Colonel Ginger T. Pratt

The 902d Military Intelligence Group, headquartered at Fort George G. Meade, Maryland, is the U.S. Army's largest strategic counterintelligence (CI) organization. Activated as the 902d Counter-Intelligence Corps (CIC) Detachment in New Guinea on 23 November 1944, the "Deuce" has a proud history as a CI organization. The 902d's role in 1944 was basically the same as it is now: to counter the foreign intelligence services (FISs) and organizations that attempted to collect against the U.S. Army. Over time, the organizations and techniques may have changed but the threat of espionage against the U.S. Army remains. During the Cold War, the threat was from the Soviet Union and the Warsaw Pact; today, the threat exists from traditional organizations like the former KGB[1], as well as new FISs and international terrorist organizations. The diversity of these threats to the U.S. Army requires us to apply our traditional counterintelligence capabilities in innovative ways to defeat these increasingly complex threats. The focus of the 902d MI Group's contribution (five articles) to this professional journal is how the "Deuce" has evolved to meet these new threats to the U.S. Army.

An Evolving Mission

The mission of the 902d MI Group is to protect our nation's forces, secrets and technologies by detecting, neutralizing, and exploiting FISs and international terrorist organizations. The traditional mission of the 902d has always been the detection, neutralization, and exploitation of FISs; however, as the threat from international terrorism increased against the U.S. Army, the 902d by direction focused its capabilities against this threat as well.

During the past ten years, the FISs and international terrorist organizations have improved their methods of collecting against the U.S. Army. These techniques include exploitation of digital Internet links and telecommunications as well as improved methods of information elicitation. As the diversity and sophistication of the threat increased, the 902d evolved its capability to counter these threats. The "Deuce" accomplished this by focusing its core competencies of collection, investigations, operations, analysis and production, functional services, and training against these "asymmetric approaches" used by FISs and international terrorist organizations. The 902d was already redirecting its core competencies against these asymmetric approaches when the terrorists struck on 11 September 2001. Since then, the 902d has continued to refine and focus these core competencies against these newest threats of international terrorism.

The attacks on September 11 resulted in the 902d MI Group assuming a major role in support of the Homeland Security (HLS) mission. However, before September 11, **Army Regulation 525-13**, **Antiterrorism Force Protection: Security of Personnel**, **Information and Critical Resources** (dated 10 September 1998), mandated that the 902d MI Group collect, analyze, and disseminate foreign threat information to the U.S. Army. Before September 11, the terrorist attacks against U.S. Army organizations and installations were all in foreign countries, which restricted the 902d's ability to collect because our primary area of responsibility is the continental United States (CONUS). However, the Army Counterintelligence Center (ACIC)—the analytical and production component for the 902d and Army counterintelligence—produced and disseminated products on international terrorism threat throughout the U.S. Army. The attacks on September 11 caused the 902d to focus entirely on the investigation of those attacks and the prevention of future attacks in the United States, thus thrusting the 902d into the HLS arena as the U.S. Army's primary CI organization.

902d Support to the Army HLS Mission

The U.S. Army's role for the Homeland Security mission is still under development. However, the newest version of **AR 525-13**, **Antiterrorism** (dated 4 January 2002), mandates antiterrorism (AT) requirements at all levels, from Department of the Army level to installation. The Army Deputy Chief of Staff (DCS) G3 is responsible for operating the Army's Antiterrorism Operations Intelligence Cell (ATOIC) in the Army Operations Center (AOC). The 902d supports the ATOIC by providing collected foreign and international terrorist threat information to them. The 902d fulfills a major role for the U.S. Army's Antiterrorism Program from the Department of the Army level to installation level, as illustrated in the examples below.

TRADOC. The Commanding General (CG), U.S. Army Training and Doctrine Command (TRADOC), is responsible for developing, implementing, and updating appropriate AT training programs across the U.S. Army. The "Deuce" supports the CG, TRADOC, by providing foreign and international terrorist threat information to all TRADOC installations and organizations.

INSCOM. The CG, U.S. Army Intelligence and Security Command

(INSCOM), is responsible for the collection, analysis, and dissemination of foreign and international terrorist threat information to U.S. Army commanders. The "Deuce," as one of INSCOM's major subordinate commands, functions as the primary CI organization responsible for the collection, analysis, and dissemination of this foreign and international terrorist threat information to INSCOM.

Installations. Installation commanders at all levels are responsible for establishing AT programs at their installations and designating a focal point for receipt and dissemination of time-sensitive threat information from intelligence and law enforcement agencies. The 902d supports the installation commanders by providing CI personnel to advise and assist their AT officers. The Group also provides the installation commanders disseminated foreign and international terrorist threat information.

The 902d In Army Transformation

The 902d MI Group, as the U.S. Army's premier CI organization, executes its mission in direct support (DS) to the U.S. Army in CONUS in support of HLS. Now that the terrorists have struck inside the United States, the 902d should be part of future versions of the Army Intelligence Transformation Campaign Plan. The current Army Intelligence Transformation Campaign Plan, from August 2001, did not adequately address the future transformation of strategic units like the 902d MI Group. It is fair to say that the current development of the Army Intelligence Transformation Campaign Plan was to illustrate how Army Intelligence would support the U.S. Army's Interim, Legacy, and Objective Forces. This campaign plan was developed before 11 September, and no one could foresee the tragic events of that day. However, as the HLS mission matures, the 902d will evolve as well and its requirements need to be addressed in these plans.

As stated in the current Army Intelligence Transformation Campaign Plan, the Army Intelligence core competencies are—

- Full dimension **protection**.
- Physical and cyber domains.
- Unique **collection** to cover information gaps.
- **Integration** of all intelligence and non-intelligence sensors to build the relevant "Red" pictures and "Gray" pictures.
- **Analysis** to transform data into information and that information into knowledge.
- **Presentation** of knowledge in a format and manner that imparts immediate understanding.

The 902d Group must benefit from the future resourcing, training, and equipment inherent with these core competencies to enable its transformation to meet the future demands of the HLS mission.

Conclusion

The 902d MI Group has responded well to the challenges of its DS role for HLS. We have leveraged the immense capabilities of our soldiers, civilians, and contractors to support the investigation of the September 11 attacks and to prevent future attacks in the United States. The 902d conducted an unprecedented number of investigative and operational activities in support of the Federal Bureau of Investigation after September 11. The ACIC produced the U.S. Army's only daily terrorism summary starting on 13 September and continues to produce this summary today. The 902d stood up the Counterintelligence Analysis and Control Element (CI ACE) to fuse force protection and terrorist threat information and to provide situational awareness to U.S. Army commanders in CONUS. The "Deuce" has met all requirements levied on us to support Homeland Security while still maintaining our capability to counter the foreign intelligence threat against the U.S. Army. The 902d Military Intelligence Group is currently transforming in preparation for the future with enthusiasm and energy. We believe the future is bright and that the 902d's capabilities—current and future—bring confidence to the U.S. Army leadership that we will win all future conflicts here and overseas.

Endnote

1. Komitel Gossudarrstvennoi Bezopastnosti (the Soviet Committee for State Security).

Colonel Ginger Pratt is the Commander, 902d Military Intelligence Group, at Fort Meade, Maryland. Her previous command positions include the 308th MI Battalion, 902d MI Group; the Fort Meade and Fort Leavenworth MI Detachments, MI Battalion (CI), 902d MI Group; and the Headquarters and Headquarters Operations Company, 102d MI Battalion (CEWI), 2d Infantry Division (2ID). Colonel Pratt recently served as the Chief, Information Operations, Headquarters, Department of the Army, Office of the Assistant Chief of Staff for Intelligence. She has served in numerous other important staff positions including Security Review Officer, Office of the Assistant Secretary of Defense for Public Affairs; J2 Forward, Joint Task Force (TF) Provide Promise, in Zagreb, Croatia; Operations Officer/S3, 527th MI Battalion; Executive Officer (XO), Office for the Deputy Chief of Staff for Intelligence, United States Army-Europe; XO, TF Brief Pause, Office of the Army Chief of Staff; Group S2, 902d MI Group; and Battalion S2, 102d MI Battalion (CEWI), 2ID. COL Pratt earned her commission as a Second Lieutenant through Officer Candidate School after her Bachelor of Arts degree in French from Lee University, Cleveland, Tennessee. She holds a Master of Arts degree in Counseling Psychology from Bowie State University, Bowie, Maryland, and she has recently completed a Master of Arts degree in Strategic Studies at the U.S. Naval War College. She is a graduate of the Armed Forces Staff College for Joint Professional Military Education (Phase II), a number of Army leaders courses, the Defense Language Institute (Arabic/EG), and Airborne School. Readers may contact COL Pratt through S3 Plans via E-mail (Minerva) at tinam@meade-inscom.army.mil and telephonically at (301) 677-2366 or DSN 622-2366.

U.S. Army Counterintelligence Center Support to Homeland Security

by Charles Harlan

The mission of the U.S. Army Counterintelligence Center (ACIC) is to provide timely, accurate, and effective multidiscipline counterintelligence (MDCI) and terrorism analysis in support of the Army, sustaining base commanders, continental United States (CONUS)-based deploying forces, ground system technologies, and counterintelligence (CI) investigations and operations. While the ACIC has always played a role in missions traditionally associated with Homeland Security (HLS) and Homeland Defense (HLD), the terrorist attacks on 11 September 2001 resulted in a refocusing of priorities and will result in long-term changes in how the ACIC does business.

ACIC Background

The ACIC is a crucial component of the DOD intelligence production effort. Each Service maintains a Service-level production center that produces general military intelligence (GMI) and scientific and technical intelligence analysis and production. Under the DOD CI Production Program, each Service's own CI elements conduct Service-level CI analysis and production rather than having it done by the GMI production centers. The National Ground Intelligence Center (NGIC) is the Army's main GMI production center.

ACIC analysis focuses on four basic functional areas: technology protection, force protection (FP), information operations (IO), and support to CI investigations and operations. Work performed by the ACIC is managed under the DOD Intelligence Production Program (DODIPP).

The ACIC is the primary intelligence producer for intelligence and security threats to developmental U.S. ground systems and technologies. The Center is also a collaborative producer for other CI areas to include foreign intelligence and foreign security agencies, international terrorism and counterterrorism (CT), and ground forces IO and information warfare issues.

The ACIC is an active player in all aspects of the intelligence cycle. ACIC products provide threat information that supports the planning and direction of Army Intelligence activities. ACIC analysts provide intelligence collectors with feedback on their intelligence reports, identify intelligence gaps, and prepare collection-emphasis reports as a means of helping focus intelligence collection activities.

Support to Homeland Defense

The terrorist attacks on 11 September 2001 resulted in an immediate refocusing of ACIC analytic support to CT and FP, both of which are critical elements of intelligence support to HLD. To support CT and FP requirements, the ACIC created a current intelligence operations cell (CIOC) and task-organized based on priorities of intelligence production requirements. On a daily basis, teams of analysts, lead by senior analysts, identified new sources of CT and FP information, culled through a large volume of intelligence reports, and began the process of synthesis and analysis. The ACIC supported both scheduled and ad hoc CT and FP production requirements. ACIC analysts identified CT and FP intelligence gaps and prepared a variety of reports and assessments, to include assessments of critical nodes and infrastructure, terrorist threats to the U.S. Army in CONUS, country and regional threat assessments, and daily CT and FP assessments.

The 902d MI Group and the U.S. Army Intelligence and Security Command (INSCOM) also responded to the September 11 attacks by creating new CIOCs and refocusing existing analytic resources. On 1 November 2001, the 902d MI Group officially opened its Counterintelligence Analysis and Control Element (CI ACE) for business. We created the CI ACE to enhance intelligence support to Army commanders in CONUS by providing a daily graphical product that commanders can use to assess security threats in their areas of responsibility. The ACIC CIOC and CI ACE work closely together, developing daily threat assessments that they fuse and forward to the INSCOM Information Dominance Center (IDC). The ACIC provides the CI ACE with analytic advice and assistance, and augments the CI ACE with experienced CI analysts. While the mission of the ACIC will continue to be the "big picture" in support of the Army, the ACIC and CI ACE will work together to ensure the identification and filling of CT and FP intelligence gaps in CONUS. The ACIC will be an integral part of the new 902d MI Group's Operations Center, working with the CI ACE to provide a complete analytical picture for the 902d MI Group's customers.

Liaison Officers and Reservists

The exchange of liaison officers (LNOs) between the 902d MI Group and the U.S. Army Criminal Investigations Command enhanced the ability of the ACIC and the 902d MI Group to support CT and FP. The goal of these LNOs is to improve the exchange of intelligence and law enforcement information and to improve each agency's CT and FP missions. This arrangement has proven extremely effective so far and will continue indefinitely. The success of the LNOs is indicative

of positive changes in the relationship between Army intelligence and CID. Reservists called up to support INSCOM and 902d CT and FP requirements are working with CID, with the Joint Intelligence Task Force-Counterterrorism (JITF-CT), and serving as CT and FP analysts in the ACIC and the CI ACE.

Final Thoughts

The attacks on September 11 highlighted the vulnerability of the United States to foreign terrorist attacks. The future role of the Army and the ACIC in HLS has not been clearly defined, but the Army can expect to have a significant role in identifying threats to the United States and supporting the national HLS program. The ACIC will continue to support CT and FP requirements through long-range studies and threat assessments, identification of critical Army infrastructure, and support to Homeland Defense programs. The ACIC has resumed its support to other Army customers and production of previously scheduled production requirements, but maintains the ability to stay focused on CT and FP as needed.

Charles Harlan began his career with U.S. Army Intelligence as a Department of the Army Civilian at the 902d MI Group, Fort George G. Meade, Maryland. He is currently assigned to the Army Counterintelligence Center (ACIC) as the Senior Analyst in the Technology Protection Branch. Readers may contact the author via E-mail (Internet/MINERVA) at harlanc@meade-inscom.army.mil and telephonically at (301) 677-4030 or DSN 622-4030.

From the Editor

(Continued from inside front cover)

procedures issued by the agency head and approved by the Attorney General. **AR 381-10, U.S. Army Intelligence Activity**, establishes the responsibility for intelligence activities concerning U.S. persons, includes guidance on the conduct of intrusive intelligence collection techniques, and provides reporting procedures for certain federal crimes.

AR 381-10 implements—

- ❑ **Executive Order 12333.**
- ❑ **DOD Directive 5240.1**, **DOD Intelligence Activities.**
- ❑ **DOD Regulation 5240.1-R**, **Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.**
- ❑ **DOD Instruction 5240.4**, **Reporting of Counterintelligence and Criminal Violations**.

AR 381-10 applies to the Active Army, the U.S. Army National Guard, and the U.S. Army Reserve. It also applies to Army intelligence components and those non-intelligence components conducting intelligence activities.

This issue also includes an extract of a memorandum signed by Lieutenant General Robert W. Noonan, Jr., Subject: Collecting Information on U.S. Persons, on 5 November 2001. In the memorandum, LTG Noonan offered the following guidance:

a. Contrary to popular belief, there is no absolute ban on intelligence components collecting U.S. person information. Rather, **EO 12333** and implementing policy in **DOD 5240.1-R** and **AR 381-10** regulate that collection.
b. Intelligence components may collect U.S. person information when the component has the mission (or "function") to do so, and the information falls within one of the categories listed in **DOD 5240.1-R** and **AR 381-10**.

LTG Noonan also explained that—

MI may receive information from anyone, anytime. If the information is U.S. person information, MI may retain that information if it meets the two-part test discussed in paragraph b above.

Finally, the subject is again addressed in this issue by a memorandum signed by LTG Claudia J. Kennedy, Subject: Policy Guidance for Intelligence Support to Force Protection in CONUS, on 19 February 1999.

As each article discusses intelligence collection to support antiterrorism, force protection, and Homeland Security, although not specifically cited or caveated, active adherence to Intelligence Oversight policy is implied.

JAC/JRISE Needs MI Reservists

The Joint Analysis Center/Joint Reserve Intelligence Support Element (JAC/JRISE) located in Atlanta, Georgia, is looking for branch-qualified Military Intelligence officers (35B/D), warrant officers (350B, 350D), and enlisted personnel (96B, 96D). Applicants must have a current TS/SCI security clearance and be MOS-qualified. Unit members typically drill at Fort Gillem, Georgia, for IDT, ADT, and AT but also participate in mission work at the Joint Analysis Center in the United Kingdom and other overseas assignments on an as-needed basis. In addition, this unit offers training, challenging work (supporting real-world intelligence missions), flexible scheduling, and combined IDTs. Interested soldiers should contact SGT Campbell, the JAC/JRISE Recruitment NCO, at (404) 469-3151 or DSN 797-3151.

The 902d MI Group's CI ACE—A Center of Information Fusion and Situational Awareness

by Major Arthur F. Palaganas

The tragic events that occurred on 11 September 2001 made all of us in the Intelligence Community examine the way we conducted business, particularly in the areas of force protection (FP), combating terrorism, and Homeland Security (HLS). When the 902d Military Intelligence Group began providing counterintelligence (CI) support for HLS, the Group determined that it needed to be able to provide information to the 902d's supported commanders and other customers rapidly. Specifically, the 902d needed to fuse information quickly, create comprehensive situational awareness products for both the U.S. Army and the Department of Defense (DOD), and to disseminate these products rapidly to a myriad of agencies. The 902d also needed to improve its ability to predict where and when terrorists might strike again in the continental United States (CONUS).

The 902d had been planning to initiate an operations center in fiscal year 2002, as a means to synchronize the Group's varied operations. A counterintelligence analysis and control element (CI ACE) was an integral part of the concept for the new 902d MI Group Operations Center. To meet the new requirements of information fusion, situational awareness, and predictive analysis, the 902d began operating its CI ACE before the operations center was running. On 1 November 2001, with minimal staffing and resources, the CI ACE became operational.

CI ACE Mission

The mission of the CI ACE is to:

Conduct information fusion, achieve situational awareness and conduct predictive analysis to protect U.S. Army installations, personnel, and technologies. Integrate with the 902d Military Intelligence Group Operations Center to conduct operational synchronization to achieve situational dominance.

The CI ACE conducts its mission using the doctrinal intelligence cycle.

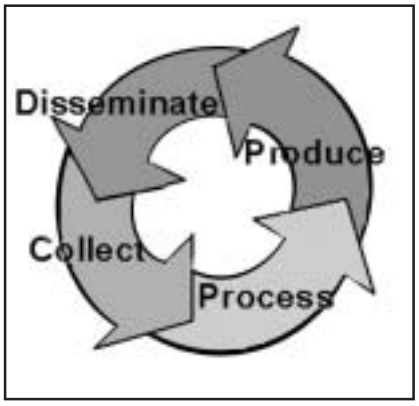


Figure 1. The Doctrinal Intelligence Cycle.

Collect. Receive information collected by 902d CI agents across CONUS and selected worldwide locations, CI and law enforcement counterparts in DOD and the federal government, and from open sources.

Process. Validate, evaluate, and correlate data, supported by intelligence software tools such as the All-Source Analysis System-Light (ASAS-L) and the Analyst Notebook to fuse information into graphical form.

Produce and Disseminate. Develop a variety of products to include link-analysis diagrams, threat pictures, and target folders. The CI ACE disseminates these products to various customers for situational awareness and operational synchronization. The CI ACE's production goal is to provide a unique product that does not duplicate work done by other agencies. It works closely with the 902d MI Group's Army Counterintelligence Center (ACIC) in the development of daily threat assessments. The ACIC provides analytical advice and assistance to the CI ACE, and augments it with experienced CI analysts. While the mission of the ACIC will continue to be the "big picture" in support of the Army, the ACIC and CI ACE will work together to ensure that they identify and fill counterterrorism (CT) and FP gaps in CONUS.

Creation and Organization of Current CI ACE

The formation of the CI ACE drew personnel and resources from within the 902d MI Group. Currently, there are 16 military and civilian analysts in the CI ACE, and they have done a superb job in building the CI ACE in record time. When the CI ACE stood up on 1 November 2001, it initially focused on building the threat picture from a CI perspective in support of FP and counterterrorism missions. The organization of the CI ACE is in analytical cells that reflect the mission sets of the 902d.

The **Force Protection Analysis Cell** provides local and regional situational awareness to support FP activities in assistance to installation and major Army command (MACOM) commanders and for troops in transit. The CI ACE disseminates force protection products via multiple media sources. The primary dissemination channel to the installations and the MACOMs is the Secure Internet Protocol Router Network (SIPRNET), a network used to process classified information up to the Secret level. The CI ACE also disseminates finished products via the local 902d resident offices. Additionally, analysts in the CI ACE pass their database to the U.S. Army Intelligence and Security Command (INSCOM) Information Dominance Center (IDC) where it merges into the IDC's database to produce an all-source intelligence picture. Furthermore, these products are provided to Headquarters, INSCOM, and archived on the CI ACE website for future reference. Readers can access the CI ACE website through the SIPRNET at 902dmi.north-inscom.army.smil.mil/902d/ci-ace/.

The **Counterterrorism Analysis Cell** supports the 902d's CT mission by developing comprehensive pictures of the terrorist elements, networks, and other information. The cell fuses and analyzes information in support of antiterrorism. This cell will often control its dissemination more tightly because of proprietary restrictions from federal agencies.

Developmental CI ACE Cells

The CI ACE is becoming an effective force multiplier for the 902d by developing the threat picture for the 902d's missions to include technology protection, activities to counter foreign intelligence services (FISs), and computer network operations. The analytical cells supporting these missions are still under development and resourcing.

The **Technology Protection** and **FIS Analysis Cells** will apply the same techniques and tools used in FP and CT but against a different set of data. These cells will produce target support packages based on the information they gather from a variety of sources; the target support packages will go to the 902d field elements and to other federal agencies, thereby allowing operational synchronization to neutralize or exploit foreign threats to Army activities.

The **Information Operations (IO) Analysis Cell** will work closely with the 902d MI Group's Information Warfare Branch to conduct cyberintelligence preparation of the battlespace and to correlate this information with the other target sets to determine any trends or patterns. By fusing the cyberthreat picture with the information from the other analysis cells, we can develop a more comprehensive picture of the threat. The CI ACE's **Fusion Cell** will perform the challenging job of fusing the numerous graphical data into a comprehensive threat picture.

The CI ACE has quickly developed to become a critical player in the Intelligence Community. Fostering the daily exchange of information and analysis with our sister Services and federal agencies has been essential to its analytical capabilities. Our sister Services, the Federal Bureau of Investigation (FBI), and other DOD organizations have used the CI ACE products. As a result, these organizations have increased their sharing of information with the CI ACE.

What Is Ahead For the CI ACE?

The CI ACE will continue to foster the working relationship with DOD and other federal agencies and look into leveraging other software, systems, and technologies to develop further the comprehensive situational awareness picture. Members of the 902d MI Group developed an automated incident submission form, which enhances the timeliness of information receipt and streamlines information-sharing across the group. We will electronically fuse this information into the CI ACE database that is the foundation of the interactive website used to share information with the MACOMs and installation commands. The CI ACE is changing how the 902d MI Group conducts CI operations; therefore, it is important for the CI ACE to start documenting its tactics, techniques, and procedures.

In the near future, the 902d's Operations Center will be fully operational. Within the Operations Center, the CI ACE will integrate with other elements of the Group S3 staff elements. The Operations Center will serve as the 902d MI Group's hub for synchronization, synergy, and fusion, allowing the CI ACE to produce the situational awareness picture that will drive the Group's operations. The CI ACE's integration into the Operations Center will combine situational awareness with operational synchronization to achieve "**situational dominance**."

Major Arthur Palaganas is currently serving as the Chief, Counterintelligence Analysis and Control Element (CI ACE), 902d MI Group, at Fort Meade, Maryland. MAJ Palaganas was responsible for establishing the CI ACE, directing its daily operations, and planning and developing its future growth and functions. His previous assignments include "dual-hatting" as Deputy G2, 5th Signal Command, and Chief, Joint Surveillance Target Attack Radar System (Joint STARS) Training Development, U.S. Army, Europe (USAREUR); Deputy Information Assurance Program Manager; MI Company Commander; Infantry Battalion S2; Assistant Secretary General Staff; Battalion Maintenance Officer; Armor Company Executive Officer; and Armor Platoon Leader. He has a Bachelor of Science degree from the University of Guam. Readers may contact the author via E-mail at arthur.palaganas @meade-ins com.army.mil and by telephone at (301) 677-3893 or DSN 622-3893.

CI Technical Capabilities for Homeland Security

**by Captain
Elizabeth M. Duncklee and
First Lieutenant
Jeremy J. McKnight**

Technical counterintelligence (CI) capabilities have proven to be invaluable assets in the Global War on Terrorism. Within the mission of Homeland Security (HLS) is the inherent task of reducing incidents by enhancing preparedness, protection, and response capabilities within the United States. The 310th Military Intelligence Battalion is responsible for conducting worldwide technical operations and investigations in support of CI and counterespionage activities. By design, it plays a crucial role in detecting, neutralizing, and exploiting foreign intelligence services. As part of the 902d MI Group, the 310th MI Battalion provides unique capabilities to aid HLS and supply needed technical security vital to the U.S. Army and Department of Defense (DOD) assets.

Technical HLS Assets

To accomplish its HLS mission, the military intelligence community needs to leverage the following technical assets:

- ❑ Information warfare operations.
- ❑ Polygraph operations.
- ❑ Technical surveillance and countermeasures force protection (FP) operations.

Each unique program covers a specific area to reduce vulnerabilities within the United States and worldwide.

The **Information Warfare Branch** (IWB) conducts diverse CI operations and investigations. The IWB leads computer forensic operations and investigations of electronic media to detect computer intrusions. It works closely with other federal agencies in conducting forensic analysis. Successes in the area have been recognized at the national level for our timely and thorough electronic forensic analysis and network intrusion detection investigations. IWB provides superior capabilities in support of the 902d MI Group's CI mission for HLS.

The **Polygraph Detachment** provides worldwide support to CI and counterespionage operations for the U.S. Army. Their specific missions include:

- ❑ Conducting counterintelligence scope polygraph (CSP) examinations to support several DOD agencies.
- ❑ Conducting polygraph examinations to support the Department of the Army Cryptographic Access Program (DACAP).
- ❑ Standard polygraph missions.

Basic polygraph activities consist of support to contingency operations, FP operations, contractor linguist screening, and counterespionage investigations.

Finally, the **Technical Operations Branch** (TOB) is the technical surveillance and countermeasures (TSCM) section of the 310th MI Battalion. The mission of the TOB is to provide a quick response and comprehensive security solutions to enhance commanders' FP and physical security postures. The first priority of a TSCM investigation is to detect and neutralize technical penetrations and hazards.

Final Thoughts

The 310th MI Battalion provides specific technologically oriented assets that are critical for Homeland Security. The advantage of these assets is that they leverage technology to arm the United States with another layer of protection against terrorist incidents in the United States or other U.S. interests, as well as against the traditional threat of foreign intelligence and security services' activities. The 310th MI Battalion is on the forefront of technology and strives to advance the use of technical counterintelligence in all CI operations.

Captain Elizabeth Duncklee received her commission as a Military Intelligence Officer from Clemson University, South Carolina. She is currently serving in the S3 Office at the 310th MI Battalion at Fort Meade, Maryland. Readers may contact the authors via E-mail at tinam@meade-inscom.army.mil.

First Lieutenant Jeremy McKnight received his commission as an MI Officer from the United States Military Academy. He currently is serving in the S3 Office at the 310th MI Battalion at Fort Meade.

Read Any Good Books Lately?

We welcome reviews of books related to intelligence professional development or military history. Please mail them to Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-FDR-CB (Ley), Fort Huachuca, AZ 85613-6000 or E-mail your book reviews to michael.ley@hua.army.mil.

Intelligence and Law Enforcement Coordination: Overlapping Mission Dictates Need for Improved Liaison

by Juan Baker

The intelligence and law enforcement communities have traditionally operated in distinct worlds, separated by law, mission, and culture. The two communities conducted liaison, but did so primarily with an eye toward protecting their separate equities. The events of September 11 forced two common goals on these communities: the identification of those responsible and the prevention of future attacks. As a result, a new premium was placed on information-sharing.

Differences Between the Communities

The law enforcement community is generally understood as those federal, state, and local entities responsible for investigating criminal activities. The Intelligence Community includes all federal and Department of Defense (DOD) intelligence components as specified in **Executive Order 12333**, **United States Intelligence Activities**, dated 4 December 1981. The Intelligence Community is responsible for conducting intelligence activities to meet national security requirements.

During the last 94 years, the Federal Bureau of Investigation's mission has been gathering information to build cases for criminal prosecution rather than prevention; the FBI's success was largely dependent on its ability to protect evidence and the identities of its sources. As a result, the Bureau grew a "culture" of agents who learned to restrict access to their criminal cases in order to protect their assets and investigations. The FBI has a decentralized command structure to facilitate prosecution of federal cases at the local field-office

Make information exchanges a two-way street. A basic tenet of liaison or coordination with other agencies is quid pro quo (something for something) exchange. An exchange of information, services, material, or other assistance is an essential part of liaison. The nature of this exchange varies widely, depending on the location, culture, and personalities involved.

Keep your supported military command informed. If you are responsible for conducting liaison between other agencies and the military community, make sure you keep your respective major command military intelligence and security officers informed of potential force protection issues.

Avoid circular reporting. When working with one or more outside agencies, come to an agreement on which agency will report the information to the national Intelligence Community.

Know your contacts. Do not wait for a time of crisis to provide your introductions and unit mission brief to the Central Intelligence Agency (CIA), local FBI, or other law enforcement organizations. You should have already established solid communications channels through routine liaison. If initial introductions are required during a time of crisis, make them and get to the point of your visit. During times of emergency, no one has time for long, drawn-out PowerPoint® presentations reflecting military history, lineage, budgets, etc.

Establish and ensure connectivity. Maintain a "Battlebook" that contains your contacts' names, telephone numbers, E-mail addresses, and other relevant data. Establish connectivity with your contacts so that you can communicate quickly in a crisis situation. When possible, establish a backup means of communication.

Network with fellow military investigative agencies, especially the local Army Criminal Investigation Division (CID). The Army's intelligence and law enforcement elements are separate. In all likelihood, incidents of a suspicious nature will be reported either to Army Intelligence or to CID, and at times to both. Coordinate all antiterrorism information with CID.

Adhere to organizational controls on information. Remember to protect information. Do not disseminate information without the express approval of the proprietary agency.

Understand contact agency mission and roles. When conducting coordination, you must understand the capabilities of agencies other than your own. Knowledge of the other agency's capabilities in terms of mission, human resources, equipment, and training is essential before requesting information or services.

Figure 1. Hints For Successfull Coordination.

level. While the U.S. Army conducts counterintelligence investigations to preserve the potential for prosecution, its primary purpose is the identification, exploitation, and neutralization of foreign-directed intelligence collection against the Army, determining the scope and extent of damage to national security and the security of Army operations, and identifying systemic security problems.

After the September 11 Attacks

Since 11 September 2001, information-sharing among intelligence and law enforcement agencies (LEAs) has vastly improved. Within 24 hours of the attacks on the World Trade Center and the Pentagon, the Strategic Information and Operations Center (SIOC) at FBI Headquarters was functioning with more than 500 individuals from 42 federal agencies. While FBI senior executives orchestrated the investigation of the Pentagon bombing, the multi-agency SIOC liaison force facilitated investigative coordination and information-sharing among their respective agencies.

Interagency cooperation at all levels is an important component of Homeland Defense (HLD). This cooperation assumes a tangible operational form in the joint terrorism task forces (JTTFs) operating across the nation. These task forces are particularly well suited to respond to terrorism because they combine the national and international investigative resources of the FBI and intelligence community with the street-level expertise of local LEAs.

The cooperation has proven highly successful in preventing several potential terrorist attacks. Perhaps the most notable cases have come from New York City, where the city's JTTF was instrumental in thwarting two high-profile international terrorism plots—the series of bombings planned by Sheikh Omar Abdul Rahman in 1993 and the attempted bombing of the New York City subway in 1997. As a result of the JTTF's work, the conspirators who planned these terrorist activities are serving time in federal prison. By integrating the assets and abilities of the FBI, local LEAs, and the Intelligence Community, joint task forces can be an effective response to the threats posed to U.S. communities by domestic and international terrorists. For specific guidance on conducting successful interagency coordination, see the accompanying figure offering "Hints for Successful Coordination."

Conclusion

Terrorism represents a continuing threat to the United States and a formidable challenge to counter and prevent. In response, the intelligence and law enforcement communities must continue to develop joint ventures based on effective communication and cooperation.

Editor's note: The author wrote this article before the FBI announced its extensive reorganization plan.

Juan Baker (U.S. Army, Retired) currently serves as the U.S. Army Intelligence National Liaison Officer to the FBI and has been on detail to the George Bush Strategic Information and Operations Center following 11 September 2001. His previous duties and assignments include the U.S. Army Foreign Counterintelligence Activity, 902d MI Group; Special Agent, San Francisco MI Detachment; Chief, Defensive Counterespionage (DCE) Section, Stuttgart MI Detachment; Operations Officer, U.S. European Command (EUCOM) CI Team; Special Agent in Charge, West Region CI Field Office; and National Liaison Officer at U.S. Army Intelligence and Security Command (INSCOM). Mr. Baker is a graduate of the FBI National Academy and the Advanced Foreign Counterintelligence Training Course. Readers can contact him through tinam@meade-inscom.army.mil.

Website for Future Leaders

CompanyCommand.com is a website (http://www.CompanyCommand.com) dedicated to company-level leaders wanting to learn and share ideas on topics such as command philosophies, Army policies, leadership counseling, officer professional development (OPD), and professional reading programs. Staff and faculty officers at the United States Military Academy at West Point, New York, operate the website during off-duty hours without remuneration.

The website meets its goal to improve institutional knowledge at the company-level by facilitating lateral information flow and serving as a user-driven forum whereby former and current company commanders share ideas, products, and lessons learned with others. Majors Nate Allen and Tony Burgess, the site's founders, commented that their sole purpose is helping leaders grow great units and soldiers.

CompanyCommand.com has a section organized by branch that links the experiences and competencies of former and current commanders. For example, it lists for the intelligence community some Military Intelligence contacts including former MI company commanders who are volunteer mentors. The operators of the site plan to expand it with platoon leader tools for junior leaders.

Among the website's other offerings are a "command tools" section with professional presentations, lessons learned, and stories. It also contains quizzes, after-action reviews, tactical scenarios, monthly updates, links to other military websites, and much more. Popularity of the site has increased since its debut in February 2000.

Installation Approach to Force Protection[1]

by Captain Bradley S. Branderhorst

As we watched the attacks of 11 September, we realized that as a U.S. Army Training and Doctrine Command (TRADOC) installation, we were not properly equipped to sustain the full time (24 hours per day, 7 days a week, or 24/7) battle to defend ourselves against terrorism. Since our primary mission at Fort Huachuca, Arizona, is to train intelligence soldiers, we have not focused on conducting tactical force protection (FP) missions. As we executed the tasks called for in our antiterrorism/force protection (AT/FP) plan and began our initial planning sessions, we realized that with innovative thinking, the basic Army tasks of the military decision-making process (MDMP) would continue to serve us well. We received initial guidance from our higher headquarters and our commanding general. In order to be effective in this emerging operating environment, we had to focus on detailed integration at both the planning and execution levels.

Initial Post-Attack FP

We quickly completed a hasty MDMP soon after the attacks and supplemented our AT/FP plan a few weeks later with a published operation plan. Fortunately, we had updated our AT/FP plan in January 2001 and exercised it with an internally driven FP exercise in March 2001. The knowledge gained from that process meant that we were not starting the AT/FP cycle at the beginning of its first evolution in the midst of a high operational tempo (OPTEMPO) FP environment. As we received news of the attacks, we immediately began implementing our January 2001 plan. We quickly staffed joint decisions on adjustments to that plan while we executed its initial requirements. One example was to increase the augmentation to the access control points to ensure adequate force protection and allow for sustained operations. This change was necessary because we had not planned on maintaining Force Protection Condition (FPCON) Delta, or even Charlie, for a prolonged period. Another adjustment we made was to the mission essential vulnerable areas (MEVAs) list. The list we developed in January was thorough; too thorough to provide us the focus we needed with our limited resources of time and engineer assets. Our barrier plans were very limited and did not place much emphasis beyond securing the gates and a few critical buildings. This forced us to take a very hard look at what was truly mission-essential and also vulnerable.

We had other, more practical, considerations in the hours and days after the attacks. We had to reevaluate who was mission essential. We had a baseline list (by unit) from which to begin but soon realized that this would have to be adapted. Again, our baseline did not deal with sustaining an increased FP level. One of our basic assumptions was that we would not sustain an elevated FP level for more than a few days. With the FPCON Delta-associated imminent threat, we ceased training, closed all nonessential functions, and sent all non-mission-essential personnel home. What we had after a few days were key personnel virtually trapped on and off post due to extremely long waits at the entry points; far fewer personnel on post due to the increased threat; many workers at home with nothing to do and little information; no food service personnel (military or concessionaires) to provide Class I support; and insufficient engineer support due to a lack of access for contractors.

The staff set out to solve these problems, anticipate the next set of

issues, and resolve them in hopes of minimizing future impact on the core mission as well as on the morale and welfare of our soldiers, civilians, and families. To accomplish our objectives, we needed a base of operations. Before the attacks, we had an emergency operations center (EOC) serving as the command and control (C^2) node during short-term issues such as natural disasters, serious training incidents, or troop mobilizations; it did not have the personnel to staff 24/7 operations. Within hours of the attack, the EOC became the installation operations center (IOC) and served as a full-time base of operations for staff members. Some of the meetings that took place in the initial days after the attack called for commanders and primary staff directors to meet with the commanding general. Additional meetings called for action officers from units and directorates to conduct working groups and make decisions while commanders tended to other business. We soon settled into a battle rhythm with commanders' meetings occurring at the post headquarters and the more frequent meetings with various organizational representatives occurring concurrently within the IOC.

Organization for FP

Staffing the IOC for 24/7 operations with crisis action team (CAT) representatives from all the units and staff directorates called for some modification of the IOC, one of the most important being a workspace and dedicated telephone sufficient for at least one person. This modification called for cooperative work by the Directorate of Installation Support (DIS), Directorate of Information Management (DOIM), and the Directorate of Resource Management (DRM).

With an improved IOC in the works, we continued our problem-solving process. Everything we did involved more than one staff directorate, often all or nearly all of them. As we worked to return some normalcy to our new increased FP levels, we first identified the personnel, equipment, and other resources that we were lacking. Many of the missing key personnel were those who we had earlier deemed non-mission-essential. For example, the food-service personnel mentioned earlier had by now become "key" personnel. We sat down as a staff and made recommendations as to what functions should return to operation and when. Such things as Intelligence Center training, public schools for our children, post exchange (PX) and commissary operations, and child care services were some of the first essential functions to resume.

There have also been changes to our organizational structure. Before September 11, several crucial garrison staff positions did not exist. We have since identified and created positions for a G3 force protection officer to coordinate all FP matters; a department of public safety (DPS) FP officer to serve as the central liaison between Fort Huachuca and local representatives (to include law enforcement, public safety, and federal agencies); and a G2 directorate to provide intelligence support to fuse all of the information as it comes in. The DRM, the Civilian Personnel Advisory Center, and the Staff Judge Advocate (SJA) worked with the appropriate directors to create these positions. The SJA also provided significant advice on the mission and organization of the G2 directorate to ensure it did not violate intelligence oversight laws and regulations. We have also augmented the G3 section with additional battle captains and noncommissioned officers (NCOs) under the mobilization table of distribution and allowances (TDA) and by filling temporary civilian positions for vital FP-related responsibilities.

As we continued our planning process, our January 2001 plan provided us with a foundation to build on even though we had based it on threat assumptions that were no longer valid. The changing threat status led us to immediately reinitiate the AT/FP cycle with a revised threat assessment. Although hastily done, the revised threat assessment was quickly completed through the staff's joint efforts. From there, we updated the installation's vulnerability assessment. DPS headed the completion of this assessment, but again received valuable input from other members of the staff.

The G3 served as the catalyst for these planning sessions and published the results in an operational plan that resulted from our review of the AT/FP plan. This operational plan compiled all of the planning we had done since the attacks, included much more detail than our January 2001 AT/FP plan, and formalized the recommendations and decisions we made in the weeks after the attacks. Some important specifics of the operational plan were the designation of the garrison commander as the tasking authority over all installation tenants on FP matters and a consolidated intelligence collection plan with appropriate reporting requirements.

Fort Huachuca has integrated this entire process across the installation, but two of the critical FP improvements we made involved every member of the staff as well as units and other installation partners in at least some ways. These improvements included the augmentation of our guard force with a U.S. Army National Guard (ARNG) infantry company, and the creation and execution of an installation-wide, prioritized DIS FP projects list. During our initial efforts to control installation access, the requirement for multiple shifts of guards on the gates was significant. The personnel numbers were not initially prohibitive from a mission standpoint because, under the increased force protection posture, we stopped all non-mission-essential training. However, the overhead as-

sociated with training these soldiers on inspection procedures, Rules on the Use of Force (RUF), and other tasks, were huge.

Lowering FP Posture

As we made preparations to resume training while maintaining the same FP posture, the personnel cost became prohibitive. We worked together to determine how many soldiers it would take to replace our guards, the possibilities for augmenting our soldiers by hiring contract security personnel, and the impact of closing additional gates to decrease the impact on our training mission. It was an unprecedented effort on the part of nearly every organization on post. These efforts included:

- The SJA provided information on posse comitatus considerations and with the Adjutant General provided information on procedures for mobilizing U.S. Army Reserve (USAR) or ARNG forces.
- The DIS and the Directorate of Community Activities (DCA) resolved housing considerations for the additional personnel.
- DIS and DPS provided impact analysis of changing traffic flow by closing additional gates.
- The DCA provided data on the impacts of closing or reducing selected services on post, such as childcare, PX, commissary, and morale, welfare and recreation (MWR) facilities.
- The DRM and the Directorate of Contracting (DOC) provided cost analysis of hiring guards. The Medical Department Activity (MEDDAC) provided information on potential impacts on family members living off post and retirees.
- The G3 served as the central planning coordinator and provided information on additional training requirements for the additional guard personnel.
- The Public Affairs Office (PAO) continued to keep the public informed about changes in access to the installation, traffic flow, medical appointments, services on reduced hours or closures, and informational briefings through the Commander's Access Channel, articles in the Fort Huachuca ***Scout,*** and off-post newspapers, and local radio announcements.
- Finally, the staff made a joint recommendation to the garrison commander, then the commanding general, and finally to TRADOC regarding the gate closure plan and a request for an ARNG infantry company to serve as a guard augmentation force.

As we were given authority to slightly lower our FP posture and as requested materials began arriving, we came together again as a staff to prioritize our continued FP improvements. The initial rush of activity soon after the attacks provided increased FP to our MEVAs and high-risk targets (HRTs). Units and staff directorates continued to generate lists of additional force protection barriers, access control devices, and additional items they needed to enhance their FP postures. The DRM took the lead on this because the end product was a prioritized list of requirements with associated costs that we sent to TRADOC. Each directorate submitted its prioritized list to the Garrison Headquarters, which, in turn, completed an internal roll up. The deputy commanding officer, the chief of staff, and the DRM headed a meeting with the staff and representatives from all units and tenants and set the installation's priorities. TRADOC approved much of this list because we provided a prompt, well-synchronized plan. This plan serves as the basis of the FP priorities of work for the installation. We have since made several changes to this list as additional information or resources become available.

Informing the Force and Community

The PAO has proactively kept the public informed on FP initiatives within the bounds of good operational security (OPSEC). For example, the PAO has run stories about the efforts to prioritize FP issues on the installation and explained that projects important to many people

Snipers from the Counterterrorist Reponse Team.

Cochise County Mass Casualty Drill 9 March 2002.

on post may not be as high on the priority list as other projects. The G3 always reviews these releases for OPSEC issues and the SJA also sees them before their release. PAO cannot provide detailed information to the public, but even providing general information has cut down on stress in the community and reduced the amount of misinformation.

Some of our public affairs events have even helped shape FP priorities. During a recent televised installation town hall meeting, someone raised a question about improvements to force protection near an HRT. Although we had considered HRTs in our priorities, it had been placed below MEVAs and other HRTs on our prioritized list. This dialogue between a member of the community and the installation's leadership made us realize that this HRT should receive a higher priority.

Evolving Battle Rhythm

To ensure we maintain our high level of coordination while still allowing time to execute, we have evolved our battle rhythm into a set of meetings and conferences that assures we are addressing all of the issues we must and with the right personnel. We have a weekly meeting headed by the DPS FP officer with local representatives of law enforcement, safety officials, and federal agencies with the Fort Huachuca G2, G3, the criminal investigation division (CID), and 902d MI detachment to share FP information, both on and off post. We have increased the level of information-sharing by gaining temporary access to Secret information for the nonmilitary representatives who regularly attend that meeting. We hold a weekly IOC update brief where all the commands and directorates provide us with an update on significant events from the previous and upcoming weeks. Biweekly, we have a meeting among the intelligence and FP officers internal to Fort Huachuca. This meeting allows us to review our FP procedures and, when appropriate, recommend changes in these procedures to the garrison commander or commanding general. These meetings have helped develop and refine such procedures as replacement of lost military identification cards, tracking rates and potential patterns in the loss and theft of ID cards, photography policies for the installation, and the installation intelligence, surveillance, and reconnaissance (ISR) plan.

We also synchronize FP priorities with the current threat situation and standing taskings in a weekly DIS synchronization meeting involving the G3 FP officer, the G2, and the DIS FP representative. The garrison commander, G3, and deputy commanding officer meet with the commanding general almost daily to review FP issues, conduct command-level synchronization, and receive updates on the commander's guidance. Our final routine meeting is a quarterly FP council in which we conduct detailed planning of FP that we agree on weeks before the conference.

These meetings have evolved over time and as we gained a better understanding of the threat and friendly situations and our own requirements, we scaled back the frequency of the meetings. This freed commanders, directors, and other important personnel to spend more time with their organizations, but meant that they had to coordinate many of the tasks directly among themselves.

FP Exercises

The weekly IOC update meeting with all members of the CAT has further evolved into a vehicle for conducting AT/FP training for the staff. As we prepared to conduct a Battle Command Training Program (BCTP) AT/FP exercise this winter, we used an expanded IOC update as the basis for the initial staff training for the exercise. We also used this meeting for exercise in-progress reviews (IPRs). After the pre-exercise seminar, we focused on several areas of concern and dealt with one or two of them during each weekly IOC update. This methodology helped us become better prepared for the exercise and real-world AT/FP operations. Upon completing the exercise, we used the meeting to conduct follow-on after-action reviews (AARs) and to create an action plan to fix deficiencies. These meetings continue to serve as the venue for correcting these lessons learned at the action officer level.

We also set specific goals on what we would fix before our second exercise, a mass-casualty exercise

with local county and city officials, a month later. Because that exercise focused more on exercising mutual aid agreements precipitated by large numbers of casualties, we established goals that focused more on the planning and initial response stages. Still, it provided a good workout of our revised plans and procedures after the BCTP exercise.

Fresh from our two recent exercises, we have set out to once again complete the AT/FP cycle. We continue to review our AT/FP plan and recently held our first FP council meeting since the exercises. During the meeting, we reviewed the current threat assessment and issued guidance for refined input from all units and staff directorates. Finally, we set a timeline for the next council meeting and agreed to review the vulnerability assessment then.

Final Thoughts

We are still not where we want to be with regard to FP but, like any military operation, we will continue to refine and make improvements until we have deeply embedded these functions in our daily operations. Hopefully, the work we have done so far and continue to do will detect and deter potential threats from targeting our installation. Through our ongoing efforts, we are better trained and more focused on C^2, communications, computers, and ISR integration throughout the installation.

Endnotes

1. All photographs are courtesy of the Fort Huachuca Public Affairs Office. The photograph used with the title shows protective measures at the Fort Huachuca West Gate.

Captain Bradley Branderhorst is currently the Installation G2 for the U.S. Army Intelligence Center and Fort Huachuca. His previous assignments include Battalion S2, 2d Battalion (Mechanized), 5th Cavalry Regiment; Assistant S2, 1st Brigade, 1st Cavalry Division and Company Command in the 1st Cavalry Division; various positions as an Infantry Officer with the 193d Infantry Brigade in Panama; and Company Executive Officer of the Infantry One-Station Unit Training (OSUT) Company, Infantry Training Brigade, Fort Benning, Georgia. Readers may contact the author via E-mail at bradley.branderhorst@hua.army.mil.

United Response: Team Support of Homeland Security Concerns in Sierra Vista and Fort Huachuca

Courtesy of the *Fort Huachuca Scout*.

Treating a "casualty" during the Cochise County mass casualty exercise.

by Major David A. Santor, Deputy Chief of Police

Clearly, the tragic and criminal events of 11 September 2001 were the genesis of a new strategy in U.S. policing. The changing role of domestic law enforcement agencies (LEAs) will require better intelligence information, new equipment, and different types of training. As a result of September 11, the Sierra Vista Police Department, along with other public safety agencies, began to play a new role in our country's Homeland Security (HLS). We have already taken steps to improve interagency cooperation and sharing of resources. Continuation of these efforts will be critical in the development of protocols to respond to any major incidents in our area. Of primary concern to the Sierra Vista Police Department are the issues of command and control (C^2), communication, and intelligence as they relate to a multi-agency response to a major event.

Cooperation and Intelligence Sharing

Even prior to September 11, members of the Sierra Vista Police Department had actively participated in emergency and terrorist exercises on Fort Huachuca as graders, controllers, and actors. Additionally, there have been many instances of cooperation and resource-sharing over the years between the Sierra Vista Police Department and Fort Huachuca's public safety personnel. However, since September 11, the Police Department has seen an unprecedented level of teamwork, coordination, training and planning between safety and security officials from Fort Huachuca and city emergency services personnel. For example, Fort Huachuca's military experts have trained crucial Sierra Vista police personnel in aspects of addressing a terrorist-related nuclear, biological, and chemical (NBC) warfare incident. Moreover, the City of Sierra Vista and public safety officials from Fort Huachuca recently began a review and update of the area's joint disaster plan. This process is ongoing, and a completed document is expected in the near future.

Fusion Cell

Spawned by the terrorist attacks on our nation, Fort Huachuca's force protection personnel established a "fusion cell" with members of local state and federal LEAs. The Sierra Vista Police Department is a regular participant in this multi-agency intelligence-sharing effort. The local fusion cell was one of the first in the country that allowed military and civilian authorities to maintain open lines of communication regarding issues of HLS.

Courtesy of the Sierra Vista Police Department.

The new Sierra Vista mobile command post.

Courtesy of the ***Fort Huachuca Scout.***

Attempting to calm a "casualty" during the mass casualty exercise.

Mass Casualty Exercise

Building on an already excellent working relationship with their military counterparts on Fort Huachuca, the Sierra Vista Police and Fire Departments assisted Fort Huachuca public safety personnel in a recent mass casualty exercise. The 9 March 2002 exercise involved two major "events" on Fort Huachuca and one within the City of Sierra Vista. Representatives from other public safety, health, and medical service providers throughout Cochise County also participated. The exercise provided the Police Department with an excellent opportunity to "shake down" its recently acquired 33-foot mobile command post. The new mobile command unit contains three dispatch stations and a number of workspaces as well as C^2 (radios and telephones) and computers. The completely self-contained command post deployed during the Sierra Vista phase of the exercise.

While the overall results were generally satisfactory, the exercise did reinforce the need for better interagency communications and more clearly defined C^2 protocols given the differing systems employed. From the perspective of the Police Department, this exercise was an excellent test of our strategic plans and assets and provided valuable information for further development and refinement of both our internal and joint emergency policies and procedures.

Major David Santor is the Deputy Chief of Police for Sierra Vista, Arizona. Readers can reach him at (520) 452-7500.

27th Annual Army Intelligence Ball

The U.S. Army Deputy Chief of Staff G2 and the Commanding General, U.S. Army Intelligence and Security Command, will co-host the 27th Annual U.S. Army Intelligence Ball on 7 September 2002. The ball will be at the Hilton Alexandria Mark Center in Alexandria, VA 22311. Information on reservations is available via E-mail at aiball@hqda.army.mil or by telephone at (703) 601-0717 or 601-1923. Please RSVP by 19 August 2002.

A-L-E-RT-S:
SALUTE for Civilians

by Neil A. Garra

Perhaps the best way to prevent a terrorist attack is by having thousands of citizens wield their cell phones as information-age weapons and **report** suspicious activity to the proper authorities. Equally critical are brave citizens who can clearly report the details of the situation and help authorities send the right emergency response teams to the right locations. However, **who** do you call, and **how** do you report?

In an infantry unit, soldiers learn to call for indirect fire (mortar) support using a specific format that efficiently provides the right information to the mortar platoon's fire direction center. However, when I was serving as a mortar platoon leader, one of our evaluated platoon tasks was to talk an **untrained** observer through a call for fire. We led him to give the correct location and composition of the enemy, and then talked him through adjusting the rounds onto the target. As you might expect, getting steel on target took much longer using this method than it did with a trained observer. Yet this is today's modus operandi for every police department dispatcher: leading the untrained observer to report the correct information during a crisis situation. Training and experience have made dispatchers very good at this, often they do it dozens of times each day. However, in a major crisis they will receive hundreds of calls and can quickly become overwhelmed if they have to talk each of these untrained observers through the reporting process. Imagine how much more efficient they would be if citizens had training to call in emergency information the way the Army trains soldiers to call for fire support.

Long ago, the U.S. Army developed a special mnemonic reporting format for combat information: SALUTE, meaning size, activity, location, unit, time, and equipment. SALUTE provided the front-line soldier an easily remembered format for reporting critical information about the enemy he was facing.

The combat information contained within the SALUTE report is similar to the type of information required by a police dispatcher in an emergency. Working with Ms. Molly Schmidt, Senior Dispatcher of the Sierra Vista Police Department, I modified and "civilianized" the U.S. Army's SALUTE format into an easily remembered format covering the most important elements of information (see Figure 1). We designated the end product "**A-L-E-RT-S**."

This format is easy to remember, and flexible enough to cover a wide variety of emergency situations. See Figure 2 for examples of A-L-E-RT-S in cases of crime, suspicious activity, and fire.

See the "Report It" website at www.Huachuca.Org, which features the details of the A-L-E-RT-S reporting format and numerous examples; instructions for describing people, vehicles, and weapons; and information on how to handle suspicious mail. Also available for download is a Microsoft® Word® file with business-card-size A-L-E-RT-S cards (see Figure 3), and a free Palm OS® tool with both the A-L-E-RT-S format and an emergency phone number database. The Sierra Vista Police Department endorses this effort, and

Element	Explanation
Activity	**What** is the crime or what did you see? Suspicious activity, fire, assault, burglary, robbery, stolen vehicle, theft?
Location	**Where** is it? An address is best, but describe the location in your own words if you do not know the address.
EMS	**Injuries** that require immediate response by Emergency Medical Services.
Response Time	**When** did this occur? Is it in progress? A few minutes ago? Hours ago? This determines the urgency of getting police or medical services to the scene. In a real crisis, they may have to decide where to go first...this will help them make an informed decision and save lives.
Suspect	**Was** it caused by a crime? Did you see suspicious activity? If so, describe the people, vehicles, weapons, and where they are, or the direction in which they went.

Figure 1. Explanation of the Elements in A-L-E-RT-S.

Element	Crime	Suspicious Activity	Fire
Activity	"Shooting...	"Someone was looking into windows of parked cars...	"House has smoke pouring out the attic vent...
Location	...at 504 1st Ave...	...at 504 1st Ave...	...at 504 1st Ave...
EMS	...one person wounded in the arm...	...no injuries...	...no injuries...
Response Time	...3 minutes ago...	...last night at 8 p.m. ...	...it is happening right now...
Suspect	...suspect is 5'10" male with brown hair and yellow shirt armed with a revolver now running north on Fry Boulevard!"	...suspect is 5'4" female about 23 and 130 pounds with long, braided brown hair yellow shirt and blue jeans walking south, unarmed."	...no suspects."

Figure 2. Examples of A-L-E-RT-S Use.

they have provided invaluable assistance in creating the A-L-E-RT-S format, suggesting examples, and reviewing the website for content and accuracy.

The next step is to ensure that the general public knows about and regularly uses A-L-E-RT-S, particularly in reporting suspicious activity. We are currently developing lesson plans so that schools and private organizations can not only train their members but also offer training opportunities for others as a community service. Organizations that have disaster-related missions, such as Neighborhood Watch, the Amateur Radio Relay League, civil defense, Scouting, and the Civil Air Patrol could use this as a community service vehicle. We are also looking for corporate sponsors to produce the cards in quantity for citywide distribution, and also to assist with general community awareness advertising.

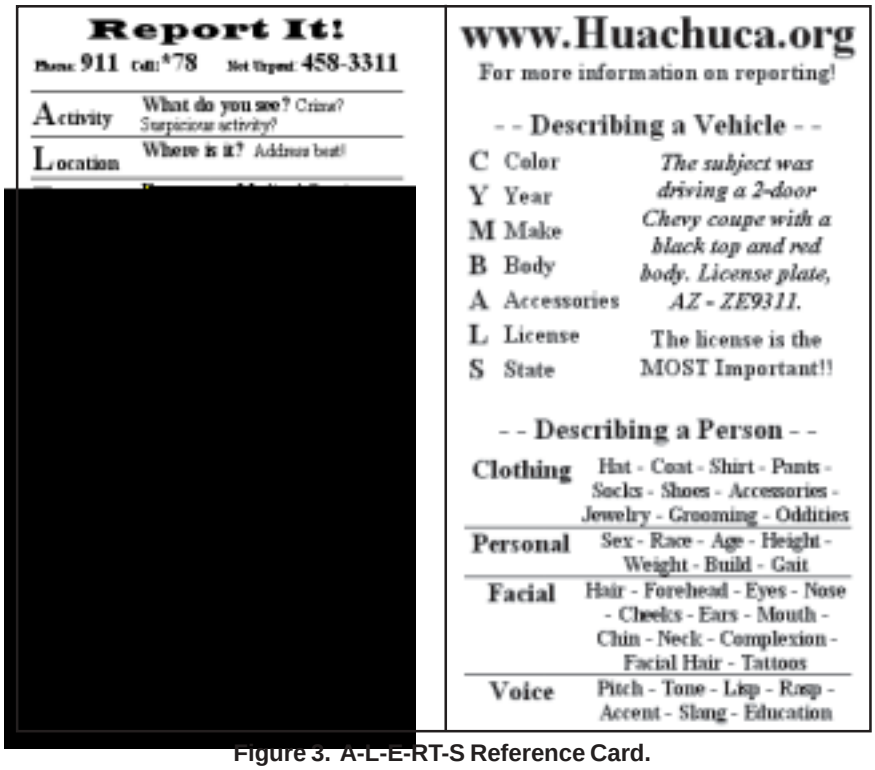


Figure 3. A-L-E-RT-S Reference Card.

The end result of this initiative is to turn Sierra Vista and vicinity into an 80,000-citizen scout platoon, armed with cell phones and trained and willing to render effective spot reports. Over time, most of these spot reports will likely be "Suspicious Activity" related to petty crimes. We cannot, however, take this for granted as Cochise County is a major infiltration route for drugs and illegal immigrants, one of whom may have something more sinister on his mind.

Neil Garra (Colonel, U.S. Army, Retired) is the "owner" of The S2 Company. While in the Army he served with the 1st, 2d, and 5th Infantry Divisions, and in several positions at Fort Huachuca in the Intelligence Center, the Battle Command Battle Lab, and in the Distance Learning Office. He is a graduate of the Sierra Vista, Arizona, Citizens Police Academy, and is a member of the Sierra Vista Information Technology Task Force. Readers may contact Mr. Garra via E-mail at g@s2company.com.

Educating MI Professionals to Meet the Challenges of Changing Geopolitical Realities and Modern Asymmetric Warfare

by George A. Van Otten, Ph.D.

The tragic events of 11 September 2001 brought into focus dramatic changes that ushered in the dawning of the new millennium. Since the end of the Cold War, the often precarious but stabilizing balance of power between the Soviet Union and the United States no longer serves as a catalyst for alignment and focus of the international relationships through which nations and transnational political groups pursue their goals and ambitions.

The U.S. Army Training and Doctrine Command (TRADOC), in response to rapidly changing geopolitical realities, has created a new contemporary opposing force (OPFOR) designed to replace the former Soviet doctrine-based OPFOR upon which U.S. military training relied for nearly half a century. The contemporary OPFOR presents an enemy no longer constrained by the traditional mid-twentieth century view of warfare.

The contemporary operational environment (COE) has far-reaching implications relative to the focus, organization, and methods of military intelligence (MI) instruction and education. It is no longer appropriate for instructors to rely on Soviet-style doctrine, concepts, and equipment as the foundation for the development of lesson plans, exercises, and instructional materials. Instead, instruction must now rest on solid principles and sound tactics that prepare soldiers to deal with the asymmetric nature of modern warfare effectively.[1]

Emergence of the COE

Great power politics dominated international relations throughout the 20th century. In the aftermath of World War II, the United States and the Soviet Union emerged as the world super powers with competing ideologies and military capabilities. The Cold War was the product of this uneasy balance of power. Their struggle for dominance shaped world geopolitical interactions for more than fifty years.

During the 1980s, aware that his country was about to collapse, Mikhail Gorbachev instituted reforms designed to stabilize the failing economy, eliminate corruption, and increase tolerance for free speech. Furthermore, Mr. Gorbachev shifted the Soviet foreign policy toward the United States from confrontation to cooperation. The changes he initiated quickly escalated beyond his control. Within a few years, the Russian people replaced communism with a representative system of government that the buffer states held captive for decades within the Soviet Union declaring their independence, and the Union of Soviet Socialist Republics disintegrated.

The end of the Cold War seemed to present an opportunity to direct resources once dedicated to maintaining the balance of power toward solving the pernicious problems that plague humanity. However, the resurrection of tribal and cultural conflicts throughout the world, as well as increased tensions and war between nations, replaced the bipolar competition of the Cold War with a multipolar distribution of power and influence that is as (if not more) unpredictable and volatile as the potential for conflict between the Soviet Union and the United States.[2]

Realities of the COE

The nature of world geopolitics is increasingly influenced by nations, groups, and individuals who have, or believe they have, unresolved grievances. Accordingly, fanatics, zealots, and terrorists feel free to ignore the sovereignty of nations for the sake of their causes. New technologies have dramatically diminished the level of protection once offered by great distances. Terrorists can now secure the information they require and travel throughout the world with relative ease.

Given these realities, a number of trends are apparent. Whereas nations will continue to dominate world politics and the United States will remain, in the foreseeable future, the most powerful of nations, growing numbers of the nontraditional "actors" will strive to disrupt and influence established international relationships. Further, the United States will find it necessary to expand greatly the efforts to protect her homeland.

Over the next several decades, it is likely that tribal, ethnic, and religious conflicts will destabilize and fragment vulnerable nations. Moreover, environmental degradation, shortages of critical resources, explosive population growth, and grinding poverty will exacerbate tensions within and between nations. As the gap between the rich and the poor of the world widens, the least prosperous will seek to punish and influence those they hold responsible for their social and economic plights. Advanced technologies have greatly enhanced the ability of those with alleged grievances to promote their agendas violently. It is now possible for a threat possessing only limited resources to exploit specific pock-

ets of vulnerability within the most prosperous and powerful nations. This will increasingly force advanced nations to dedicate considerable time, energy, and resources to protecting the security of their homelands and their interests throughout the world.

The security of the United States is without doubt directly linked to the willingness of her citizens to make the sacrifices, and commit the resources, necessary to deal effectively with those seeking to destroy our way of life. Potential enemies and allies generally believe the U.S. citizenry is unwilling to stay the course in a prolonged conflict with a tenacious enemy. The United States' laudable abhorrence of casualties causes many analysts to view our military strategies as predicable. This perception encourages potential enemies to practice asymmetric warfare against both the international interests of the United States and against our homeland. In keeping with their views of U.S. idiosyncrasies, they will avoid a head-on fight with U.S. forces. Instead, they will seek the cover of unpredictable actions designed to inflict great loss of life and carnage (such as the September 11 attack on the World Trade Center and Pentagon) while at the same time denying the United States the opportunity to employ its massive combat power. In some cases, the enemy may wait a long time between strikes. These strikes may be multifaceted or individual, and their operations and operatives will remain flexible and variable. It is clear that the United States must develop increasingly sophisticated and flexible measures with which to respond effectively to a wide range of potential conflicts including traditional and asymmetric warfare.[3]

Educating MI Professionals for the COE

U.S. soldiers and their leaders must prepare to fight and win under extremely fluid and complex conditions. In keeping with this realization, TRADOC has created a new type of enemy against which Army personnel will test their skills in exercises and simulations reflective of the COE. Soldiers will no longer pit their skills against a characteristically predictable and generally robotic OPFOR. The idea is to simulate the wide range of possibilities associated with modern types of conflict. The OPFOR does not represent the military doctrine and strategies of any given nation or group. Instead, it provides a realistic challenge based on the characteristics of a contemporary enemy expert in asymmetric warfare. Such an enemy studies the weaknesses and strengths of potential adversaries and, when engaged in battle, exploits weaknesses while avoiding strengths. A thinking enemy will always attempt to dictate the rules of engagement, and will never fight the kind of war preferred by its opponent.[4]

The basis for training and education of MI professionals must be realistic appraisals of the conditions of modern warfare and the nature of the threat. MI soldiers must become conversant with the multiplicity of world views that now comprise international geopolitics, the settings in which adversaries may be most likely to operate, the impacts of technological advances, and the potential of any possible threat to launch conventional or unconventional attacks. They must learn to identify accurately the characteristics and variables of the COE that will impact all future military operations. These variables and characteristics should serve as the foundation upon which courses of study in military intelligence rest.[5]

According to the TRADOC White Paper, *Capturing the Operational Environment*, published 2 February 2000, there are eleven variables (see Figure 1) that most directly affect military operations. These form the basis of the COE and should serve as a focal point of MI training and education.

Whereas analysis of the physical environment has long been an integral part of intelligence preparation of the battlefield (IPB), the COE requires expansion of the traditional view of the battlespace. Potential enemies know that U.S. Army tactics and equipment are most vulnerable in urban environments or in extremely complex terrain. Therefore, the analyst must use IPB to analyze these complexities thoroughly, and IPB exercises should emphasize operational situations and environments that do not lend themselves to a few standard IPB products lacking adequate detail.

The governments of many of the poorest nations maintain control of their populations by force instead of consensus. Some of these developing states, such as Iraq, knowing they cannot win in a direct confrontation with the United States and her allies, pursue their agendas by exporting terrorism throughout the world. It is likely that the United States and allied nations will engage in war in the future to protect their interests and for humanitarian reasons. In either case, U.S. forces may participate in long-term peacekeeping and nation-building activities. MI professionals must have the analytical skills needed to understand the

- ❑ Physical environment.
- ❑ Nature and stability of the state.
- ❑ Sociological demographics.
- ❑ Regional and global relationships.
- ❑ Military capabilities.
- ❑ Information.
- ❑ Technology.
- ❑ External organizations.
- ❑ National will.
- ❑ Time.
- ❑ Economics.

Figure 1. Variables Most Directly Affecting Military Operations.

nature of the cultures in which they are operating, and must be able to use this knowledge to provide their leaders with accurate and useful syntheses of information as relevant intelligence to facilitate the commanders' situational understanding.

In the past, the assessment of a potential enemy's strength was fairly straightforward; in the COE, it is no longer that simple. New technologies and the innovative implementation of asymmetric warfare now complicate intelligence assessments. Soldiers must be prepared to accomplish on-the-spot analysis and synthesis.

Moreover, the potential enemies of the United States are aware of the value of information. Open societies encourage free speech, and hostile groups gain vital information through open sources. Intelligence professionals must be able to identify information available to adversaries and must become skilled in planning for and protecting information. Furthermore, U.S. intelligence analysts must be ready to evaluate accurately a potential enemy's access to advanced technologies.

The economies of the world are increasingly linked to one another, and modern communications systems have significantly advanced the flow of information between geographic regions. The expanding interconnection of national economies through transnational corporations and groups has resulted in the active participation of the United Nations and private groups in crisis situations that, only a few decades ago, they would have considered regional or internal issues. The U.S. Intelligence Community should be ready to include the probable actions of such "actors" in their intelligence products.

Modern telecommunications technologies make it possible for noncombatants to witness almost all aspects of an ongoing battle. A single turn of events can greatly influence the will of a nation to support military forces against a determined enemy in a prolonged fight. In the COE, a thinking enemy will capitalize on the openness of the U.S. media through propaganda or by initiating military actions that might not win the battle but would sap the national will to continue the fight. MI training and education courses must teach analysts to detect, recognize, and report efforts to undermine the national will.

Intelligence professionals must include the fact that many terrorists believe that time is on their side in their macro-analysis of situations. After an act of terrorism, people initially demonstrate a great sense of purpose and a strong desire for revenge. After sufficient time has passed, however, they tend to turn their attention to other issues, thereby leaving the terrorist free to strike again. The U.S. MI community must make soldiers aware of the relationship between time and the COE. Conflicts may now be prolonged and may go on for decades or more.[6] The War on Terrorism will not be won in a single battle or over the period of a year or two.

Economics have always played a role in determining the outcome of wars. With all else being equal, affluent nations are usually in better positions to defend their interests than those with fewer assets. In the COE, however, the enemy does not need great assets or huge military expenditures. A few well-trained operatives with minimal resources can inflict tremendous casualties and property damage on the homeland or on U.S. soldiers and citizens abroad with little financial investment.

The reality of asymmetric warfare is that the U.S. military must be prepared to fight and win in almost every conceivable venue. Despite the great wealth of the United States, our ability to fund military operations is not without limits. Therefore, efficiency is important. Accurate and solid intelligence able to thwart an enemy's plans to carry out a terrorist act against the United States or her allies is an essential element in enhancing the efficiency of the nation's national and homeland defense.

Application of Constructivist Learning Theory

Constructivist theory rests on a foundation of interactive or experiential learning. Courses developed in keeping with the constructivist model focus on fully engaging students in the educational process.[7] Traditionally, the faculty of the U.S. Army Intelligence Center (USAIC) at Fort Huachuca relied upon information-packed lectures and practical exercises as the dominant method of instruction. However, throughout the past decade, training developers and instructors at the USAIC have increasingly integrated constructivist theory into course development and implementation. As a result, intelligence courses are now more reliant on small-group dynamics and realistic exercises that stress—

- ❑ Critical thinking skills (analysis and synthesis).
- ❑ Flexible problem-solving in a fluid and unpredictable environment.
- ❑ Risk assessment.
- ❑ Geopolitical analysis.
- ❑ Application of technical skills.
- ❑ Participation in realistic simulations and exercises.
- ❑ Cultural awareness.
- ❑ Teamwork.
- ❑ Personal communications skills.

The current need is for highly skilled, well-trained, thinking MI soldiers and leaders who are able to successfully counter and defeat thoughtful, perceptive, and capable enemies dedicated to the destabilization of the world order and the demise of our lifestyle. Given its emphasis on problem-solving and the development of critical thinking skills, the constructivist learning theory provides a solid general foundation for the development of courses that reflect the realities of the COE. More-

over, leaders at the USAIC stress the need for instructors and training developers to integrate the COE immediately into all appropriate classes throughout the curriculum. As a result, course developers are writing exercises and preparing class activities that will allow students to develop intelligence products in the context of modern asymmetric warfare. Instructors encourage students to take risks, learn from mistakes, and hone their abilities to make solid decisions under great pressure.

Conclusions

The nature of world conflict has changed dramatically since the end of the Cold War. In order to effectively meet the challenges of the COE and modern asymmetric warfare, U.S. MI soldiers and leaders must stand ready to fight and win in every conceivable physical and cultural setting. The new realities of the threat require well-trained thinking soldiers who can quickly solve problems, produce accurate intelligence products, and survive in an often unpredictable and fluid hostile environment. USAIC is committed to the development and implementation of courses that fully prepare MI professionals to meet these challenges.

As technologies and world events continue to advance the pace of change, the need to respond quickly and effectively will also intensify, and the need for useful and accurate intelligence will grow incrementally. The transcendent challenge for all charged with the education and training of MI professionals will be to maintain the relevance of programs of instruction, individual courses, and practical exercises in keeping with the rapidly changing nature of the COE.

Endnotes

1. U.S. Army TRADOC, *Capturing the Operational Environment,* White Paper (Fort Leavenworth, KS: TRADOC, 2 February 2000).

2. Kegley, Charles W., and Wittkopf, Eugene R., **World Politics: Trends and Transformation, 6th Edition** (New York: St. Martins Press, Inc., 1997), pages 81-98.

3. TRADOC White Paper.

4. Ibid.

5. Interviews with Custer, John M., Colonel, Deputy Commander, U.S. Army Intelligence Center and Fort Huachuca, 4 March 2002, and Ingram, Mark Q., Chief Warrant Officer Three, All-Source Intelligence Technician Instructor, 11 March 2002.

6. TRADOC White Paper.

7. ***SED Letter***, "The Practice and Implications of Constructivism," Volume IX, Issue Number 3 (Austin, Texas: Southwest Education Development Laboratory, 20 December 2000).

George Van Otten, Ph.D., earned his Bachelor of Science degree in Social Science at Oregon College of Education, and his Master of Science degree in Education and Doctor of Philosophy degree in Resource Geography from Oregon State University. He is currently serving as the Dean, 112th MI Brigade (Provisional) (Advanced Training and Education), U.S. Army Intelligence Center, Fort Huachuca, Arizona. He served as the Dean of Academics at Sheldon Jackson College and as the Professor and Director, Office of Rural Resource Management and Planning, Department of Geography and Public Planning, Northern Arizona University. He was a Professor and the Chair, Department of Geography and Public Planning at Northern Arizona University. Dr. Van Otten served as an active duty U.S. Air Force Pilot and in 1996 retired as a Lieutenant Colonel from the U.S. Army Reserve. Readers may contact the author via E-mail at george.vanotten@hua.army.mil and by telephone at (520) 538-7303 or DSN 879-7303.

Wings of Fallen Stewardess Worn in Afghanistan

by Specialist Heather M. Curtis
Fort Campbell, Kentucky (Army News Service, 23 May 2002).

The flight wings of an American Airlines stewardess killed September 11 were worn in battle above Afghanistan. Staff Sergeant Mark Baker then returned the wings to her family at a ceremony here May 21.

Sara Elizabeth Low died when her plane crashed into the World Trade Center. Her father, Mike Low, sent her flight-attendant wings to Afghanistan with a letter to the 160th Special Operations Airborne Regiment (SOAR) (ABN) commander. His letter said, *"I ask this favor of you. Would it be possible to have some soldier, some good man or woman carry these wings with them in our war against terrorism?"* When the letter was read to the "Night Stalkers" of the 160th SOAR, it was SSG Mark Baker, an MH-47E Chinook crew chief, who asked to wear the wings into combat.

Baker said that wearing the wings made the fight more personal, and his fellow soldiers made sure the wings were always on his chest, pinned to his body armor. Sara's wings traveled on more than 20 missions, rescuing, resupplying, inserting, and removing special operations forces.

First Lieutenant Marie Hatch, Public Affairs Officer, HHC, 160th SOAR (ABN), said the wings were a symbol of the memory and pride of Sara Low and that they represented the perseverance and spirit of a father who lost his daughter, and also of the perseverance and spirit of the people of the United States.

SSG Baker returned the wings to Sara's father inside a framed print. Each crew member who flew on a mission with the wings signed the print.

Staff Sergeant Mark Baker, 2d Battalion, 160th SOAR (ABN), thanks Mike Low for the honor of wearing his daughter's wings in combat.

Distortion of Islam by Muslim Extremists

by Michael G. Knapp

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

In the aftermath of the 11 September 2001 terrorist attacks against the World Trade Center and the Pentagon, the people of the United States (and her allies) became much more aware of the goals, methods, and motivations of Islamic terrorist groups. However, we in the West need a clearer picture of the ideologies of these groups, as well as an understanding of how radical extremist militant fundamentalist ("REMF") Muslims have distorted some essential traditional Islamic concepts to justify their campaigns of terror. This understanding is important, especially in light of the anticipated length and complexity of the newly begun campaign against terrorism. We are still vulnerable to attacks, but we **must** ultimately be successful to maintain our form of government, way of life, and ideals.

Very few people, non-Muslim or Muslim, agree with the increasingly violent methods REMF Islamic groups employ against innocent noncombatants and the symbolically important facilities and personnel of what they perceive as "secular" societies. These radical Muslim ideas not only have endured during most the 20th century and into the 21st but also have resonated increasingly in the last 30 years. The new believers are often the disaffected and disadvantaged masses in crucial states of the Middle East and Southern Asia, since these societies still appear to offer little hope for real reforms, or broad political, social, and economic participation in those societies. These disadvantaged people tend to believe what they are told about what is wrong with their world, and how strict REMF interpretations of Islam can correct these ills.

This article builds upon previous research into radical Muslim groups' philosophies and practice of violence contained in my report, "**Jihad In Islam**," published by the National Ground Intelligence Center (NGIC) in October 2001. The goal here is to enable the reader to "get inside the adversary's head" to discern why these groups act the way they do, as well as what they may do in the future.

The Setting: A "Boiling Cauldron"

The environment from which REMF Muslim groups grow includes conditions both inside Muslim societies and perceived threats from outside the *ummah* (nation or community). Within secular Islamic states, especially if a government is overwhelmingly authoritarian, it is viewed as "corrupt" and "illegitimate" by the fundamentalists. These fundamentalists speak to the rest of the population, mainly the increasingly educated youth, who have little opportunity for meaningful employment. Interestingly, many members of the Islamic extremist groups have received extensive professional training in areas such as engineering, science, medicine, and law. Many governments in the Middle East and Southern Asia are attempting to cope with persistent economic failure by repressing even mild forms of dissent, disallowing any legitimate means of political participation or the addressing of grievances by any other than the sociopolitical elite. Most of these secular nations derive their beliefs not solely from the *shari'a* (Islamic law),[1] but rather a mixture of Islamic and Western law. When combined with the perception that they are promoting impure forms of Islamic beliefs and practices, the fundamentalists see these regimes as "apostate" and therefore not worthy to rule. A secular government will certainly never lead the "struggle" (jihad) against the continued political, economic, and cultural assault from "the West" and Israel. Thus, radicals see violence as the only way to effect real societal change.

Islamic radicals see Western reliance on oil and subsequent negotiations for oil resources as exploitation, or even a "Crusade" (in the true medieval sense) by "the Jews" and "the Western neocolonials," to continue "domination" of all Muslim states. The radicals feel this negotiated economic agreement comes somehow at the expense of their livelihoods. Concepts such as secularism and "human rights" imported

from (or, as they see it, imposed on them by) Western nations have not worked in Muslim societies, and these "foreign ideas" are a primary reason for the *ummah*'s continuing disadvantaged condition. The "non-believer regimes" of the West continue to support Israel's "terrorism" against the Arabs (and all Muslims, for that matter) while propping up unpopular (i.e., secular) regional governments. These perceptions, however unrealistic and inaccurate, provide fertile soil for Islamic extremism.

Radical Islamist Groups and Their Beliefs

Historically, radicalism existed as part of a wider Islamic resurgence movement that seeks to implement some form of reform *(islah)* and renewal *(tajdid)* at least once in every century. Relatively recent attempts at change occurred in reaction to the challenges to Islam that have been building since the middle of the 19th century but reached a crisis point during the last 30 years. This sense of crisis grows from the inability of Muslims to overcome their "backwardness" and "weakness" (when compared with the West), as well as the many challenges from modernization. (The West underwent the same fundamental transformational pain in the era commonly referred to as the Industrial Revolution, but the Islamic radicals fail to acknowledge that fact.) Islamic states are not blind to the need to gain some improvements in their societies, but they do not want the "alien values" that come with these advances.

Radical Islamist thinking capitalizes on widely held beliefs in various Muslim countries (such as conspiracy theories) resulting in blaming regional problems on others (the West) and a culture of victimization. Other ideas exploited by REMF Islamists include—

- The world is a perpetual battlefield between competing opposites (good versus evil; truth against falsehood, belief (or faith) versus disbelief (or apostasy, etc.) in which there is no coexistence or compromise.[2]
- Islam is a revolutionary movement charged with altering the unjust political, economic, and social status quo.[3]
- Current secular regimes are apostates (or k*afirs*, unbelievers). "True" Islam-based, Allah-oriented governments predicated upon *Shari'a* must depose and replace them.[4] Creating this change requires active jihad—which the radicals claim is the most effective and divinely sanctioned method of reform—an urgent required duty for all Muslims that, until recently, they had neglected. (A radical will also, after enumerating the faults of his audience, state something like "*May Allah be merciful*," to reinforce the sense of guilt, shame, and need for active repentance in the minds of the listeners.)
- Armed struggle (or *jihad bil saif*, jihad by force) is required until the restoration of all Islamic lands to pure Muslim control (e.g., the reestablishment of the early unified Islamic caliphate and the elimination of the Jewish state of Israel).[5]
- Muslims must carry out a staged process *(manhaj)* in accordance with Sayyid Qutb and other REMF Islamists, and focus on building the ideal society, one governed only by the *Shari'a*. This process includes—
  - Formation of the *jama'ah* (vanguard) of the movement and beginning to sound the call (*da'wah*) to "true" Islam.
  - Persecution of the movement from the disbelieving *(jahili)* society of which it is a part, so the movement separates itself *(hijra)* spiritually—and if necessary physically—to "purify" itself and build up the movement's strength in preparation for the next stage.
  - Conduct of a jihad by force to establish a "just" and purely Islamic society.

When they have finished the process, the movement will declare victory and will finally establish the desired utopian "Pax Islamica."

Radical Reinterpretation of Concepts

The basis of many of the ideas for reform and renewal of the Islamic faith and practices derive from Islam's sacred textual sources (the *Qur'an* or Koran and *hadith*) or from interpretations by Muslim scholars and jurists. However, REMF Islamists are adept at distorting the traditional, widely accepted understandings to support their violent and non-Islamic actions. There are seven primary radical interpretations.

Jahiliyya. Traditionally used in a pejorative sense to describe the prevailing state of pagan ignorance and barbarity of pre-Islamic Arabia. Muhammad Ibn 'Abd al-Wahhab (1691-1787), founder of the Wahhabi movement that later gave birth to the Saudi Arabian state, first expanded this concept to include Muslim societies of his time that had diverted from pure Islamic practice to sin. Sayyid Qutb redefined this concept to mean the modern, pervasive, willful secular state of disbelief and foreignness that seized Muslim societies, which are not based on the original Muslim holy sources and not operating under the *Shari'a*.

Takfir. Originally used during the seventh century rebellions by Muslim Kharijites to condemn Muslims who disagreed with them as k*afirs, Takfir* was proscribed by the *ulama* (Islamic scholars) against professing Muslims. Al-Wahhab reintroduced the concept and used it against other Muslims he defined as

hypocrites; labeling Muslims in this manner opened the way for proclaiming jihad against them. Contemporary radicals have similarly widened the use of the idea of *takfir* against Muslim governments seen to be too Western or not pure enough in Islamic beliefs and practice.

Hakimiyya. Ideally, this is the concept of the lordship of or governance by Allah but, according to Qutb, man has "de-throned" Allah from his rightful dominion by establishing the sovereignty of man over men. "True" Muslims must, therefore, strive through jihad by force to reestablish the supreme sovereignty of Allah. In practice, this is a call to destroy all secular nations and replace them with Islamic states (the Islamic Republic of Iran, the Islamic Republic of Afghanistan, etc.).

Hijra. This was the early physical migration of Muslims to Medina to escape persecution from the pagan inhabitants of Mecca who had felt increasingly threatened by the Prophet's success in attracting followers. Mawdudi, Qutb, and other radical Islamists reinterpreted this to mean the spiritual (and physical if necessary) separation from the *jahili* society required by the "true believers" to increase the strength and organization of their movement. However, Egyptian Islamic Jihad (EIJ) and some other extremist groups have interpreted *hijra* to mean spiritual and moral separation only, while trying to penetrate the *jahili* society and its institutions so that they can initiate jihad as soon as possible. In practice, this is a precondition for brainwashing and indoctrination.

Jihad. Most Muslims have traditionally understood this as the internal, greater struggle *(jihad al-akbar)* to purify oneself spiritually and lead a good life. The lesser jihad *(jihad al-asghar)* is the physical (external) struggle, a shared communal obligation for some Muslims *(fard kifaya),* on behalf of all, to defend the *ummah* from aggression. However, radicals such as Hasan al-Banna and Abdullah Azzam insist that the "greater" jihad is the forceful struggle, which they label as defensive (but which is actually more offensive in nature). Furthermore, they state that it is the duty for all Muslims *(fard 'ayn)* to not only return all territories to Muslim control but also destroy "injustice" (secular law, as opposed to *shari'a*) and "disbelief" (anyone who does not believe and practice as they do) **wherever they are**.

Questions of Strategy. The internationalization of this struggle and the linking of such efforts after the initial jihad in Afghanistan poses two important questions regarding the strategy to radical Islamists.

- Should they follow the ideals of Abd al-Salam Faraj, who advocated destroying the "near enemies" within their own societies first, in his pamphlet **The Neglected Duty** written as the ideologue for the EIJ?
- Should they follow the ideals of Ayman al-Zawahiri of the EIJ and Al Qaeda, to strike the "far enemy" first (e.g., the United States and other "oppressive" powers of the West)?

Ayman al-Zawahiri urges the latter course of action in his book, **Knights Under the Prophet's Banner**, smuggled out of Afghanistan in December 2001.

***Istishad* (martyrdom).** In Islam, *istishad* historically meant making the "ultimate sacrifice" in conventional combat against armed foes. Radical Islamists, however, twisted this concept to allow suicide operations (or *intihar*)—forbidden in traditional Islam—against innocent noncombatants, as well as against personnel or facilities of the secular governments (for which suicide actions are permissible). Interestingly, this distortion of mainstream Muslim thought revives the tradition of suicide killings as a legitimate method by the extremist Kharijites and Assassins[6] in early Islamic history—a methodology frowned upon by most Muslims, regardless of the age in which they lived.

Significant Islamist Ideologues

There are eight major articulators of radical Islamic thought and they are the most effective reinterpreters of traditionally accepted concepts. They significantly inspired other extremists.

Sayyid Qutb (1906-1966) was executed by Nasser's Egyptian Government for advocating violent societal change in his 1964 book, **Milestones** (***Ma'alim fil tariq***, or "Signposts Along the Road" in Arabic). This publication is considered crucial for the Muslim Brotherhood in Egypt, and remains the great inspiration for most Sunni Muslim radical groups. Besides his reinterpretations of *jahiliyya, takfir,* and *hijra*, and his emphasis on the perpetual battle of competing ideas, Qutb also held up jihad as permanent conflict that is an essential part of the phased process to remake Islamic society. His writings also rekindled anti-Semitism as a part of radical Islamic thought and practice. This prolific Egyptian Islamist writer's reinterpretation of traditional Islamic concepts was the catalyst for the rise of radical Islamic groups.

Sayyid Abul A'la Mawdudi (1909-1979) was the founder and leader of the Jama'at-I Islamic group, and was a significant voice in the negotiations to remake Pakistan as a true Islamic state after its partition from India in 1947. Like Qutb, he was a prolific writer on many issues of concern to Muslims in areas of religious faith, and the proper relationship between Islam and the political structure, law, and practices of the state. Besides his major works, **Islam and Jahiliyya** (believed to have inspired Qutb) and

Towards Understanding Islam, Mawdudi wrote **Jihad in Islam**. His writings became available in Arabic in the 1950s and are known to have inspired Qutb and other Islamist radical thinkers. Mawdudi's **Jihad in Islam** analyzed what this concept "really" means for those Muslims attempting to reform their societies, as well as insisting that **jihad must continue until the whole world is the abode of Islam** (*dar al-Islam*) or belief (*dar al-iman)*.

Hasan al-Banna (1906-1949), the founder of the Muslim Brotherhood, was assassinated by the Egyptian Government for his anti-regime views. His contribution to Islamist thought was his redefinition of jihad (a part of his **Five Tracts of Hasan al-Banna**) as an Allah-ordained defensive requirement for all Muslims, as long as unbelievers rule any Muslim lands. He also forcefully denied that the greater jihad was the internal spiritual struggle, but rather that it was the armed physical struggle against injustice and disbelief.

Ayatollah Ruhollah Khomeini (1902-1989) of Iran, though he was a Shi'ite cleric, his writings (such as **Islamic Government**, the best known of this works) and life example have ironically been a significant inspiration to Sunni Muslim extremists. Khomeni motivated radical Islamics to persist in their goal to establish similar Islamic governments in all nations of the Middle East and beyond. This was due to success of Iran's revolution in 1979 to establish a "true" Islamic state (governed by the *shari'a*), and Khomeini's insistence that Muslims must resist the "domination" by and dependence on the "decadent, infidel" governments of the West. Khomeini, like Qutb, also added to regional anti-Semitic sentiments by painting "Jews" and "the West" as "enemies of the faith" who want to distort and destroy Islam.

Muhammad 'Abd al-Salam Faraj (? -1982) was the founder and ideologue of EIJ. Following Egyptian President Anwar Sadat's assassination on 6 October 1981, the Egyptian Government imprisoned Faraj. In October 1982, the Government executed him with Sadat's other known, captured assailants. Faraj was the author of **The Neglected Duty**, which combined his ideas with those of Ibn Taymiyya (1263-1328), a medieval Islamic scholar, and of Sayyid Qutb. Faraj agreed with them in advocating the overthrow of Muslim rulers he saw as having become "un-Islamic" by not actively pursuing jihad against "the occupiers of Muslim lands." (In practice, this meant that since Sadat made peace with Israel, Sadat would have to be eliminated.) Faraj expanded on the concept and practice of jihad, stating that the "sixth pillar"[7] of Islam—which he claimed Muslims have forgotten—is a "required duty" for all to destroy corrupt local regimes so that they can then wage an effective campaign against all unbelievers.

Abdullah Azzam's (1941-1989) significance to radical Islamist thought, as contained in his two fundamental works, **Join the Caravan** and **Defense of Muslim Lands**, is his expansion of the ideas of al-Banna and Faraj. Azzam was assassinated in Pakistan in 1989, possibly by Usama bin Laden, over differences in the strategy of the Afghan jihad that both had been supporting. His writings (heavily influenced by Qutb's ideas) are the primary source of inspiration for the proclamations of jihad against Jews and the Western "crusaders" by bin Laden and Ayman al-Zawahiri (al-Zawahiri was orginally a member of the EIJ and later a member of the transnational Al Qaeda terrorist network too). Azzam, like al-Banna, repudiated the idea that the spiritual form of jihad was more important than armed struggle, and insisted that jihad by force is the greatest religious obligation for Muslims after faith (*iman*) itself. He also seconds al-Banna's and Faraj's notions of jihad as required for all and immediately, in light of the Muslims' "state of crisis" vis-á-vis their ("defensive") struggle against "*the campaign to destroy Islam*." Of course, this alleged campaign is, they claim, led by Israel and the West. Azzam highlights the importance of support by the mujahiden to the jihads in Afghanistan (1980-1989) and the Palestinian territories, and also advocates expanding the Islamic jihad beyond current nationalist borders (e.g., promotion of pan-Islamic jihadist solidarity).

Ayman al-Zawahiri (1951- 2002), besides recycling many of the major Islamist ideas mentioned above in his most recent book, **Knights Under the Prophet's Banner**, provides some interesting thoughts on how the transnational extremist movement should develop. He counters the traditional radical strategy of targeting the "near enemy" first, saying that the great oppressive powers will not allow the mujahiden to achieve power in their own societies; thus, they must strike the "far enemy" first. Zawahiri states that for the worldwide jihad to be successful, the battle must move to the enemy's territory. He says further that the effort should focus around small suicide teams (since these are the most cost-effective), and must establish a fundamentalist "base of operations" in the Middle East to support and coordinate the various jihad movements. Zawahiri also indicates that jihad movements must better define their message to Muslims; then the mujahiden will attract more support by providing needed services to the societies they are defending. This thought process appears to mirror the success of other groups (e.g., Hamas, Palestinian Islamic Jihad) which provide health clinics and schools in the Palestinian territories, thereby attracting support. (It is also important to note that the Palestin-

ian Authority has been unable to create these health clinics and schools.) People have a natural tendency to feel obligated to those who assist them.

Usama bin Laden (1957-present), unlike his fellow Islamist radicals above, although an impassioned revolutionary, is not implementing original ideas. Rather, even more than Zawahiri, he has simply borrowed the thoughts of Qutb, al-Banna, Faraj, and Azzam, and added his own charismatic spin to them. (See his 1996 "Declaration of War" and 1998 "Fatwa" in Figure 1.) Bin Laden is really more a product of Saudi Arabian *Wahhabism*[8]. He focuses on an active, "defensive" jihad to rid his homeland of what he sees as a corrupt government and the continuing occupation of the "land of the two holy places," by the "U.S. crusaders" since the end of the Gulf War. Bin Laden's other claims of solidarity with, and a desire to assist, the Iraqis and Palestinians in their struggles against the United States and Israel, have proven hollow. His support in men, materiel, money, and more, is virtually nothing compared to what he has pumped into other causes (e.g., the attempted control of all Afghanistan, funding REMF Islamist groups in Indonesia, the Philippines, and Bosnia).

Toward A Better "End State"

Governments in the Middle East and Southern Asia that are friendly to the United States, and whose societies have been under attack by radical Islamist groups, have not responded effectively against these ingrained and persistent threats. To effectively meet the threat and eliminate the sources of discontent would require fundamental changes in their internal political, economic, and social structures. The fact that these nations have, so far, been successful in preventing takeovers by radical Islamist groups gives them little impetus for change. Three of the nations most important to U.S. foreign policy deserve more study.

Egypt. Egypt is a secular state that serves as the intellectual center of both the Sunni faith, and Sunni extremism. The Egyptian Government continues to avoid making the kind of significant political and economic reforms that would weaken the sympathy for its homegrown radical groups, such as the EIJ and al-Gama'at al-Islamiyya (Islamic Group, or IG). As an indicator of social, political, and economic discontent, note that many of the primary radical Islamists mentioned in this paper are of Egyptian origin.

Saudi Arabia—a Muslim monarchy that is the birthplace and religious center of Islam—is also an exporter of *Salafi*[9] (also pejoratively called "*Wahhabi*" to denote its Saudi variant) extremist thought. Saudi Arabia is also a worldwide bankroller of Islamic charities, financial activities, and schools and movements sympathetic to radical causes. While its ruling family members are the guardians of the "two holy places," they allow persecution of the country's *Shi'ah* minority and ignore centers of disaffection, such as the disadvantaged southwest corner of the Kingdom (from whence 15 of the 19 September 11 airplane hijackers came). As in Egypt, Saudi Arabia's rulers also have avoided making any difficult but meaningful societal reforms.

Pakistan is a center of separatist radicalism (a legacy from its anti-colonial and partition days) with an active military jihad in Kashmir. In the past, elements of the government gave tacit support to the radical groups fighting against Indian troops in the disputed Kashmir region. Since September 11, however, Pakistani leadership is under great pressure, due to Pakistan's support of the U.S.-led campaign in Afghanistan. This situation has forced Pakistan to curtail military support to radical groups such as Jaish-e Muhammad (JeM) and Lashkar-e Tayyiba (LT). Additionally, India's political and military reaction to the December 2001 attack on its parliament building by Pakistani-based jihadists, has forced President Pervez Musharraf's regime to crack down on these groups even further. Pakistan's leader must continue to walk a careful line to keep his society from fracturing any further.

Unfortunately for the United States, most of what really must be done—but has not yet been attempted—to resolve the long-festering societal problems in Middle Eastern and Southern Asian states must be accomplished by these states themselves. These regimes must—

- ❑ Be able to look inward, and start to take responsibility for their own shortcomings and mistakes.
- ❑ Begin comprehensive, painful but meaningful reforms that will really address the underlying problems that continue to sustain radical groups.
- ❑ Expand opportunities for all citizens, and ensure that even the poorest members of society have the necessary services, as well as a "safety net," once reforms have started.
- ❑ Speak out more widely and forcefully on the part of both political and religious leaders—on behalf of tolerance and against radical distortions of the Islamic faith.

The United States, for its part, can attempt to—

- ❑ Better understand the cultures of crucial friendly states in the Middle East and Southern Asia.
- ❑ More carefully balance its foreign policy toward all states in these regions.
- ❑ Be willing to lean on its allies, when necessary, to ensure a balanced, nonconfrontational approach.

Yvonne Y. Haddad, "Sayyid Qutb: Ideologue of Islamic Revival," in John L. Esposito (Editor), **Voices of Resurgent Islam** (New York: Oxford University Press, 1983).

Charles J. Adams, "Mawdudi and the Islamic State," in John L. Esposito (Editor), **Voices of Resurgent Islam** (New York: Oxford University Press, 1983).

Sayyid Qutb, **Milestones**, translated by S. Badrul Hasan (Karachi: International Islamic Publishers (Private) Limited, 1988). Also available on the Internet at www.witness-pioneer.org/vil/Books/SQ_Milestone/default.htm.

S. Abul A'la Maududi, **Jihad in Islam** (Lahore: Islamic Publications Limited, 1976).

Hasan al-Banna, "Jihad," **Five Tracts of Hasan al-Banna**. Available on the Internet at www.youngmuslims.ca/online_library/books/jihad.

Ruhollah al-Musavi Khomeini**, Islamic Government (Hukumat-I Islami)**, translated and annotated by Hamid Algar; available on the Internet at http://khomeini.hypermart.net/hukumat/right.html.

Johannes J. G. Jansen, **The Neglected Duty: The Creed of Sadat's Assassins and Islamic Resurgence in the Middle East** (New York: MacMillan Publishing Company, 1986).

Abdullah Azzam, **Join the Caravan** (London: Azzam Publications, 1996) and **Defense of Muslim Lands** (Ahle Sunnah Wal Jama'at, not dated); both formerly available on the Internet from www.azzam.com.

"Maudoodi on Takfir," translated by Zahid Aziz, in ***The Light and Islamic Review***, November-December 1996; available on the Internet at www.muslim.org/light/96-6.htm.

Usama [Osama] bin Laden, "Declaration of War Against the Americans Occupying the Land of the Two Holy Places," 26 August 1996, formerly available on the Internet at www.azzam.com/html/articlesdeclaration.htm.

Usama [Osama] bin Laden, "World Islamic Front Statement Urging Jihad Against Jews and Crusaders," 23 February 1998. Available on the Internet at www.fas.org/irp/world/para/docs/980223-fatwa.htm.

Ayman al-Zawahiri, **Knights Under the Prophet's Banner: Meditations On the Jihadist Movement**. Excerpts are available through the Foreign Broadcast Information Service (FBIS) as "Al-Sharq Al-Awsat Publishes Extracts from Al-Jihad Leader Al-Zawahiri's New Book," 2 December 2001.

David Zeidan, "The Islamic Fundamentalist View of Life as a Perennial Battle," **Ramat Gan Middle East Review of International Affairs**, December 2001 (available through FBIS as "Academic Says Fundamentalists Reinterpret Islamic Concepts to Justify Violence," 27 January 2002).

Robert Worth, "The Deep Intellectual Roots of Islamic Terror," ***New York Times***, 13 October 2001.

Robert Marquand, "The Tenets of Terror: A Special Report on the Ideology of Jihad and the Rise of Islamic Militancy," ***Christian Science Monitor***, 18 October 2001.

Abd al-Salam Faraj's pamphlet, **The Neglected Duty**, an ideologue for the Egyptian Islamic Jihad (EIJ) group.

Figure 1. Recommended Sources On This Topic.

- ❑ Demonstrate, with time and significant resources, real commitment to helping to solve the problems with which these governments are wrestling.

Editor's note: Mr. Knapp is graciously permitting us to include his extensive Glossary of Islamic Terminology on our website for use by our readers. It will be available at http://huachuca-usaic.army.mil.mipb.mipbhome/welcome.html in a month or two.

Endnotes

1. "*Shari'a*" is Islamic law, derived primarily from the Koran and the *Sunna* (custom, way of acting, "the trodden path"; literally "the way to the water hole").

2. Egyptian Islamist writer Sayyid Qutb.

3. Indo-Pakistani Islamist writer Sayyid Abul A'la Mawdudi. This idea occurs not only in Sunni radical thought but also in Shi'ism. According to 'Ali Shari'ati (1933-1977), the primary ideologue of the

Iranian Revolution, active revolution is seen as necessary even in the absence of the Hidden (12th) Imam of the Shi'ites (who is in mysterious hiding but will return as the *Mahdi* to lead the Islamic *ummah* back to greatness).

4. Egyptian Islamist Muhammad 'Abd al-Salam Faraj.

5. Egyptian Hasan al-Banna and by the Palestinian Abdullah Azzam.

6. The Assassins were an order of Muslim fanatics who were active in Persia and Syria from about 1090 to 1272. Their chief objective was to assassinate Crusaders.

7. True Islam recognizes five pillars of faith: public conversion, prayer at the prescribed five times per day, fasting during the month of Ramadan, the *Hajj* (pilgrimage to Mecca), and charity, especially to widows and orphans.

8. *Wahhabism* is a puritanical brand of reform Islam concentrated in the Arabian Peninsula that focuses on removing all traces of idolatry, forbidding the veneration of saints (as *Sufis* do), and severely punishing all who go against its strict interpretations of the Koran and *hadith*.

9. *Salafi* originally meant "early Muslim" or someone who died in the first four years after the Prophet. Followers of Muhammad Abduh revived this term for later-day Muslims who advocate a return to the *Shari'a*-minded orthodoxy that will purify Islam from unwarranted accretions.

Michael Knapp has worked in Military Intelligence for more than 20 years. In that time, he has served in the U.S. Army on active duty (as Battalion S2, Division G2 and Force Development Staff Officer, and Brigade S2); in the Virginia Army National Guard (as an All-Source Production Section Chief, Division Tactical Operations Center Support Element Chief, and Brigade S2); and in the U.S. Army Reserve as a Military Capabilities Analyst. Mr. Knapp spends most of his time as a civilian Middle East and South Asia analyst at the National Ground Intelligence Center (NGIC). Readers can contact him via the Internet at frknamg@ngic.army.mil and telephonically at (434) 980-7479 or DSN 521-7479.

Personnel For the U.S. Northern Command

This is an extract of two articles published in the **Early Bird** *(Bill Gertz and Rowan Scarborough, American Forces Information Service, 21 and 29 March 2002) with comments from Lieutenant Colonel James H. Harper, Chief, MI Branch, U.S. Total Army Personnel Command.*

A memorandum signed 7 March 2002 by General Richard Myers, Chairman of the Joint Chiefs of Staff, said that President Bush will likely approve creating a command responsible for Homeland Defense (HLD) and will probably designate it the "U.S. Northern Command" (NORTHCOM). With a projected operational date of 1 October 2002, NORTHCOM's headquarters will probably be in the Washington, D.C., area. It will have an area of responsibility encompassing the continental United States, Alaska, Canada, Mexico, and the surrounding waters out to 500 miles. General Myers' memo further stated that the Joint Chiefs have approved the following definition of Homeland Security:

The preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggression directed towards U.S. territory, sovereignty, domestic population, and infrastructure; as well as crisis management, consequence management, and other domestic civil support.

Regarding future Army Military Intelligence officer assignments to NORTHCOM, LTC James H. Harper stated that—

…at this time we do not have the personnel requirements nor do we know the location for the headquarters. This activation will cause a very accelerated timeline to organize and staff this new joint command. We could possibly receive many requirements for summer 2002 to send qualified officers to this new command. We can anticipate (because it is a joint unit) that most of the requirements will be for majors and lieutenant colonels to staff a J2 section and possibly a joint intelligence center (JIC). To fill this priority headquarters, we may divert officers or move other officers early, and there may be no backfill in either case. We continue to manage wartime requirements in support of engaged units, and this will not change. If you are interested in a not yet specified job at a not yet specified location to serve in the HLD joint headquarters, contact your assignment officer. I expect we will have very little time to react and any preparation we can make will save us time and effort.

Lieutenant Colonel James Harper is available telephonically at (703) 325-5502 or DSN 221-5502 and by facsimile at DSN 221-5668/6707.

The Growing Importance of Languages in the Fight Against Terror

by Ray Lane Aldrich

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

The War on Terrorism involves a number of aspects of foreign language proficiency as a critical factor in combating the terrorist threat. The higher the proficiency of the Army's linguists, the greater potential quality of the information they will provide.

Proficiency Level 3/3 Is Necessary

Our military linguists need to be at the 3/3 proficiency level to combat terrorism. However, the Army standard for foreign language proficiency is level 2 in both reading and listening, expressed as 2/2 or L2/R2. That level of proficiency is also the goal of the Defense Language Institute Foreign Language Center (DLIFLC) Basic Course. As the Interagency Language Roundtable (ILR) defines it, a "2" (in plain language) is "limited working proficiency." It roughly equals the ability to handle both*"...routine social demands and limited job requirements...."* This equates to an apprentice proficiency level; military linguists at this proficiency level can generally handle repetitive, proforma, simple, uncomplicated language. This is the proficiency level at which training exercises and organized military operations take place.

The language used by terrorists is more complex than the Army standard. One can safely assume that terrorist communication, whether electronic or face-to-face, will be in the realm of colloquial, complicated, jargon-rich chatter between people who share a deep philosophical commitment and a common cultural background. The opportunities for misunderstanding by a 2/2 linguist are significant.

Linguist Training Priorities

What does the Army need to do? We should train linguists in accordance with the following priorities:

- ❑ Languages listed in Figure 1 are suggested as appropriate for initial Army concentration. With the spread of the War on Terrorism to countries beyond Afghanistan, the list of languages must also expand.
- ❑ The Army should first begin by training current speakers of the languages to higher proficiency levels: at least 3/3. While not simple to do, it will not take as long as training non-linguists to a "limited working proficiency," and has a good chance of being successful.
- ❑ The Army should, at the same time, expand the dialect understanding of current linguists in new target languages. The goal of this training should also be 3/3. This, too, will take a shorter time than training non-linguists and will provide the ability to understand communication common to the less-well educated and to those who do not want to be understood.
- ❑ The Army should begin teaching new target languages in which we have no trained professional linguists. The goal of this training should be 2/2. After these linguists gain experience they should receive training to higher levels. These soldiers would form a cadre upon which we could build additional structure only when we need it (see Figure 2).
- ❑ The Army should actively seek current soldiers and incoming recruits with proficiency in and knowledge of any foreign language. We must record these skills in current databases for both the Active and Reserve Components (AC and RC, respectively).
- ❑ The Army should selectively use nonprofessional linguists who are adequately skilled in new target languages.

- ❑ Arabic, Modern Standard, AD
  Dialects
  - ♦ Arabic-Egyptian (AE)
  - ♦ Arabic-Syrian (AP)
  - ♦ Arabic-Libyan (AL)
  - ♦ Arabic-Maghrebi (AM)
  - ♦ Arabic-Gulf (DG)
- ❑ Persian-Iranian (Farsi) (PF)
- ❑ Pushtu (PU)
- ❑ Persian-Afghan (Dari) (PG)
- ❑ Azerbaijani (AX)
- ❑ Punjabi (PJ)
- ❑ Sindhi (SD)
- ❑ Siariki
- ❑ Urdu (UR)

Figure 1. Initial Language Concentration Language Identification Codes (LICs).

- ❑ Kurdish (KU)
- ❑ Baluchi (BU)
- ❑ Turkoman (UB)
- ❑ Tadjik (TB)
- ❑ Brahui
- ❑ Hindko/Hazaragi

Figure 2. Cadres For Languages Lacking Army Linguists.

- ❑ Only when the Army has accessed all Components and depleted their inventories of linguists should it hire contract linguists to meet its requirements.
- ❑ The Army should direct and mandate technological solutions. These systems may include remoted linguist augmentation, one-way translators, or other systems not as yet practical. Control of this technology should remain with the Army and not with a contractor who has no motivation to employ it.

Lane Aldrich (Chief Warrant Officer Three, U.S. Army, Retired) has been an active military linguist since 1961. He has attended DLIFLC and received military language-school training in Russian and German to the 3/3 level. Mr. Aldrich earned a Bachelor of Arts degree from the University of California. Readers may contact Mr. Aldrich via E-mail at ray.aldrich@hgda.army.mil.

Intelligence Oversight Guidance from G2/DCSINT

(Continued from page 9)

ATSD-IO, DTG 181700Z Nov 98, Subject: Policy Guidance for Intelligence Support to Force Protection, is the most current DOD guidance. This memo implements the 18 November 1998 ATSD-IO message and provides additional guidance.

a. Although the ATSD-IO message refers to a DOD list of U.S. persons and organizations against whom DOD intelligence elements may collect, Army MI elements may not conduct intelligence activities specifically targeting them. Because the Army maintains its law enforcement separately from its intelligence elements, it is inappropriate to collect information on these persons and organizations through intelligence activities. The Army designated law enforcement as the responsible agency, according to **AR 525-13**.

b. MI elements will no longer report U.S. criminal threat information as intelligence or SAEDA incident reports. This change is being included in the revision of **ARs 381-12** and **381-20**. Note that this does not pertain to national security crimes (treason, spying, espionage, sedition, subversion, etc.), which are within MI responsibility per **AR 381-20**.

c. MI personnel will pass, via the most expedient method, U.S. criminal and U.S. terrorist threat information received through normal assigned activities ("incidentally acquired") to the Provost Marshal/Director of Security and the U.S. Army Criminal Investigations Command (USACIDC). Receiving and passing the information fully complies with **AR 381-10** and the ATSD-IO message. Do not send copies to the HQDA Antiterrorism Operations and Intelligence Cell or Army Counterintelligence Center, as it could create circular reporting or false confirmation. USACIDC has that reporting responsibility, according to **AR 525-13**. A synopsis may be filed in general correspondence files ("administrative purposes"), as needed, for crediting work done.

d. MI personnel will refer requests for U.S. terrorist and U.S. criminal threat information and assessments to USACIDC or the Provost Marshal, as stated in **AR 525-13**. Local threat assessments are the installation's responsibility; MI may augment the local information with foreign intelligence and counterintelligence information and analysis.

e. MI personnel participating in AT/FP assessment teams according to **AR 525-13** are responsible for foreign intelligence and counterintelligence information and analysis. They may provide analytical advice and assistance to other team personnel in developing the overall assessment, but should not be used as the analytical subject matter expert for non-MI functional areas.

f. Any MI element may request a collectability determination through command channels to HQDA (DAMI-CHI), in accordance with references **AR 381-10** and the ATSD-IO message. Because of the 90-day retention time limit in **AR 381-10**, commanders must ensure speedy transmittal to HQDA.

Writers of the Quarter for July-September 2002 and April-June 2002

MIPB is pleased to announce that the Writer of the Quarter for July-September 2002 is Major David A. Santor for his article "United Response: Team Support of Homeland Security Concerns in Sierra Vista and Fort Huachuca," and the runner-up is Ms. Regan K. Smith for "Homeland Security: An Intelligence Oversight Perspective." The Writer of the Quarter for April-June 2002 is Lieutenant Colonel Stephen K. Iwicki for "The Challenges and Organizations of the National Counterdrug Intelligence Community," and the runner-up is LTC Jeffrey F. Mitchell for "The MultiComponent Contingency Support Brigade: A Force Multiplier." Congratulations to the winners and thanks to all of our authors for their articles, book reviews, and letters to the editor. Contributions like yours make ***MIPB*** the professional forum for military intelligence professionals.

CIA Support To Operation Enduring Freedom

by J. Daniel Moore

Central Intelligence Agency (CIA) intelligence support to the U.S. military in Operation ENDURING FREEDOM played a decisive role in the defeat of Al Qaeda and Taliban forces in Afghanistan. This added a new dimension to the long relationship of intelligence-sharing.

The Agency's primary missions have historically focused on strategic warning and coordination of clandestine activities abroad. During and after the Cold War, Agency intelligence collectors and analysts increased the confidence with which our leaders made decisions that helped maintain the peace between the United States and the Soviet Union. The CIA continues to perform these missions, but in recent years the Agency has acquired increased responsibility to provide direct support (DS) to military operations and deployments. Indeed, the Agency's close and innovative interface with military intelligence and U.S. Special Forces made a major contribution to our first battlefield victory in the war against terrorism.

The CIA's history of support to the U.S. military originated during World War II with the Office of Strategic Services (OSS), two-thirds of which included U.S. military personnel on rotation to the fledgling intelligence service. Many of these officers stayed on when, in 1947, Congress created the CIA. Established in 1942 by William J. Donovan on orders from President Franklin D. Roosevelt, the OSS soon built for itself a covert paramilitary force. OSS officers served as guides in the Allied landings in North Africa in 1942, established productive intelligence networks, and ran commando operations with resistance fighters in Europe, Africa, and the China-Burma Theater. OSS commandos also teamed up with the French Resistance, collected intelligence, and conducted sabotage to support Allied landings in Normandy in June 1944.

In addition to the tactical and strategic intelligence support provided to the U.S. military by the CIA since 1947, CIA paramilitary teams have operated with U.S. military forces in many conflicts, including those in Korea, Vietnam, and the Gulf. Some CIA commando teams collected intelligence on North Korean and Chinese forces and set up escape and evasion routes for airmen shot down over Korea. During the Vietnam era, the CIA conducted counterterrorist and counterinsurgency operations in support of the U.S. effort. The CIA supported Operations DESERT SHIELD and DESERT STORM through intelligence briefings in Washington, generated operationally derived intelligence in DS of military planning, and defended the political and diplomatic flanks of the Coalition by suppressing planned Iraqi terrorist activities.

Joint CIA-U.S. military strategy and combat operations in support of Operation ENDURING FREEDOM have transformed unconventional warfare. CIA paramilitary teams familiar with the local terrain and culture teamed with U.S. Army Special Forces and linked up with anti-Taliban Afghan commanders on the ground. The synergy created by CIA paramilitary specialists and U.S. Special Forces exceeded expectations. Intelligence collected by the CIA teams, coupled with the lethal combat arms capabilities of the Special Forces, wreaked havoc with Al Qaeda and Taliban ground forces, first demoralizing, then routing them.

Joint operations involving fast-moving CIA paramilitary teams and specialized U.S. military forces in Afghanistan may well serve as a model for future encounters against terrorism in other parts of the world. The dramatic success of specialized use of reconnaissance weapons and a dynamic, small-unit combat strategy obviated a deployment of large numbers of U.S. ground troops. Although the environment and circumstances in which terrorists operate today varies from one part of the world to another, CIA-U.S. military intelligence cooperation with local allies may well become a template for counterterrorist efforts elsewhere.

Daniel Moore currently works for the Center for the Study of Intelligence. Readers can reach the author through CIA Public Affairs Office (PAO) at (703) 613-1779.

Attention NCOs

Send us your articles and book reviews. If you have any experience you can share on MI doctrine, professional development, or "how-to" tips, please send them to ***Military Intelligence***. Topics of interest for future issues include: ISR, ENDURING FREEDOM, global conflicts, MI skills training, and tactical operations. E-mail them to michael.ley@hua.army.mil or call (520) 538-0979 or DSN 879-0979.

Leadership Notes

Army Intelligence Master Plan

by Collin A. Agee

As with all of the Intelligence Community, the Army Intelligence Master Plan (AIMP) office reacted with shock and outrage at the attacks against the United States on 11 September 2001, mixed with introspection and the questions: "*Could we have prevented this*?" "*Could we have anticipated the use of commercial aircraft to attack structures that are icons of our society*?" Their use only served to highlight discussions already underway regarding terrorist threats, asymmetric means of delivery, and ways to counter them.

That these threats were under discussion, however, brought us no solace. On the contrary, our conclusions regarding these attacks in many respects validated our notions of a future very different from the past, and our need for change to deal with the new realities. In a larger sense, September 11 also validated the impetus for Transformation of the Army as a whole. If anything, the future had arrived sooner than expected, revealed by a threat last seen in the battle-tossed seas around Okinawa.

Some see asymmetric warfare as a war—

- ❑ In which our adversaries do not fight by "the rules."
- ❑ In which there are no limits on their selection of targets.
- ❑ That violates the tenants of the Law of War regarding the deliberate murder of the noncombatants.
- ❑ In which the terrorist organizations have such effective operations security (OPSEC) and compartmentalization that their operations are virtually impenetrable to U.S. Intelligence.

We do not buy it! While the rules are different—or ignored—terrorists cannot ignore the laws of physics or the requirements to plan and execute their operations. Indeed, they must recruit, train, command, control, and communicate with their members as well as move to conduct their attacks. These functions vary from the Cold War-era Soviets in the much smaller size and greater flexibility of the terrorist organizations, their more secretive nature, and their deliberate attempts to avoid becoming predictable. This, however, does not mean they are immune from detection, only that their indicators and vulnerabilities—and they are present—are disparate. We also believe we can counter these asymmetries with other asymmetries; we believe the United States is capable of asymmetries beyond the reach of any other nation or armed force on the planet. This includes resources, technology, doctrine, training, and the skill of our soldiers. In this latter category, Army Intelligence plays a central role by conducting the most sophisticated analysis in the history of warfare.

Here is our idea of asymmetric warfare. A terrorist dies in his cave before he can ever do harm to another U.S. citizen, killed by a weapon he never heard or saw, after identification by sensors of which he is unaware, fused in an all-source fashion using automated tools and analytical methodologies.

One of the truisms of Military Intelligence is that we must think like the enemy. That is hard to do when his actions include the deliberate murder of innocents, a crime directed not only at the United States but also to all of civilization. Unfortunately, however, we must accomplish this if we are to counter the threat. In the following article, Mr. Brad Andrew provides considerably more detail on how the emerging threats, asymmetric warfare, the Homeland Security aspects of Army Transformation, and the evolution of Army Intelligence are interwoven into the future of Military Intelligence.

Collin Agee (Lieutenant Colonel, U.S. Army, Retired) is a Futures Analyst on the Army Intelligence Master Plan office. His MI assignments included J2 Operations for U.S. Forces in Haiti, XVIII Airborne Corps Analysis and Control Element (ACE) Chief, and G2, 10th Mountain Division (Light). He has earned a Master of Military Arts and Science degree from the School for Advanced Military Studies (SAMS), and a Bachelor of Science degree in National Security and Public Affairs from the U.S. Military Academy. Readers may contact him via E-mail at collin.agee@hqda.army.mil and telephonically at (703) 601-0391.

MI Corps Hall of Fame Inductees

The Military Intelligence Corps honored its latest inductees into the Hall of Fame on 28 June 2002: Colonel Richard Allenbaugh, Lieutenant General (LTG) Donald Kerrick, Chief Warrant Officer Five Michael Maroney, LTG Ira Owens and Major Walter Unrath.

Army Intelligence Support to Homeland Security

by Brad T. Andrew

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

The U.S. Army Intelligence Vision applies to all future Army missions. Anticipation of asymmetric threats significantly shaped the Vision, and as such it provides the overarching construct for the application of Army Intelligence's core competencies in support of Homeland Security (HLS) and Homeland Defense (HLD), or HLS/HLD.

This is not to say that the Army Intelligence Vision focuses only on support to HLS/HLD. Rather, HLS/HLD support is an application of the Vision's components and Army Intelligence core competencies to these missions. The Vision and core competencies remain equally relevant to Army Intelligence support to the Legacy, Interim and Objective Forces throughout the entire spectrum of conflict, to include simultaneous major theater wars (MTWs) and small-scale contingencies (SSCs). The bottom line is the application of Army Intelligence tactics, techniques, and procedures (TTP) in the continental United States (CONUS), combined with its operations outside CONUS (OCONUS), and provides a seamless, global ability to identify and interdict threat activities aimed at the U.S. homeland and the fabric of our society. HLS cannot be confined to actions within the United States.

Army Intelligence contributes to the HLS/HLD mission by **collecting, integrating and analyzing** massive amounts of data and information on large numbers of seemingly diverse entities to **predict** what the threat intends, so that authorities can take action to prevent the threat activity before it occurs. In essence, Army Intelligence enables proactive actions rather than reaction to events in the execution of the HLS/HLD mission.

This article imparts a general understanding of how Army Intelligence provides its product—dominant **knowledge—**to combat leaders, installation commanders, and local law enforcement personnel at the point of decision as they conduct the HLS/HLD mission. As President George W. Bush said during the swearing-in ceremony for Governor Tom Ridge as the first Director of the Office of Homeland Security, "*In the War on Terrorism, Knowledge is Power.*" Knowledge reduces risk or uncertainty for the decision maker, regardless of the echelon—squad leader through the President.

Overview of Army Transformation

The U.S. Army has an inherent obligation to protect CONUS as well as all U.S. interests worldwide. Army Transformation is an all-encompassing campaign that fundamentally overhauls the U.S. Army to ensure the Army fulfills these obligations. Transformation changes how the Army staffs, organizes, equips, and trains. It also modifies how the nation's leaders engage the Army as an instrument of U.S. foreign policy, how the Army defends the United States, and when required, how it fights and wins the nation's wars. In the Transformed Army, "dominant knowledge" provides the decision and action advantages essential for mission success. Army Intelligence provides the Transformed Army with the "knowledge edge."

Army Intelligence Enables Army Transformation and HLS Mission Success

Commanders have always sought a knowledge advantage to defeat enemies while minimizing their own losses, to include protecting their own countries and support bases. On tomorrow's battlefield, commanders must have knowledge about the battlespace unavailable to previous generations—knowledge which we must continually refresh. Army Intelligence will provide that knowledge. To achieve knowledge superiority and decision dominance in HLS, Army Intelligence must—

- ❑ Integrate national, joint, Service and law enforcement agencies' (LEA) intelligence, surveillance, and reconnaissance (ISR) capabilities.
- ❑ Apply its predictive analysis expertise.
- ❑ Disseminate predictive intelligence down to the lowest levels of local government and law enforcement.

Army Intelligence will **think globally** and enable the HLS team to **act locally**!

Army Intelligence Support to HLS

Army Intelligence in support of HLS/HLD is a globally focused, rapidly deployable, knowledge-based force composed of expert personnel harnessing the collaborative, analytical, communications, and presentation power of modern information technology to support leaders at the point of decision. It operates globally, within a national, joint, and combined context, and leverages the capabilities and expertise of the U.S. Intelligence Community, friends and allies, LEAs, academia, media, and private

industry to provide commanders focused, "near-certain," knowledge. Its core competencies are:

- Full-dimension **protection**, including protection in the physical and cyber-domains.
- Unique **collection** to cover information gaps.
- **Integration** of all intelligence and non-intelligence sensors and fusion (knowledge) centers to build the relevant "Red" and "Gray" (neutral, such as terrain and weather) pictures.
- **Analysis** to transform data into information and that information into relevant knowledge.
- **Presentation** of knowledge in a format and manner that imparts immediate understanding.

Expert Army Intelligence personnel operating collaboratively to develop knowledge focused on the commander's or decision maker's requirements underpin the core competencies.

Challenges to Army Intelligence Support for HLD Authorities

Army Intelligence is resourced, equipped, and trained primarily to operate OCONUS. Legal authorities consisting of laws, policies, and regulations are undergoing review and change to enable Army Intelligence to bring all of its expertise to bear on HLS operations within CONUS. The threat operates globally; therefore, the HLS/HLD effort must be global in nature. Army Intelligence can merge on-going OCONUS operations with CONUS-focused HLS/HLD efforts to provide seamless, predictive intelligence support.

Education-Based Training

The Army Intelligence Vision includes changes to the Institutional Army as we adapt Military Intelligence Corps professional training to include the focus and skills necessary to operate within the United States. Ongoing initiatives are moving Army Intelligence from a training system to an education system with established certification requirements and procedures at each level (apprentice, journeyman, and master) and professional degrees for soldiers. MI is consolidating some military occupational specialties (MOSs) to create multifunctional soldiers better able to handle the differing demands and required skill sets for operations across the spectrum of conflict. This will necessarily include the skills required to operate with LEAs and within the legal parameters that protect all the rights of U.S. citizens.

We must know this new threat, how they think, and how they operate. Institutional changes include developing counterintelligence (CI) and human intelligence (HUMINT) or CI/HUMINT All-Source Analysis System (ASAS) software applications, HLS/HLD modeling and simulation tools, and training based on HLS/HLD intelligence preparation of the battlespace, "plug and play" classrooms, mentoring programs, and distance learning. Army Intelligence will also revise its doctrinal base to complement evolving national and joint HLS/HLD doctrine by publishing new versions of the **FM 2-X** series of field manuals and using object-oriented doctrinal development to expedite the distribution of doctrine to the field.

Editors' Note: See Mr. Strack's article in the TSM Notes on page 59 for discussion of the ASAS CI/HUMINT systems and software.

HLS Operational Concept

The principal operational challenge facing U.S. military forces in this century is the requirement for early and continuous application of strategic responsiveness across the full spectrum of conflict, while simultaneously protecting against physical and asymmetric attacks targeting the CONUS and global infrastructure that serves as its power-projection base. The basis of our post-Cold War strategic military posture is power projection, with the preponderance of U.S. forces stationed in CONUS. Power projection emphasizes rapid deployability, an overarching need for transcendent speed of action, and HLS/HLD as an integral component of all operations. Army Intelligence enables "proactive" rather than "reactive" action to events in the execution of the HLS/HLD mission.

LEAs, the judicial system, consequence management activities and organizations such as the Federal Emergency Management Agency (FEMA), and even the Department of Defense's Joint Task Force (JTF)-Civil Support are fundamentally reactive in nature, mind-set, policy, structure, training, and TTP. Their responsibilities are primarily consequence management and building legal cases to prosecute those charged with terrorist acts. Conversely, Army Intelligence anticipates, collects, integrates, analyzes, and predicts so the decision maker can take action to stop the terror before it happens or to be waiting for the terrorists when they try to execute their planned action. To achieve this goal, we must know this threat and how they think and operate; we must integrate and analyze information in resident databases with global collection to provide predictive intelligence to the decision maker at the decision point regardless of echelon or agency. This effort must be truly global, as terrorists may conceive an attack in Asia, plan it in Europe, finance it via a global network of front organizations, and execute it with operatives not just in CONUS, but wherever there are U.S. citizens (including military personnel) to attack. In the Global War on Terrorism, the area of interest is the planet Earth and the surrounding space that includes satellite arrays.

Intelligence and security elements organic to the installation, units of action, and units of employment will not likely possess the expertise locally to satisfy all of the commander's

full-spectrum intelligence requirements. The expertise resident in echelons above corps (EAC) intelligence organizations can dramatically expand organic units' capabilities. Army Intelligence must conduct distributed intelligence operations linking organizations that have capabilities or possess expertise and resources required to provide predictive knowledge to the decision maker. We will conduct disperse operations, but must remain interconnected. The goal is getting the "*right knowledge, to the right person, at the right time*" so the decision maker *"Sees First, Understands First, Acts First, and Finishes Decisively*." EAC linkages could provide the framework to refine the HLS and installation force protection (FP) functions, while engendering confidence through real-time, continuous (24/7) support.

An interconnected information network is the goal, a combination of commercial and government communications capabilities serving as the transport layer for collaboration, information exchange, and knowledge production. This is the future global information environment (GIE) and the essence of network-centric concepts. The Objective Force will use the information dimension to deploy rapidly and operate effectively once it is in the area of operations, and to protect the homeland and its power-projection base worldwide. Our foes will use this dimension to conduct terrorist as well as political, economic, and cultural activities. To be successful, the Army must dominate the "digital high-ground" in the information dimension of the battlespace as surely as it must occupy or control the high ground in a strategic river valley. Information assurance is a fundamental consideration.

An essential element of the Army Intelligence HLS effort will be the architectures that link the various Knowledge Centers to the warfighting commanders in chief, MACOM (major Army command) and installation commanders, units of action and employment, and national, regional, state and local law enforcement leaders. The focal point of such an effort could be joining the U.S. Army Intelligence and Security Command (INSCOM) Information Dominance Center (IDC) with the 902d MI Group's CI Analysis and Control Element (CI ACE), National Ground Intelligence Agency (NGIC), and other Knowledge Centers. INSCOM could link the various classified and unclassified local area networks (LANs) and communications networks via the IDC with the TROJAN Backbone, providing a near-term global Army Intelligence communications system reaching down to garrison locations and tactically to the Interim Brigade Combat Teams (IBCTs), divisions, and corps. These communications would be through TROJAN SPIRITs (TROJAN Special Purpose Integrated Remote Intelligence Terminals) and TROJAN LITEs (Lightweight Integrated Telecommunications Equipment).

Once we establish the organizational construct and connectivity at the required classification levels, we must explore and develop the requirements, TTP, and training for "reach" and "collaboration." Effective and efficient execution and application of these concepts are in the rudimentary stages.

At the installation level, CI/HUMINT personnel collect information, conduct liaison with LEAs, and operate the intelligence cell in the emergency operation center (EOC). The EOC intelligence cell could inextricably link to a global knowledge-based intelligence family of systems (people, systems, processes, etc.) through the IDC that focuses on projecting instantaneous, near-certain knowledge. As the ultimate integrator and presenter of threat and environmental information for the commander, the installation EOC intelligence cell would integrate information from non-organic intelligence collectors, organic intelligence collection assets, and non-intelligence collectors such as LEAs to provide the relevant Red and Gray pictures to the commander.

At the operational and strategic levels, intelligence professionals in INSCOM and its subordinate brigades and groups would provide the nucleus for support to the Army Service Component Commands (ASCCs) in the operational theaters, MACOMs, installations, and LEAs. Since INSCOM also provides the Army subject matter experts (SMEs) at Knowledge Centers, they would likewise link and leverage them for HLS support. The majority of these Knowledge Centers are pre-existing, easily identified intelligence nodes that are centers of excellence in a specific intelligence discipline or intelligence process. These Knowledge Centers include the joint task forces and unified command joint intelligence centers, Joint Chiefs of Staff J2, the Defense Intelligence Agency (DIA), National Security Agency (NSA), the National Imagery and Mapping Agency (NIMA), Regional Security Operations Centers (RSOCs), NGIC, Land Information Warfare Center (LIWA), the intelligence centers of our sister Services and coalition partners, the 902d MI Brigade's CI ACE, etc. The objective would be to link and leverage these capabilities through INSCOM's Information Dominance Center to facilitate the integration, filtering, and analysis of information and predictive intelligence dissemination in support of the ASCC warfighter, MACOM and installation commanders; **and** to national, regional, state, and local law enforcement leaders at the point of decision.

Many actions such as those listed in Figure 1 are currently underway to accomplish this type of HLS concept. These actions need monitoring for lessons learned and "success stories" that will need rapid reinforcement.

Too often, today's discussion of "knowledge management" quickly and incorrectly reverts to a discussion of

Open-source intelligence (OSINT) strategy

How Army Intelligence will support U.S. Northern Command (NORTHCOM).

Installation security/force protection (FP) support demonstration

- ❑ Select two or three installations
- ❑ Equip with hardware/software/bandwidth/accesses (NIPRNET, SIPRNET, JWICS)
- ❑ "Hook" INSCOM's IDC
- ❑ Training on "how to think" about HLS/HLD

HLS/HLD modeling tools, visualization capability, and ASAS software

Cross-agency LNOs—put structure in place right now to solve the cross-compartment coordination problem below the departmental level (e.g. JWAC, DTRA, JTAC, CTC, etc.)

Strategy for gaining relief from existing policy and regulatory prohibitions

- ❑ Ascertain if we doing all we can within context of current laws, regulations, and policy
- ❑ Change internal Army policy and regulations as appropriate
- ❑ Participate in joint forums on reform of existing legal prohibitions

Army Intelligence's primary applicable core competency and value-added in HLS is analysis and predictive intelligence. Army Intelligence should support whomever it can, train others (such as LEAs), and assist them to the full extent of the law

Strategy for the effective use of the Reserve Component intelligence assets apart from their regular WARTRACE missions

Comprehensive strategy to address CI/HUMINT HLS/HLD issues—develop a list of recommendations to consider, coordinate, and execute

Monitor, support, and reinforce success of the initiatives already underway in the areas of:

- ❑ Access
- ❑ Analysis nodes
- ❑ Increased number of CI agents at installation and MACOM levels
- ❑ Partnering with CID

Key:
CID – Criminal Investigation Division
CTC – Combat Training Center
DTRA – Defense Threat Reduction Agency
JTAC – Joint Terrorism Analysis Center
JWAC – Joint Warfighting Analysis Center
JWICS – Joint Worldwide Intelligence Communications System
LNOs – Liaison Officers
NIPRNET – Nonclassified Internet Protocol Router Network
SIPRNET – Secure Internet Protocol Router Network

Figure 1. Areas of the HLS Operational Concept Under Development.

storage devices, switches, routers, protocols, etc. "Knowledge management" must include expert personnel; increased resident knowledge in databases; data, information, and knowledge mining; collaboration; rehearsal; and enhanced presentation capabilities and skills. Knowledge management must enable commanders and decision makers to understand rather than merely see the battlespace. Army Intelligence expert personnel at the MACOMs, installations, Knowledge Centers, and INSCOM's IDC must focus on collaboration to share knowledge and expertise to enable this awareness. Such understanding includes an improved capability to predict and assess intentions and courses of action of any adversary to include asymmetric attacks against our homeland. The Bush Administration is currently receiving criticism for a failure to heed the warning in a Federal Bureau of Investigation (FBI) agent's report that went "unnoticed" in the ever-increasing mountains of data and information that our information technology allows us to process. As the saying goes, "*if we only knew what we know*."

Conclusion

The Army is developing a warfighting concept that is more dependent upon **knowledge** than ever before. It applies equally to HLS/HLD, installation security, FP, and the defense of our power-projection base. What has changed is an attack on the continental United States, something that has not occurred since the War of 1812, and the accompanying loss of our sense of invulnerability. Superior intelligence, surveillance, and reconnaissance and cutting edge information operations are integral to achieving that dominant knowledge required for HLS/HLD success. Army Intelligence is prepared to provide the **knowledge edge**.

Brad Andrew (Lieutenant Colonel, U.S. Army, Retired) is a Futures Analyst working on the Army Intelligence Master Plan. His active duty assignments included Commander, 303d MI Battalion (Operations), 504th MI Brigade, Fort Hood, Texas; Deputy Director of Operations, 718th MI Group, Bad Aibling, Germany; J2 Joint Task Force-Bravo, Soto Cano, Honduras; and Force Integration Staff Officer, Department of Army Office of the Deputy Chief of Staff for Operations. He has a Master of Military Arts and Sciences degree from the Command and General Staff College at Fort Leavenworth, Kansas, and a Bachelor of Science degree in Engineering from the U.S. Military Academy at West Point, New York. He is also a graduate of the NSA Junior Officer Cryptologic Career Program and has a Space Operations specialty. You may contact him via E-mail at brad.andrew@hqda.army.mil and telephonically at (703) 824-4136 or DSN 761-4785.

Doctrine Corner

The Challenges of Homeland Defense

by Chief Warrant Officer Three Del Stewart

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

Members of the Fort Huachuca Doctrine Division participated in the December 2001 Homeland Defense and Crisis Management Workshop to obtain information concerning national Homeland Defense (HLD) efforts. The role of the Armed Forces was clearly a significant portion of the workshop. The workshop also discussed how those efforts might affect the U.S. Army Intelligence Center, and specifically noted how the proposed changes may affect future Army doctrine. As additional information became available, we updated some critical points.

Since the War of 1812, HLD has not been a significant concern for the nation nor the Army. The United States was blessed with great natural defenses (the Atlantic and Pacific Oceans), a strong ally to the north, and, since the conclusion of the Mexican-American War in 1848, a relatively peaceful border to the south. However, the events of 11 September 2001 changed our perspective, and HLD is now a genuine concern. In general, Homeland Defense, as a problem set, requires—

- ❑ Dedicated focus.
- ❑ Commitment to resolution.
- ❑ A working partnership between government and the private sector.
- ❑ Integration of effort (essential).
- ❑ Network-building (must include institutional structures, not just cyber-structures).
- ❑ Fundamental change to the bureaucratic thought processes.

The Office of Homeland Security (OHS)

The roles and responsibilities for the nation's OHS are not clear. Because of this ambiguity, the specific missions, personnel requirements, levels of classification, and logistical needs (how many computers, how many network administrators, how many safes, how much floor space, etc.) are not known. We do not know what its involvement and impact will be or its budget.

In February 2002, some resolution was provided when the Department of Defense (DOD) announced the formation of a new joint military command to support Homeland Security (HLS) and Defense. The DOD portion of the OHS will combine elements of the Norfolk-based U.S. Joint Forces Command (USJFCOM) and Colorado-based North American Aerospace Defense Command (NORAD) into the U.S. Northern Command (NORTHCOM). Established 17 April 2002, the new command will stand up on 1 October at Peterson Air Force Base, Colorado. NORTHCOM will be responsible for U.S. military operations throughout North America and will take charge of maritime defense operations currently under USJFCOM. NORTHCOM will also assume USJFCOM's authority for a national network of military support teams that assist civilian authorities in responding to natural disasters and terrorist attacks. The shift will allow USJFCOM to concentrate on its primary mission: training forces from different military Services to fight jointly. The Commander of NORTHCOM will also be the designated head of NORAD, which is a partnership between the United States and Canadian military forces. In addition to specific roles, responsibilities, and requirements, there are some legal concerns.

Legal Issues

Changing the law to allow the U.S. military more involvement in the HLD mission is a top priority for many, including the National Security Agency (NSA). Executive Orders, DOD regulations, Army regulations, etc., all act to limit the use of the military in the continental United States (CONUS), except for those units that have a specific law enforcement mission (such as the Military Police branches for each of the Services). We have a presumption in the United States that personnel encountered driving legally licensed vehicles are U.S. persons, that telephone conversations originate from citizens, etc. The mission of the military is to protect and defend the Constitution and our way of life, including the right to privacy. Current laws prohibit the Active Component (AC) military from being a full, unrestricted partner in Homeland Defense—for sound reasons. However, until and unless certain aspects of the legal constraints fundamentally change, legal matters will hinder DOD effectiveness in many HLD areas; one possibility would be to change such limiting laws via Presidential Directive instead of via the lengthy legislative process. The primary goal of these legal changes would be to enable greater inter-

agency coordination and cooperation, while retaining security controls.

Security Clearances

Most state and local law enforcement agency (LEA) personnel do not have appropriate security clearances; this is a major problem for the Federal Bureau of Investigation (FBI) and DOD when working these agencies. According to an FBI representative, fewer than ten percent of all crucial participants in state and local law enforcement have the level of clearance to access necessary federal classified or sensitive information. In the Washington, D.C., area, all chiefs of police have submitted their materials to obtain DOD security clearances to facilitate the sharing of classified information.

Interagency Coordination and Information-Sharing

Coordination among the many participating agencies is the greatest problem in effective HLS. The major difficulties relate to information-sharing. Clearly, information that may save lives must be shared immediately; however, regarding investigative data, most agencies (military and civilian) are reluctant to share this information since it often pertains to on-going investigations.

Information-sharing is not an easy tightrope to negotiate, but it is critical. It includes several essential aspects:

- ❑ Federal, state, and local agencies must share information.
- ❑ The information system must be secure.
- ❑ Passage of information must be both vertical and horizontal.
- ❑ DOD must be an essential player.

While analysts have sufficient information to draw correct conclusions and make recommendations to commanders or department superiors, there are also other valid concerns including:

- ❑ Assure case integrity.
- ❑ Ensure that no compromise occurs.
- ❑ Make sure that the agency sharing information will still be able to prosecute the case legally.
- ❑ Overcome inability to share information due to legal limitations.
- ❑ Resolve the lack of compatible communications and data-sharing systems.

An Emerging Software Solution for Information-Sharing

One software-driven solution, the Information Dissemination Management-Tactical (IDM-T) is now in the beta-testing stage at the U.S. Army Training and Doctrine Command (TRADOC) Headquarters (the sponsor) and at Forts Monroe, Gordon, Leavenworth, and Huachuca. The IDM-T is a menu-driven situational awareness tool for use, in part, by the installation operations center (IOC) for each installation. Essentially, the system links into a collateral Secret local area network (LAN). From this portal, the IOC monitors the macroview (such as everything else in the region and nation, all daily reports like the ***Early Bird***, etc.) and the microview (including all incoming reports from elsewhere within the installation or nearby cities considered linked to the installation (within normal daily driving distance)). The IOC can also transmit via the IDM-T platform.

Proactive measures and interdiction now become possibilities. Let us look at a specific scenario (see Figure 1). It is impossible to overstate the power of immediate situational awareness. The ability to proactively alert others, as well as to stand down unneeded security measures, can greatly decrease the confusion levels. However, as Figure 1 shows, for this to work, critical civilian agencies must have the appropriate security capabilities to legally and properly handle DOD classified and sensitive information.

Step 1: A DOD installation in Arizona reports that it detected a suspicious white powder on the boxes unloaded that day for the commissary. The installation submits a report, and it hits the SIPRNET (Secure Internet Protocol Router Network).

Step 2: Other DOD installations equipped with this tool (IDM-T) are immediately informed of the situation, and can proactively contact the commissary personnel on their respective bases and alert them to this fact, so they can be vigilant with incoming shipments.

Step 3: The Department of Public Safety (DPS) at the first installation receives notification that a fire extinguisher accidentally discharged in the delivery van that had boxes destined for the commissary. Since they have the explanation for the presence of the white powder, the DPS passes this report to their nearest DOD installation.

Step 4: The installation receiving this update can now pass this data to all other installations receiving the first message, so any extra security measures that they prudently emplaced can now cease.

Figure 1. Scenario Illustrating an Advantage of Using the IDM-T.

Roles of the U.S. Military Forces

U.S. Marine Corps. Effective 29 October 2001, the U.S. Marine Corps reactivated the 4th Marine Expeditionary Brigade (Anti-Terrorism) as part of its long-range strategy in support of HLD. The 3d Battalion, 8th Marines, is the lead element for the Brigade; in addition to the AT Battalion, the Brigade also includes a Chemical, Biological Incident Response Force, a Marine Corps Security Force Battalion, and a Marine Security Guard Battalion. According to a USMC representa-

tive, this Brigade could support local authorities when so authorized by the Secretary of Defense.

The Chief, Defense Consequences Management Systems Office, at the U.S. Marine Corps Systems Command, stated that one of the most pressing problems facing the military is a lack of doctrine and procedures. He suggested that doctrine development must be a top priority for the military.

U.S. Navy, Air Force, and Coast Guard. Given manpower constraints and the configuration of these Services, each of these Services will execute its mission and actively participate in an information-sharing role. Other factors will also have an impact.

Active Army. Even though NORTHCOM (DOD support to HLD) is still somewhat in its conceptual stage, the Army signed up to be the Executive Agent. Some of the issues it faces from a doctrine, training, leadership, organization, material, and soldier (DTLOMS) perspective are detailed below.

Guard and Reserve. The U.S. Army National Guard (ARNG) and U.S. Army Reserve (USAR) have substantial leadership and support roles in the HLS mission. Unfortunately, there is inadequate understanding of intelligence needs, doctrine, and operational practice in providing intelligence support to these organizations. The Reserve Component (RC) inconsistently implements infrastructure across the ARNG and USAR communities, which is understandable since each state makes decisions for its Guard force. There are also underused units and facilities within the RC force dedicated to intelligence support.

Currently, there are 23 Joint Reserve Intelligence Centers (JRIC) facilities operating at the Top Secret sensitive compartmented information (SCI) level, fully equipped with state-of-the-art information technology (IT) and communications infrastructure. Some of these facilities are doing superb work supporting the combatant commanders engaged in the Global War on Terrorism, while others are not fully employed in the effort. The Army could devote one or more of these sites to providing intelligence support to ARNG and USAR units supporting HLS on a continual basis if it identifies and resolves tasking, doctrine, and support issues. There were no major problems apparent with the RC CBRNE (chemical, biological, radiological, nuclear material, and high-yield explosives) team missions.

DTLOMS Issues

Doctrine. The primary doctrinal issue is the consolidation of current doctrine, and the development of new doctrine to meet the contemporary challenges associated with the HLD concept. Some would point out that there are volumes of information related to antiterrorism and force protection (AT/FP). However, that is also the problem: this information is dispersed throughout numerous joint publications, Army field manuals, Army regulations, and training publications.

A single point of reference would allow commanders, staffs, and intelligence personnel rapid access to the information and would enable doctrine developers to find gaps and deficiencies in order to address those issues. While it is impossible to create a single reference that is compact and usable, all doctrine must at least cross-reference other pertinent requirements. For the most part, conducting AT/FP operations is unit-specific for most Army installations and units. This unit-specific aspect does not allow for effective collaborative planning by commanders, nor does it facilitate effective collection, analysis, production, reporting, and dissemination of usable intelligence in a timely manner. The lack of standardized tactics, techniques, and procedures (TTP) and emphasis on AT/FP by combatant commanders can lead to misunderstandings and degrade Army operations. To be effective from an intelligence perspective, we must standardize doctrine and TTP to meet the commanders' needs better.

Currently, Doctrine Division, USAIC&FH, is actively engaged in producing this new reference. It not only addresses identified gaps but also comprehensively cross-references other appropriate manuals.

In addition, TRADOC drafted its **Installation Commander's Antiterrorism/Force Protection Handbook**. The projected release for an approved version is this year.

Training. Training is not currently adequate for AT/FP. Entry level, intermediate, and advanced training is required. Even with adequate training, Army forces will need documents for refresher training and for keeping abreast of new doctrinal developments. Additionally, due to legal distinctions within CONUS versus outside CONUS (OCONUS), training for AT/FP is, and likely will continue to be, conducted differently.

Currently, Doctrine Division envisions using the Global Information Grid to provide the Special Text (ST) versions as on-line products to facilitate dissemination, reduce costs, and rapidly incorporate changes and updates to the base document. Further, new chapters may address more specialized topics within AT/FP, which we will upload upon completion. If deemed appropriate, there may also be a Service site for data provided via SIPRNET or other secure links.

Leader Development. Our leaders must develop and maintain proficiency in accomplishing AT/FP operations and with doctrine-related TTP. Once the documentation is in place, incorporation of the doctrine into lesson plans, programs of instruction, and other

material will fall into place. Leaders will experience AT/FP differently, dependant upon their assignments in CONUS or OCONUS; this aspect may affect their perceptions throughout their careers. For future assignments, the Army must consider experiential differences; for example, if leaders have not yet worked AT/FP matters overseas, their next tours should provide growth opportunities OCONUS.

Organizations. Currently, neither MI Branch nor the Army at large has any force structure designed specifically for AT/FP. The Army and MI Branch can, however, task-organize personnel and equipment to execute these special requirements. Some CONUS organizations may have no significant role for AT/FP, while others may be loaded with taskings. OCONUS commanders are fully aware of and have the capabilities to execute the AT/FP mission due to their experience, lessons learned, different legal parameters, and so forth.

Soldiers. While soldiers can research doctrine in FMs, joint publications, Army regulations, or via the on-line Reimer Digital Library, they must first know that the doctrine exists. Soldiers must also know where to locate this doctrine. As we train new MI soldiers, they will carry this knowledge with them to the field. Additionally, professional magazines, such as the ***Military Intelligence Professional Bulletin***, facilitate disseminating this information.

Implementation

Standardization of AT/FP doctrine and TTP is a revolutionary project. Inherent to this concept are several facets:

- ❑ Shorten the doctrine development timelines.
- ❑ Staff development with critical stakeholders.
- ❑ Integrate it Armywide.
- ❑ Remain focused on the warfighter.

Beyond AT/FP

In addition to the on-going efforts and issues described above for AT/FP doctrine, there is also no consolidated reference for the more highly specialized and resource-intensive offensive counterterrorism (CT) operations. Work is also continuing in this arena.

Conclusion

As overarching Homeland Security matters solidify, it will become easier to orchestrate unity of effort. For the Army, standardization of intelligence doctrine and TTP for AT/FP operations will benefit all Army units, including those deploying or already deployed. Standardization will allow commanders and soldiers at all echelons through the full spectrum of operations to identify, find, and understand quickly, and to use the information effectively. They can thereby better support the Armed forces anytime, anywhere, under any circumstances.

Chief Warrant Officer Three Del Stewart is a doctrine writer for the Doctrine Division, Concepts Directorate, Futures, U.S. Army Intelligence Center and Fort Huachuca. Readers may contact him via E-mail at del.stewart@hua.army.mil. The Doctrine Division's primary point of contact for Homeland Defense and related matters is Chief Warrant Officer Five Green; his E-mail address is clyde.green@hua.army.mil.

Would You Like to Contribute to *MIPB*?

The ***Military Intelligence Professional Bulletin*** is your magazine and we need your support in writing articles, letters to the editor, and book reviews for publication. When writing an article, select a topic relevant to the MI community; it could be historical or about current operations and exercises, equipment, TTP (tactics, techniques and procedures), or training. Explain lessons learned or write an essay-type thought-provoking piece. 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 new technology will change the way we operate.

MIPB Themes and Deadlines for Article Submission

2002-2003

Issue	Theme	Deadline
Oct-Dec 02	Battlefield Visualization and Presentation	5 Jul 02
Jan-Mar 03	Fundamentals of MI (ISR Integration and Synchronization)	5 Oct 02
Apr-Jun 03	Force Protection	5 Jan 03
Jul-Sep 03	Information Operations	5 Apr 03

The ***MIPB*** staff will edit the articles and put them in a style and format appropriate for the magazine. All those who submit articles, letters, or book reviews will get two copies of the issue in which their input appears.

Proponent Notes

Stop Loss. As of 5 April 2002, the Stop Loss continues unabated. The only significant adjustment under discussion is a suggestion by the Army Deputy Chief of Staff (DCS) G2 and the MI Proponent to target Stop Loss by grade, skills, and specific language. Since many of our military occupational specialty (MOS) shortages are for specific grades, this action would certainly bring relief to some of our MOSs. Army guidance is undergoing reassessment monthly so your best sources of current information will be your local adjutant general and Personnel and Administration Center (PAC). You may also want to check the U.S. Total Army Personnel Command (PERSCOM) homepage at http://www.perscom. army.mil/ for their latest information.

Army Training and Leader Development Panel (ATLDP). We have also been heavily involved in working with the ATLDP during the last few months. As you may recall, the Chief of Staff of the Army (CSA) established the ATLDP to examine training and leader development as a fundamental part of Army Transformation. By way of update, the commissioned officer panel is complete and the noncommissioned officer (NCO) effort is nearing completion. The warrant officer (WO) effort is in its final stages and the results should be briefed to the CSA sometime this summer. Chief Warrant Officer Five Lon Castleton, the Chief Warrant Officer (CWO) of the MI Corps, is a member of the Executive Warrant Officer Panel and will continue to represent the MI Corps in this important effort. We will keep you apprised of changes as they are approved.

The Director, Office of the Chief, Military Intelligence (OCMI) is Lieutenant Colonel Eric W. Fatzinger. Readers may contact him via E-mail at eric.fatzinger@hua.army.mil.

Enlisted Actions

For this issue of the ***Military Intelligence Professional Bulletin* (MIPB)**, I have elected to provide a few notes to highlight the impor-

mation on proponent issues relevant to soldiers and leaders in the field. Currently on the OCMI website are a wide range of topics to include promotion board input and results, MOS Career Maps, Notice of Future Change (NOFC) documents, and MI Proponent points of contact. In the near future, we hope to add an SGM Hot Topics section that will be a direct line to me as the OCMI SGM. Take a look at the site at http://huachuca-usaic.army.mil/ocmi/ and let me know what you think. As with all websites, we are at the mercy of the server, so if you have trouble connecting, try again later in the day.

Upcoming NCO Boards. The calendar year 2002 Sergeants First Class (SFC) list should be available during late August 2002. The CSM/SGM Board will meet during 1-23 October 2002. *The point of contact (POC) for enlisted actions is SGM Crossman via E-mail at walter.crossman@hua.army.mil.*

Warrant Officer Actions

The following is an update of some of the actions we are taking to improve warrant officer accessions, training, and utilization assignments.

MI Senior WO Work Group Initiatives. In March 2002, the DCS G2 and Commanding General, U.S. Army Intelligence Center (USAIC), received an initial response from the Army DCS G1 on the 15 recommendations addressing WO issues developed by an MI Senior Warrant Officer Working Group. This working group represented PERSCOM, the Army DCS G1, the Warrant Officer Career Center, U.S. Army Forces Command (FORSCOM), the U.S. Army Reserve (USAR), U.S. Army National Guard (ARNG), U.S. Army Intelligence and Security Command (INSCOM), DCS G2, and USAIC. The group submitted its recommendations in June 2001.

The events of 11 September 2001 delayed the response but now the actions are moving forward. Those actions requiring further study and coordination went back to the appropriate agencies and those that were immediately actionable are already undergoing implementation. We were especially pleased with the reception given to both pay differentials and pay incentives. Many of the issues went to the ATLDP with a supporting DCS G2 endorsement; by the time you read this, they should be on the way to the CSA for resolution or decision. We hope to update you with more specifics in the next issue of ***MIPB***.

Army Development System (ADS) XXI Task Force. The responsible agencies are implementing the recommendations submitted by the ADS XXI Task Force and approved by the CSA for implementation in May 2001. (The task setup was to address WO and enlisted issues much as the Officer Professional Management System (OPMS) XXI Task Force addressed commissioned officer issues.) Some of the more noteworthy WO recommendations undergoing implementation include—

- ❑ Rollback the Active Component (AC) WO grade structure to fit the Army model. This should immediately improve overall WO promotions within MI. The DCS G1 tasked all proponents to submit the grade adjustments in March 2002. They should be at the major Army commands (MACOMs) for their comments by this writing. For MI, this meant recoding 73 CW4 positions to CW5, CW3, or CW2 to balance our grade structure.
- ❑ Assign AC WOs by grade. PERSCOM is now doing this to the extent possible. In the long run, this should help put the right person with the right experience in the right job. In the near term, however, expect some growing pains.
- ❑ Establish a WO tenure program. The Army is now working this program, which will allow continuation of twice "non-select" CW3 and CW4 on active duty until they are retirement-eligible.
- ❑ Implement the U.S. Army Training and Doctrine Command (TRADOC) recommendation to expand the WO technical accessions base. This could mean recruiting some WO candidates from trade schools, the other Services, or from related feeder MOSs.
- ❑ Design training specifically for warrant officers' next assignments, dubbed "assignment-oriented training."
- ❑ Implement the DCS G3 is working a recommendation to access WOs at the five- to eight-year time-in-service mark. If the Army was able to access WOs within this timeframe, it could potentially eliminate our shortage of senior grade WOs. Currently, the average MI WO pins on warrant officer one (WO1) rank at 10.8 years time in service.
- ❑ Overhaul the WO Candidate Course. This recommendation is also at HQ TRADOC for approval. This would provide a phased approach to the course acknowledging attendance at the Basic and Advanced NCO Courses (BNCOC and ANCOC, respectively) for candidates that have met that requirement.

The POC for Warrant Officer Actions is CW5 Castleton via E-mail at lon.castleton@hua.army.mil.

Officer Actions

ROTC Summer Camp. Branch orientation days will not be conducted this year at the ROTC Basic Camps at Fort Knox, Kentucky, by any branch proponent. OCMI, however, will provide support for both Advanced ROTC Summer Camps at Fort Lewis, Washington, in June and again in August.

Officer Education System (OES) Update. Development of the OPMS XXI OES is progressing. The Process Action Team for the Leader Develop-

ment Campaign Plan hosted another OES Conference in March. The Army has yet not finalized intermediate-level education (ILE) decisions. However, we continue to get further guidance. Essentially, the three-month common core will give all majors Military Education Level Four (MEL-4) and Joint Professional Military Education Level One (JPME-1). Following that, the Operations Career Field officers (including Branch 35) will go on to attend the Advanced Operations and Warfighting Course while officers designated to a Functional Area will go to their functional-area qualification training. If the CSA approves this approach, then assignment of officers to attend the resident CGSC (Command and General Staff College) course at Fort Leavenworth, Kansas, will become a personnel process and not a board selection action. We anticipate that this may happen as early as June 2003. There are also significant changes in the works for the Officer Basic (Lieutenants) and Career Courses (Captains) across the Army. As information on these become final, we will provide additional updates.

MI Officer Website. The OCMI has updated its home page and the officer section now includes both Branch 35 and Functional Area 34 information. OCMI recommends that you check this site on a regular basis as we will post new information when it is available.

Upcoming Officer Selection Boards. The tentative dates for the only remaining fiscal year 2002 officer selection boards are Colonels on 30 July through 23 August and Command and Staff Courses (CSCs) on 20 August through 20 September. Remember, it is essential that you have an up-to-date photo in your files—do **not** wait until the last minute. *The POC for officer actions is Ms. Borghardt at E-mail charlotte.borghardt@hua.army.mil.*

Readers can access the OCMI website through the Intelligence Center Homepage at http://usaic.hua.army.mil/, then linking to OCMI with the "Training/MI Professionals" button. You will be able to find information on issues ranging from enlisted career field overviews to officer, warrant officer, and civilian updates.

Lieutenant Colonel Eric Fatzinger is currently the Director, Office of the Chief, Military Intelligence (OCMI). Readers may contact him via E-mail at eric.fatzinger@hua.army.mil and by telephone at (520) 533-1173 or DSN 821-1173. The Deputy Director is Robert C. White, Jr. You can contact him through E-mail at robert.white@hua.army.mil and telephonically at (520) 533-1190 or DSN 821-1190.

The Official Logo for the Army's 227th Birthday

This logo is the official design commemorating the 227th birthday of the U.S. Army. Since 14 June 1775, when the Second Continental Congress approved and enacted legislation to establish an army, the U.S. Army has been "On Duty For America's Freedom."

The U.S. public and the rest of the world are reminded of this theme whenever they see our soldiers through the eyes of the media—both on television and in print—serving in Afghanistan and supporting our homeland against terrorist threats. They have performed their missions with professionalism and pride for 227 years.

The front image of the logo signifies that the Army is deployed worldwide (the soldier on the right) as well as here in our nation's communities providing frontline support for Homeland Defense (the soldier on the left). Our nation's colors and the bald eagle represent a visual image of the United States and her values.

The reverse image of the logo is a reminder that in the oath of office every soldier and civilian swears or affirms to "*support and defend the Constitution of the United States against all enemies.*" The Preamble to the Constitution—beginning with the unforgettable line "We the People"—is depicted in the center of the logo's reverse side. The phrase around the Preamble—"Support and Defend Against All Enemies"—is the short and most precise mission statement that all soldiers carry with them throughout their careers. The wars and challenges that soldiers and civilians have faced for 227 years may change over time; however, their mission to support and defend the Constitution remains constant!

TSM Notes

Operational Test of the CHIMS Software and Hardware

by Michel M. Strack

Between 18 and 23 March 2002, the Army conducted an Operational Test (OT) at Fort Hood, Texas, of all the new Counterintelligence (CI) and Human Intelligence (HUMINT) systems. These systems incorporate common baseline software called "CI/HUMINT Automation Management System (CHAMS)." CHAMS, the baseline software, provides for common functionality and user interface across all the platforms discussed herein and provides increased capabilities at all echelons. The hardware pieces of the system include the Individual Tactical Reporting Tool (ITRT), the CI/HUMINT Automated Tool Set (CHATS), and the Counterintelligence/Human Intelligence Workstation (CI/H WS). This software includes select modules of the All-Source Analysis System/Army Tactical Light Analysis Systems (ASAS/ATLAS) baseline providing CI/HUMINT systems with the requisite interoperability to the rest of the Intelligence battlefield operating systems.

Software Functionality

During the test, we found the new CHAMS software to be a vast improvement over the existing CI/HUMINT Utilities software found on previous equipment. The system is much more powerful, in terms of both the processing hardware and software improvements that include the Microsoft™ (MS) Windows® 2000 operating system. This operating system meets the security concerns, eliminating the need for additional security software that has caused some problems in the past.

CHAMS provides common basic functionality and user interface from the ITRT to the CI/HUMINT Workstation. This will simplify training here at the U.S. Army Intelligence Center and Fort Huachuca, for the New Equipment Training Teams, and in the proficiency training within the unit. Additionally the Windows 2000 baseline provides a user interface familiar to almost everyone. System crashes are almost nonexistent and the new software will also be usable with the existing CHATS Version 2 (V2). We will make every effort to get the new software to the field as soon as possible.

The CHAMS software also gives increased functionality for things like performing analysis (CrimeLink[1]) and posting the results of this analysis onto web pages (using the Apache Web Server) so analysts can easily share information. Other commercial software on these systems includes MS Office 2000 Pro, MS Internet Explorer, WinZip®, Paint Shop Pro®, Norton AntiVirus™, and device driver software.

Government software will include Foreign Area Language Converter (FALCon) and the Biometrics Automated Toolset (BAT). FALCon, which provides text-based language translation, was produced by the Army Research Lab. The BAT is able to read and record fingerprints and do limited facial recognition; it will include a Federal Bureau of Investigation-compliant fingerprint reader. The integration work for these packages was not complete in time for the test but they will be in the 4.1 version CHAMS software (fielded version).

Courtesy of Norm Boring, SETA Support to PM-CHIMS.

Individual Tactical Reporting Tool (ITRT), AN/PYQ-8(V)1.

CI/HUMINT Automated Tool Set (CHATS), AN/PYQ-3(V)3.

Formats and Peripherals

The bases for the reports, messages, and masks on the system are current doctrine and the Defense Counterintelligence Information System (DCIIS). CHAMS V4.1 will not only support U.S. Message Text Format (USMTF) but also provides support for investigations, collections, and analysis through the use of DCIIS-like data-based reports and Form-Flow™ or MS Word® templates.

New peripherals also complement the systems. The CHATS comes with a Nikon 995 high-resolution digital camera capable of both still photography and video clips. New printers, scanners, compact disc read-write drives, and large flat-screen monitors for the CHIMS workstation are some of the other improvements. The total packaging of the systems includes water- and dust-resistant cases suitable for shipping as well as versatile *"taking only what you need"* carry-on soft bags and hard cases.

Toughbook-Based Workstations

The ITRT, AN/PYQ-8(V)1, is an individual device for use by each CI agent and HUMINT collector in the field to aid in the collection and reporting of information. A Panasonic Toughbook CF-34 hosts the ITRT.

The CHATS, AN/PYQ-3(V)3, is based on a Panasonic Toughbook CF-72, and provides team leader-level automation and management functions for collecting and reporting information. Many of you are already familiar with the CHATS V1 and V2 that have been in the field for several years. The CHATS tested and being fielded is now a much-improved Version 3.

Finally, the CI/H Workstation, AN/PYQ-7(V)1, is also built around a Panasonic Toughbook CF-72. The CI/H WS provides management and analysis capabilities at levels from MI battalion operations through brigade and task force G2 to theater-level CI staff officers.

The Operational Test

The 321st MI Battalion (Reserve Component), currently activated and serving as the CI/HUMINT Battalion of the 504th MI Brigade at Fort Hood, Texas, volunteered for the duty and was selected as the test unit for the CI/HUMINT Information Management System (CHIMS) operational test. The simplicity of that statement could be misleading. This OT was the culmination of a great deal of work by many agencies during several months. Much work had been done in the last year with the initial test unit, the 202d MI Battalion, 513th MI Brigade. When current world events necessitated that the 202d MI Battalion focus its efforts elsewhere, many months of preparation had to change overnight.

CI/HUMINT Workstation (CI/H WS), AN/PYQ-7(V)1.

In order to keep the existing test schedule, the Army had to accomplish a significant amount of work in a short time. The final test unit, the 321st MI Battalion, began training on the new systems in January and continued through the final test.

Basis of Issue

Now that the testing is complete, selected units could be receiving the systems as soon as May 2002; these units include III Corps, XVIII Airborne Corps, and the Special Forces. Additional funding has made this possible, with fielding for other units to begin possibly after the fielding decision in September 2002.

The OT tested all the systems' communications capabilities over the Single-Channel Ground and Airborne Radio System (SINCGARS), Secure Telephone Equipment (STE), Mobile Subscriber Equipment (MSE), and local area network (LAN). The ability to communicate via the PSC-5 (SPITFIRE) Tactical Satellite, International Maritime Satellite (INMARSAT), TROJAN SPIRIT (Special Purpose Integrated Remote Intelligence Terminal), AN/PRC-117 manpack radio, and the AN/PRC-138/150 radios, while not yet tested, will all be demonstrated prior to fielding.

We know that every unit is different, but the simple answer for basis of issue of the equipment is three ITRTs per four-man CI/HUMINT team, and one CHATS per CI/H team leader. This gives each team member an automation device.

Issue of the CI/HUMINT WS will be one per CI/HUMINT battalion (at corps and theater support). There will be one for each division-level MI battalion operations section, as well as one for the CI staff officer at brigade (Interim Brigade Combat Team or IBCT) and higher levels.

Conclusion

We believe that CHAMS and the associated hardware will offer a great hardware addition to echelons currently without automation and provide increased management and analysis through improved software capabilities. With the completion of the OT, the CI/HUMINT Team at the TRADOC System Manger All-Source Analysis System (TSM-ASAS) will begin anew.

One of our jobs is to identify requirements for the next generation of CI/HUMINT systems. To do this, we need your input. Please contact us with your requirements, suggestions, and ideas. We will continue to improve the fielded software by making incremental software drops throughout its life cycle. We will incorporate improvements that we cannot implement as incremental changes in the next generation of hardware and software. It does, however, require your input if we are to get it right.

We will try to contact interested readers through the ASAS User's Conferences, and unit visits, but we are always glad to receive phone calls or E-mails here at the office. Visit our website for contact information at http://tsmasas.futures.hua.army.mil. Share your experiences and ideas and together we can continue to provide you with better products to meet the intelligence needs of commanders' worldwide.

I wish to thank Ed Carter and Cecil Dildine for their contributions.

Endnote

1. CrimeLink is an investigative analysis tool designed to assist the intelligence analyst in compiling data into various formats (e.g. time event charts, link analysis, telephone charts, and association matrices).

Mike Strack is the Acting TRADOC System Manager (TSM) for ASAS. Readers may contact him via E-mail at mike.strack@hua.army.mil and telephonically at 520-533-3507 or DSN 821-3507. Lieutenant Colonel Vic Fink is the Deputy TSM; readers can reach him through E-mail at james.fink@hua.army.mil and by telephone at 520-533-5145 or DSN 821-5145. Please visit the TSM ASAS website at http://www.tsmasas.hua.army.mil.

Update on Joint STARS, JTT, CGS, and the Distributed Common Ground System-Army

by Colonel Stephen J. Bond

The U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM) for the Joint Surveillance Target Attack Radar System (Joint STARS) and the Program Manager (PM) have been actively involved with the Common Ground Station (CGS) and the Joint Tactical Terminal (JTT) in preparing, deploying, and supporting systems with Army and joint elements participating in Operation ENDURING FREEDOM. We have also continued our efforts to meet the demands of Army Transformation. One example of this latter effort, within the next year, will be TSM Joint STARS' formal designation as the TSM for one of Military Intelligence's flagship Objective Force systems, the Distributed Common Ground Station-Army (DCGS-A). We will provide more on this future system in the coming months.

Joint STARS Tactics, Techniques, and Procedures (TTP)

The Joint STARS MultiService TTP are currently under review by the Air, Land, and Sea Agency (ALSA). This draft ALSA document, dated March 2002, will become Army **FM 2-00.1,**

Joint STARS: MultiService Tactics, Techniques, and Procedures for the Joint Surveillance Target Attack Radar System, in the future. It is currently available on the Internet to ".mil" users at http://www.dtic.mil/alsa/pubs/JointSTARS2ddraft.pdf. Commanders and staffs at all levels using Joint STARS or CGS will find this document useful. It provides a succinct depiction of Army and Marine operations with CGS and on Joint STARS tasking, missions, and operations.

Joint Tactical Terminal (JTT)

The JTT is a project designed to replace current Commanders Tactical Terminals (CTTs) and other tactical receive equipment. It is the designated receiver for the "Legacy" information broadcasts, including the—

- TRAP (Tactical Related Applications Program) Data Dissemination System (TDDS).
- On-Board Processing/Direct Down-Link (OBP/DDL), formerly called Tactical Data Information Exchange System-B (TADIXS-B).
- Tactical Information Broadcast Service (TIBS).
- Near-Real-Time Dissemination (NRTD).
- Tactical Reconnaissance Intelligence Exchange System (TRIXS).

The JTT will also be the receiver and transmitter for an Objective Force, information superiority enabler, the Integrated Broadcast Service (IBS).

As part of Operation ENDURING FREEDOM, selected units received, on an "urgent need basis," the briefcase version stand-alone model of the JTT. The Army accelerated this system from limited production quantities and placed it into the hands of users. It is currently and successfully in use by operational elements to provide locational information on threat elements and friendly forces for force protection (FP) purposes.

The JTT terminal will also be a component of Legacy systems such as CGS, All-Source Analysis System (ASAS), Tactical Exploitation System (TES), Guardrail Common Sensor Improved Processing Facility, and future Objective Force systems such as Aerial Common Sensor (ACS) and the Distributed Common Ground System-Army. Air Defense and Aviation systems will also host the JTT, as well as aircraft, ships, and ground stations from other Services and Special Operations Forces. The JTT project will have a scheduled production decision in late 2002. TSM Joint STARS is the designated TSM or user representative for JTT.

CGS Software Upgrade

As part of the Army's Future Digitized Division (FDD) and Army Transformation initiatives, we modified the CGS software to enable any Army Battle Command System (ABCS) or Army Tactical Command and Control System (ATCCS) workstation to display a view from the CGS. The Common Ground Station can also bring in any ABCS or ATCCS screen display. This new software was in CGSs in the 4th Infantry Division (Mechanized) (the FDD) and in the 3d Brigade, 2d Infantry Division (the IBCT-1). This upgraded CGS software version, Common Software Baseline (CSB), is currently undergoing fielding to other units, beginning in June 2002. This software also facilitates satellite communications (SATCOM) and tactical unmanned aerial vehicle (TUAV) connectivity.

Joint CGS-Joint STARS Training Initiative

In an effort to improve Joint STARS-related training, the PM and the TSM Joint STARS-CGS, in conjunction with the U.S. Air Force, are developing a "Joint Distributive Virtual Combat Range" (JD VCR) concept. JD VCR is a distributive mission training concept that makes use of modeling and simulation; it will provide CGS crews realistic training from their homestations. The JD VCR has three components—the synthetic battlespace "hub," the CGS "outstation," and the network infrastructure that connects the geographically dispersed outstations to the hub. The concept is for CGS crews to connect virtually to a synthetic battlespace that can provide a realistic, tactically relevant scenario for training with Joint STARS crews. The intent is to leverage an existing virtual battlespace built and managed by the Air Force's Theater Air Command and Control Simulation Facility (TACCSF) at Kirtland Air Force Base, New Mexico. Designated the joint distributed training hub for the Air Force, this $250 million facility hosts quarterly exercises called "Desert Pivot."

While the main users of the facility have been Air Force units, the TACCSF is eagerly expanding to integrate the training needs of the other Services to create joint training opportunities. Our plan in working with the TACCSF is to offer eventually monthly training opportunities to CGS crews and to facilitate quarterly joint training opportunities for CGS crews and intelligence staffs from brigade through corps levels. Last July, we demonstrated the capability to connect the TACCSF's battlespace to multiple CGSs from Fort Huachuca, Arizona, using a dedicated T1 line. The CGS crew successfully sent radar service requests and received moving target indicator data and synthetic aperture radar imagery. Additionally, they were able to receive UAV telemetry from a simulated Hunter UAV "flying" within the virtual battlespace. We will draw on Desert Pivot exercises in May and September 2002 to demonstrate the viability of using a more eco-

nomical network infrastructure that can reach the many CGS outstations rather than using dedicated T1 lines. We anticipate being ready to connect "pilot" CGS outstations for the Desert Pivot exercise scheduled in December 2002. Once this occurs, we will be seeking units with CGSs to participate in this training. For more information on the JD VCR concept, please contact the TSM or the JD VCR Project Leader, Major Tim Chyma (Assistant Program Manager CGS) via E-mail at timothy.chyma@iews.monmouth.army.mil and by telephone at (732) 427-4278 or DSN 987-4278.

Colonel Steve Bond is the U.S. Army Training and Doctrine Command (TRADOC) System Manager (TSM) for Joint STARS, Common Ground Station, and the Joint Tactical Terminal. Readers can contact him via E-mail at bonds@hua.army.mil and telephonically at (520) 533-3605/2480 or DSN 821-3605/2480. The Deputy TSM is Lieutenant Colonel Trip Sproul. Readers can reach him at sproulm@hua.army.mil and telephonically at (520) 533-8937 or DSN 821-8937.

Olmsted Scholarship—
The Greatest Leaders Are Educated Broadly

The Olmsted Scholarship is a fantastic but perhaps little known opportunity for Army officers. While serving full time on active duty, Olmsted Scholars learn a foreign language and then do two years of post-graduate study at a foreign university. The program's intent is to recognize and develop senior military leaders. Although relatively few military intelligence (MI) officers have served as Olmsted Scholars, the program is particularly well suited to the development of future MI leaders.

Officers who have completed at least three, but no more than eleven, continuous years of active duty service are eligible to apply. Officers apply by seeking permission from MI Branch at the U.S. Army Total Personnel Command (PERSCOM). The officer submits a formal request letter and endorsements. MI Branch then decides whether to forward the officer's request, a decision based on the competitiveness of the officer's file and appropriateness of the Olmsted Scholarship for his or her career path. The branches forward their nominees' packets; PERSCOM reviews the officers' packets and selects seven Army candidates for the scholarship. These officers' files go before the Olmsted Foundation Board, which routinely meets at the end of April. The Olmsted Board then selects that year's class and the locations where they will study. Once selected, the officers commence language study at the earliest opportunity, either at the Defense Language Institute (DLI) or at another institution.

After completing the language training program, the students make permanent-change-of-station moves to their designated countries, where they will have the opportunity and funding to continue their language training. Scholars begin post-graduate studies with the commencement of their chosen academic program, spending two years studying, learning, traveling, and immersing themselves in the local culture to the greatest extent possible. By direction, Olmsted students have as little contact as possible with U.S. facilities and personnel. The scholarship includes funding for tuition, books, and cultural and educational travel. Officers continue on active duty and receive all regular pay and allowances from the Army. This is a rare opportunity.

A program focused on developing leaders that also affords officers the opportunity to learn a foreign language, conduct post-graduate study in the social sciences and international relations, and immerse themselves in foreign cultures has obvious application to MI leader development. The post-graduate studies focus on research and writing—good preparation and practice for senior MI officer-analysts. Learning a foreign language—besides opening one's mind and perspective—also offers Olmsted Scholars the opportunity to understand soldier-linguists better by sharing in the DLI experience and the rigors of the Defense Language Proficiency Test (DLPT). Foreign immersion, although not specifically oriented toward MI analysis, obviously enhances officers' abilities to understand those coming from different backgrounds. This, at a minimum, contributes to our understanding of current or potential alliance partners. It also helps MI officers develop their ability to "Think Red."

In the 41 years of the Olmsted Scholar Program, the Olmsted Board has selected only nine Army MI officers as scholars. In recent years, the Olmsted Foundation, in concurrence with the Services, has expanded the number of candidates chosen annually. Thus, now is an opportune time for junior officers to apply to become Olmsted Scholars. We, as a Branch, should strive to identify and promote our young leaders to take advantage of this fantastic opportunity.

Additional information regarding the Olmsted Scholarship is available on the Olmsted Foundation's website at http://www.olmstedfoundation.org. MI Branch at PERSCOM also has useful information on the program under Future Readiness Notes on its web page at http://www.perscom.army.mil/OPmi/minews.htm.

Readers may contact Major Tim Chafos via E-mail at timothy-chafos@us.army.mil.

304th Notes

Officer Training

by Ken L. Welsh

The 304th Military Intelligence Battalion at Fort Huachuca, Arizona, is responsible for conducting intelligence training for Army field grade officers. The purpose of this article is to provide information about these courses.

Military Intelligence Precommand Course (PCC)

Developed in the mid-1970s, the MI PCC provides MI Active and Reserve Component (RC) battalion and brigade command-designees with a review and update of major ongoing doctrinal, organizational, equipment, and process developments to prepare them to be effective commanders. The course also trains Aviation officers who will command MI aerial exploitation battalions (AEBs), and Acquisition Corps officers who will serve as MI systems project managers. Due to the wide variety of units our students will command, we tailor each class to meet the students' needs.

PCC student training is in a small-group environment, and subject matter experts and guest speakers lead discussions. We also arrange one-on-one assignment-oriented training as requested by students. We conduct the MI PCC three times each year. The exact class dates are in the Army Training Requirements and Resources System (ATRRS) and the course number is 2G-41. (The ATRRS homepage is at http://www.atrrs.army.mil/info/atrrsinfo.asp.)

G2 and ACE Chief Course

Fort Huachuca developed the G2/ACE Chief Course in 1998 based on the need to better prepare division G2s and analysis and control element (ACE) chiefs, warrant officers, and senior noncommissioned officers (NCOs) notified of assignment to an ACE. The first week of this three-week course is strictly for personnel never before assigned to an ACE. It focuses on automated intelligence systems, intelligence architecture, and ACE section operations. Beginning with the second week, the course includes the G2s and focuses on G2 operations. During the last week, the ACE chiefs participate in the MI Captain's Career Course capstone exercise while the G2s travel to Washington, D.C., to receive briefings from national intelligence agencies.

A critical part of the G2/ACE Chief Course is the presentations made by former division G2s and ACE chiefs. These presentations address actual operations and the guest speakers provide insights and share their experiences with the prospective G2s and ACE chiefs.

We offer the G2/ACE Chief course twice a year and the exact class dates appear in ATRRS; the course number is 3A-F73. This course is open to active duty and RC G2s, G2 sergeants major, ACE chiefs, ACE warrant officers, and ACE NCOs in charge.

Strategic Intelligence Officer Course (SIOC)

The 304th MI Battalion developed the SIOC in 1999 to support the Army's Officer Personnel Management System (OPMS) XXI. Under OPMS XXI, the Army developed a new Career Field Designation (CFD) for Strategic Intelligence Officers. Functional Area (FA) 34 replaced the old 35B Strategic Intelligence area of concentration. Formerly, MI Branch officers filled the 35B positions, but FA 34 is open to officers from all branches.

The SIOC will prepare field grade officers for assignments to intelligence positions at joint and national levels. The course teaches basic through advanced intelligence subjects, with emphasis on analysis and collection management. During the course, guest speakers from various joint commands and national agencies provide insight into the roles and responsibilities of Strategic Intelligence Officers. The class training is in a small group environment and requires completion of research, written assignments, and intelligence briefings outside scheduled class times. A common thread throughout the course is the Army's contribution to joint operations.

We hold the SIOC once a year between the Command and General Staff College Course graduation and the beginning of the Postgraduate Intelligence Program (PGIP). Specific dates for course 3A-34(T) are in ATRRS. The course is open to officers selected for FA 34. Prospective participants should coordinate their attendance through the FA 34 assignments officer.

Ken Welsh is the point of contact for the MI PCC and G2/ACE Courses. Readers may contact him via E-mail at ken.welsh@hua.army.mil and by telephone at (520) 533-6527 or DSN 821-6527. Captain (P) Robert Scanlon is the POC for the SIOC. You may reach him via E-mail at robert.scanlon@hua.army.mil and telephonically at (520) 533-1466 or DSN 821-1466.

Military Heritage

Citizenship by Choice: Alfred Rascon

by Katherine W. Schmidli

Most of us in the Military Intelligence community were born in the United States where our citizenship is automatic. However, when do we choose to accept the responsibility for our citizenship by taking on the duties of defending our freedom and democratic process? Perhaps it occurs when we travel overseas and witness the alternatives to democracy, or when we read intelligence reports or hear survivor accounts of repression and strife in other countries. Do we choose to become actively involved when we compare our national ethos with that of others and conclude that the freedoms we experience in the United States outweigh the flaws?

Alfred Rascon was always involved. He was always "American by choice." Born in Chihuahua, Mexico, he immigrated with his family to Oxnard, California, where he attended school and grew up thinking he was an American. After graduating from high school in 1963, Rascon joined the Army.

It was only when he enlisted that Alfred Rascon discovered that because he was born in Mexico, he was not an American citizen. Even so, the U.S. Army accepted him, trained him as airborne and a combat medic, and assigned him to 1st Battalion, 503d Parachute Infantry Regiment, 173d Airborne Brigade (Separate).

In May 1965, Alfred Rascon went to Vietnam to serve with the Reconnaissance Platoon of the 1st Battalion, 173d Airborne Brigade, 503d PIR. He was first wounded in September 1965 on a mission with his Reconnaissance Platoon. Refusing evacuation, he treated five injured soldiers.

In March 1966, as part of Operation SILVER CITY, the 173d Brigade was clearing enemy forces from the Song Be River area in Long Khanh Province. On 16 March, Specialist Four Rascon's reconnaissance platoon was called to assist the 2d Battalion, which had been surrounded by a North Vietnamese Army (NVA) regiment. Advancing through the jungle, the platoon was attacked and suffered a number of casualties including SP4 Rascon. Though shot in the hip and wounded by grenade fragments, he immediately treated his fellow soldiers; then, under grenade attack, he used his own body as a shield to protect two soldiers. Both times he suffered additional injuries. Later in the engagement, despite guidance to pull back and in the face of advancing NVA soldiers, he recovered the platoon's M-60 machine gun and ammunition, which allowed his platoon to hold its position. SP4 Rascon then returned to care for the wounded and had to be forcibly dragged to the medical evacuation area by his fellow soldiers after the firefight. Rascon's wounds were so severe, he was given the last rites but he eventually recovered.

After Vietnam, he earned a college degree and became a naturalized United States citizen. In 1969, he applied for Officer Candidate School and earned a commission as an Infantry officer. He graduated from the Special Forces Qualification Course and the Defense Language Institute (German). He had follow-on orders for an airborne unit in Germany but the Army inexplicably diverted him at the last minute to the 470th MI Group in Panama. There he served as the Assistant Adjutant, an Area Intelligence Officer, and later commanded a Special Forces MI Detachment assigned to the 470th. As a result of this assignment, he received orders transferring him to Military Intelligence Branch.

In 1972, Rascon volunteered to return to Vietnam. This time, he served

The President of the United States of America, authorized by Act of Congress, March 3, 1863, has awarded in the name of The Congress the Medal of Honor to

SPECIALIST FOUR ALFRED RASCON
UNITED STATES ARMY

for conspicuous gallantry and intrepidity at the risk of his life above and beyond the call of duty:

Specialist Four Alfred Rascon distinguished himself by a series of extraordinarily courageous acts on 16 March 1968, while assigned as a medic to the Reconnaissance Platoon, Headquarters Company, 1st Battalion (Airborne), 503d Infantry, 173d Airborne Brigade (Separate). While moving to reinforce its sister battalion under intense enemy attack, the reconnaissance platoon came under heavy fire from a numerically superior enemy force. The intense fire from crew-served weapons and grenades severely wounded several point squad soldiers. Specialist Four Rascon, ignoring directions to stay behind shelter until cover fire could be provided, made his way forward. He repeatedly tried to reach the severely wounded point machine-gunner lying on an open enemy trail, but was driven back each time by withering fire. Finally, he jumped to his feet and, with total disregard for his personal safety, he raced through heavy enemy fire and exploding grenades to reach his wounded comrade. He then intentionally placed his body between the soldier and the enemy machine guns, sustaining numerous shrapnel injuries and a serious wound to the hip. Ignoring his own wounds, he dragged the larger soldier from the fire-swept trail. Hearing a second machine-gunner yell that he was running out of ammunition, Specialist Four Rascon, still under heavy enemy fire, crawled back to the wounded machine-gunner, stripped him of his bandoleers of ammunition, and gave them to the machine-gunner who continued his suppressive fire. Later, Specialist Four Rascon, fearing the abandoned machine gun, its ammunition, and spare barrel would fall into enemy hands, made his way to retrieve them. On his way, he was wounded in the face and torso by grenade fragments, but continued to recover the abandoned machine gun, ammunition and spare barrel items, enabling another soldier to provide added suppressive fire to the pinned-downed squad. While searching for additional wounded, he saw the point grenadier wounded by small arms fire and grenades. With complete disregard for his own life, Specialist Four Rascon covered the wounded soldier with his body thereby absorbing the blasts from the exploding grenades, and saving the soldier's life. As grenades were being thrown at the wounded point squad leader, Specialist Rascon again, in complete disregard for his own life, covered the soldier with his body, absorbing the full force of the grenade explosions. Once more, Specialist Four Rascon was critically wounded by shrapnel, but again he continued to search for and aid the wounded. Although severely wounded, he remained on the battlefield, inspiring his fellow soldiers to continue the battle. After the enemy broke contact, he disregarded aid for himself, and continued treating the wounded and directing their evacuation. Only after being placed on the evacuation helicopter did he allow aid to be given to himself. Specialist Four Rascon's extraordinary valor in the face of deadly enemy fire, his heroism in rescuing the wounded, and his gallantry by repeatedly risking his own life for his fellow soldiers are in keeping with the highest traditions of the military service and reflect great credit upon himself, his unit and the United States Army.

William J. Clinton

as an advisor to an MI unit of the Army of the Republic of Vietnam (ARVN).

From 1974 to 1984, he served in the 4th Infantry Division (Mechanized), attended the Military Intelligence Officer Advanced Course at Fort Huachuca, then returned to the 470th MI Group as an intelligence liaison officer and Detachment A Commander. He left the Army in 1984, having most honorably fulfilled his responsibilities as a U.S. citizen.

Alfred Rascon, however, was not finished serving his country. He dedicated the next ten years to developing intelligence resources for the Justice Department, starting in the Intelligence Division of the Drug Enforcement Agency (DEA). He later transferred, accepting a promotion, and established the first intelligence unit at the United States National Central Bureau (USNCB), the U.S. office of the International Police Organization (INTERPOL). His next promotion moved him into the Intelligence Division of the Immigration and Naturalization Service (INS) where he helped establish the Intelligence and Analysis Branch. He next served as the Senior Special Agent in Charge of Overseas Operations for the Anti-Smuggling Branch of the INS. Later, he returned to the Intelligence Division and served as the Senior Intelligence Operations Officer. In 1995, he became the Inspector General of the Selective Service, a position he held until his retirement in 2001.

This time, it was the United States which was not done with Alfred Rascon. Three months into his retirement, President George W. Bush asked him to accept a Political Appointee-Senate (PAS) confirmed position. His name went forward to the Senate Armed Services Committee with those of the proposed Secretaries of the Army, Navy, and Air Force. He was immediately confirmed without opposition. Now the Honorable Alfred Rascon, he continues to serve the nation as the Director of the Selective Service, with a rank equivalency of Lieutenant General.

In 1994, Alfred Rascon attended a reunion of the 503d Parachute Infantry Regiment where a comrade in arms, former Sergeant Ray Compton, asked him how it felt to be a Medal of Honor winner. Rascon said he did not know, since he had not received anything. Ray Compton told him that after the second action in which he was wounded, nomination paperwork for the award of the Congressional Medal of Honor (CMH) went forward. Ray thought that Rascon had received it and was shocked when Alfred stated that he had not. It took five more years, but Ray Compton and others from the reconnaissance platoon were able to have this oversight corrected, and in 1999, the Secretary of Defense approved the nation's highest combat award for Alfred Rascon's heroic actions in Vietnam.

On 8 February 2000, President Bill Clinton draped the Medal of Honor around Alfred Rascon's neck. He said, *"Thank you for reminding us that being an American has nothing to do with the place of your birth, the color of your skin, the language of your parents, or the way you worship God."*

Alfred Rascon did not automatically obtain his American citizenship. When his family immigrated here, he says he was *"just a poor kid, brought up with nothing...(who) lived in the house behind the big house."* However, Alfred Rascon voluntarily took on the duties of citizenship. He chose to sacrifice his personal safety to protect his buddies in Vietnam, and he chose to become an officer and be responsible for the lives of other men. He chose to go back to Vietnam, and later chose to continue serving our nation in ever-increasing levels of responsibility. For almost four decades, Alfred Rascon's purposeful service has defined what being an American is all about. It is to be American by choice.

Kate Schmidli is the curator for the U.S. Army Military Intelligence Museum at Fort Huachuca, Arizona. She is a retired MI First Sergeant whose first goal is the preservation of MI Corps heritage and soldier histories. 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 schmidlik@hua.army.mil and telephonically at (520) 533-1107 or DSN 821-1107.

Professional Reader

Kaigun: Strategy, Tactics, and Technology in the Imperial Japanese Navy 1887-1941
by David C. Evans and Mark R. Peattie (Annapolis, MD: Naval Institute Press, 1998), 661 pages, $49.95, ISBN 0-87021-192-7.

Sunburst: The Rise of Japanese Naval Air Power 1909 41 er

Introduction to Communication Electronic Warfare Systems

by Richard A. Poisel, Ph.D. (Norwood, MA: Artech House, Inc., 2002), 555 pages.

Dr. Richard Poisel's intent in writing **Introduction to Communication Electronic Warfare Systems** was to provide an introductory-level textbook for communications electronic warfare (EW) engineers. This was in part due to his own experience when he first joined the U.S. Army Communications-Electronics Command as a communication EW systems engineer in 1976. At that time, his sources were college books on the basics of radio and electronic theory, and his own experience. While he had texts and manuals addressing EW systems for radars, none existed for communications EW systems.

Although Dr. Poisel's intended audience for this book was the communications EW engineering community, it is also a good reference for the Military Intelligence signals intelligence (SIGINT) officer, analyst, or operator. The book provides an intermediate-level overview of radiowave propagation theory, how various types of communications systems operate, and the basic engineering principles of communications EW system design. While the number of mathematical equations found throughout the book may seem overwhelming, one does not need an electrical engineering background to understand what the author is saying. The mathematical equations are primarily for illustrative and instructional purposes.

While much of this book focuses on the principles of communications EW system engineering, Dr. Poisel does attempt to address the operational application of communications EW systems. This includes the application of electronic warfare support (ES) as it pertains to detecting, collecting, and locating communications emitters, and electronic attack (EA) which involves the application of directed electromagnetic energy to a communications receiver. However, the reader should be aware that this book does not represent the "state of the art" in communications EW. As the title states, this book is only intended as an introduction to communications EW systems; it will not make the reader an expert in communications EW after reading this book.

Staff Sergeant
John H. Girardeau
Fort Huachuca, Arizona

From Out Front

How to Submit an Article

Please send the article via E-mail to michael.ley@hua.army.mil with a "cc" copy to elizabeth.mcgovern@hua.army.mil or mail it (with a soft copy on disk) to Commander, U.S. Army Intelligence Center and Fort Huachuca, ATTN: ATZS-FDR-CB (MIPB Editor), [expedited shipping: Bldg 61730, Room 102], Fort Huachuca, AZ 85613-6000. (Please do not use special document templates and do send the graphics separately if you submit by E-mail). We can accept articles in Microsoft Office 2000, Word 6.0, Word Perfect 6.0a, and ASCII with Adobe, Corel, and Power Point graphics. Please include with your article—

- ❑ A cover letter with your work, home, and E-mail addresses and telephone numbers, stating your wish to have the article published. Please include your social security number (SSN) so that we can locate you if you transfer, PCS, or ETS/retire before we publish your article; we will protect your SSN and make no other use of it. Also, indicate whether we may put your article on our Internet web site even if we do not publish it in the printed magazine.
- ❑ Pictures, graphics, and crests/logos with adequate descriptions. Try to find good "action" photographs that illustrate your article; photos and other graphics really enliven an article. We need complete captions for the photographs (the who, what, where, when, why, and how), the photographer credits, and include the author's name on photographs. We can return photographs if so requested—be sure to include the address to which you want the photographs sent after we use them. We will gladly accept photographs without articles too.
- ❑ A release signed by your local security officer or SSO stating that your article is "unclassified, nonsensitive, and releasable in the public domain." (***MIPB*** is available for sale by the Government Printing Office and posted on the Internet.)
- ❑ The full name of each author in the byline and a biography for each. The biography should include the author's current duty position, other related assignments, civilian degrees (degree, school, major), and advanced military education (CGSC, War College, SAMS, MSSI, SEIP, PGIP, etc.). (Tell us if we may print your telephone number and E-mail address with the biography.)

Please inform us of your current E-mail address, telephone numbers, and postal addresses if you change jobs, move, or PCS. It can take a year or more before we run some articles.

308th Military Intelligence Battalion

The 308th Military Intelligence Battalion's distinctive unit insignia consists of a compass rose, a shield, a saltire, and two griffin heads. The blue color appearing on the insignia is the primary color associated with the Military Intelligence Corps. The saltire, or diagonal cross-shape, represents strength and cooperation. Griffins embody vigilance, alertness, and courage and reflect the unit's motto and mission as the "Guardians of America." The compass rose alludes to the collection and reporting of critical information and the black and silver shield underscores the night and day scope of the Military Intelligence mission.

The 308th MI Battalion first activated on 1 April 1952 as the Headquarters and Headquarters Detachment, 308th Communication Reconnaissance Battalion, in the Organized Reserve Corps. (The Army later redesignated the "Organized Reserve Corps" as the "Army Reserve" on 9 July 1952.) On 23 January 1956, the Battalion became the Headquarters and Headquarters Company (HHC), 308th Communication Reconnaissance Battalion. The Battalion became HHC, 308th Army Security Agency (ASA) Battalion, on 1 September 1956, and then inactivated 1 July 1959.

On 1 February 1990, the Army redesignated the Battalion as the HHC, 308th MI Battalion and concurrently assigned it to the Regular Army. On 17 October 1991, the unit's name changed and it activated as the Headquarters and Headquarters Service Company, 308th MI Battalion, in Panama. The Army inactivated the Battalion from Panama on 16 September 1995. The U.S. Army Counterintelligence Security Battalion inactivated and redesignated as the 308th Military Intelligence Battalion on 16 October 1995.

The mission of the 308th MI Battalion is to neutralize foreign intelligence services' activities directed against U.S. Army forces, secrets, and technology. The Battalion consists of four companies located at Fort Meade and Aberdeen Proving Ground, Maryland; Redstone Arsenal, Alabama; and Fort Leavenworth, Kansas. A combination of 27 military intelligence detachments and resident offices located throughout the continental United States support the companies.

Guardians of America!

Comander
U.S. Army Intelligence Center and Fort Huachuca
ATZS-FDR-CB (12)
Fort Huachuca, 85613-6000

BULK RATE
U.S. POSTAGE & FEES PAID
NIAGARA FALLS, NY 14304
PERMIT NO. 300

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

PIN: 063028-000