

# MIPB

**Military Intelligence Professional Bulletin**

**July-September  
2003**

**PB 34-03-3**



**Intelligence Support to  
Information Operations**

# From the Editor

Information operations (IO), and intelligence support to IO, are simultaneously frustrating and intriguing. This “new” field of warfare fascinates many. A word of caution is advisable.

*...there is no new thing under the sun.* —Ecclesiastes 1:9

Indeed, if one considers the various forms and types of IO, one can easily make the case that various forms of IO have been around for more than 2,500 years. Need proof?

**Therefore there are five kinds of spies used: local spies, internal spies, double spies, doomed spies, and living spies.... For doomed spies we use agents to spread misinformation to the enemy.... This is essential for warfare, and what the army depends on to move** [emphasis added]. —Sun Tzu, *The Art of War*, Chapter 13, *The Use of Spies*

Information is a weapon and a force multiplier. This crystal-clear understanding of the nature of information is the primary underpinning to all of our current security regulations; that is, to protect friendly information. Likewise, this understanding is precisely what drives our need to collect information about our adversaries; establish priority intelligence requirements; conduct the art and science of intelligence synchronization; engage intelligence, reconnaissance, and surveillance systems; and so forth. That IO now extends to the World Wide Web, and includes “cyberwarfare,” assessment of adversary and neutral media sources, etc., does **not** make it a new principle of war. It is merely that with these new applications, we are in the process of considering the IO aspect of war in new ways, with new implications and ramifications.

When considering carefully the contributions contained in this issue of *MIPB*, it is vital to return to the basic definitions of terms. Some of these appear below:

**Essential Elements of Friendly Information (EEFI)** are questions by adversary officials and intelligence systems are likely to ask about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. [JP 1-02, **DOD Dictionary of Military and Associated Terms**]

**IO** are actions taken to affect adversary information and information systems (INFOSYS) while defending one’s own information and information systems. [JP 3-13, **Joint Doctrine for Information Operations**]

**IO** are continuous military operations within the military information environment that enable, enhance, and protect the friendly force’s ability to collect, process, and act [up]on information to achieve an advantage across the full range of military operations; [IO] include interacting with the global information environment and exploiting or denying an adversary’s information and decision capabilities. [Draft FM 3-13, **Information Operations**]

**Information Security** is the protection and defense of information and INFOSYS against unauthorized access or modification of information whether in storage, processing, or transit, and against denial of services to authorized users. INFOSEC includes those measures necessary to detect, document, and counter such threats. Information security comprises computer security and communications security. [JP 3-13]

**Operations Security.** OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to a) Identify those actions observable by adversary intelligence systems. b) Determine indicators hostile intelligence systems might obtain with which they could interpret or piece together to derive critical information in time to be useful to adversaries. c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [JP 3-13]

Although the intuitive understanding of IO is solid, actually codifying the principles; doctrine; and tactics, techniques, and procedures of IO in modern venues—across the full spectrum of operations—is a daunting task. First, there is the matter of proponentcy: Since IO cuts across all echelons tactical through national, affects all services, and is both offensive and defensive in nature, who “owns” it? “Ownership” means responsibility for training, leader development, personnel management, and a host of other issues. Again, reach exceeds grasp. It is one thing to be aware of the issues, another to solve them.

Many of the articles in this issue of *MIPB* should provoke thought, and are not meant as a definitive statement of where the Army is heading; rather, these are the insights and suggestions from readers like you who feel they have an idea they should contribute for public debate. We thank you for your efforts in this vital and multifaceted debate.



CW3 Del E. Stewart  
Managing Editor



# MILITARY INTELLIGENCE

PB 34-03-3  
Volume 29 Number 3  
July-September 2003



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

## FEATURES

### STAFF:

#### Commanding General

Major General James A. Marks

#### Deputy Commandant for Futures

Jerry V. Proctor

#### Director of Training Development and Support

Colonel Jack W. Russell

#### Deputy Director, DTDS

Russell W. Watson, Ph.D.

#### Chief, Doctrine Division

Stephen B. Leeder

#### Managing Editor

Chief Warrant Officer Three  
Del E. Stewart

#### Editor

Elizabeth A. McGovern

#### Associate Editor

JoNell M. Elkins

#### Operations Supervisor

Captain Dean A. Phillips

#### Design Director

Specialist Ernesto A. Bolaños

#### Associate Design Director and Administration

Specialist Misty L. Simpkin

#### Cover Design:

Specialist Misty L. Simpkin

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

**Subscription:** Subscription rates are \$21.00 (Domestic, APO, and FPO) and \$29.40 (Foreign). For information on changes of address and subscriptions, see page 8.

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

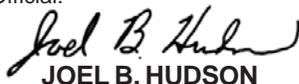
**Contact Information** for *MIPB* is on page 68.

- 5 **Visualizing the Information Environment**  
by Marc J. Romanych (Major, U.S. Army, Retired)
- 9 **Information Operations in Support of Demonstrations and Shows of Force**  
by Lieutenant Colonel Arthur N. Tulák
- 12 **Measures of Effectiveness in the Information Environment**  
by Lieutenant Colonel David C. Grohoski, Steven M. Seybert (Major, U.S. Army, Retired), and Marc J. Romanych (Major, U.S. Army, Retired)
- 17 **Reserve Support to IO: The 3431st MI Detachment (USAR) at NGIC**  
by Sherwin H. Terry, Jr.
- 19 **Intelligence Support to Information Operations: Staff Chaplains**  
by Major Norman Emery
- 22 **Like Adding Wings to a Tiger—Chinese Information War Theory and Practice**  
by Timothy L. Thomas
- 28 **Determining Battlefield Effects in an Urban Environment: MOUT Terrain Analysis**  
by Lieutenant Colonel Alfonso J. Ahuja
- 32 **The New Counterintelligence Response to the Cyberthreat**  
by Chief Warrant Officer Two Bobby Allen
- 36 **CI in Information Operations: Enabling Operators and Defining Emerging Roles for CI in Army IO**  
by Chief Warrant Officer Two Jason L. Morton
- 38 **Nonpassive Defense of the Army's Computer Networks**  
by Thomas G. King
- 40 **Intelligence in Support of Strategic Signal Units**  
by James R. Lint
- 43 **Bridging the Intelligence Gap in the Heartland: Evolving MI Roles in Support to Domestic Criminal Threats**  
by Major James Klotz and Lieutenant Colonel Michael French
- 47 **Get Your Soldiers Ready for Deployment**  
by Command Sergeant Major Lori L. Brown
- 49 **Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT)**  
by Captain Misty L. Martin
- 51 **CGS and Apache-Longbow Linkage—A 2d Infantry Division Initiative**  
by First Lieutenant Christine V. Fallon, Staff Sergeant Steven D. Jaime, and Sergeant Tony Donaldson
- 53 **Global War on Terrorism: Polygraph—An Intelligence Tool**  
by Chief Warrant Officer Three Joe Don Castleberry

## DEPARTMENTS

2	Vantage Point	65	111th Training Notes
3	CSM Forum	66	Distance Learning
56	Doctrine Corner	67	Professional Reader
61	Proponent Notes		Unit Profile: 310th MI Battalion
64	Sly Fox		

By order of the Secretary of the Army:  
Official:

  
JOEL B. HUDSON

Administrative Assistant to the  
Secretary of the Army

0314302

JOHN M. KEANE

General, United States Army  
Acting, Chief of Staff

# Always Out Front

by Brigadier General John M. Custer  
Commander, U.S. Army Intelligence Center and Fort Huachuca



## Intelligence Community Online Network—A Portal Into MI's Future

The U.S. Army Intelligence Center (USAIC) will deploy ICON, the Intelligence Community Online Network, in July 2003 as our newest effort to transform the Intelligence Center into a Digitized Center of Excellence for the Army. It will be a secure web portal for MI professionals worldwide to conduct collaboration, as well as an online workspace to conduct daily operations within USAIC. ICON will be MI's portal under Army Knowledge Online (AKO)—we envision ICON to be the daily center of business at the Intelligence Center and across the MI community. It will integrate many daily use processes and applications to include E-mail, web content, command reports, and connection to local databases, among other features. ICON will also have collaborative capabilities like chat rooms, message forums, and document sharing. ICON will provide MI professionals worldwide with a powerful tool to exchange ideas; tactics, techniques, and procedures (TTPs); and other mission-essential information. MI professionals should seek out ICON as the primary Branch and program proponent forum through which to gather information from USAIC and other organizations. It will be the "one-stop shop" for anything and everything MI.

USAIC designed the ICON portal to have single sign-on capability with AKO; this means that users can jump from the ICON portal into AKO and back again. After signing in to either portal, you will have access to both portals. This design will provide users a seamless online experience between all of the AKO options, mail capabilities, and a direct access to ICON applications. Our goal is not to duplicate AKO, but to complement its capabilities with ICON features tailored specifically for MI professionals.



ICON will look and feel like AKO but users may completely customize it to make the system user-friendly and ultimately to provide MI users with a better overall experience. The portal desktop will consist of smaller windows of information called "channels," each having a specific topic of information. On the portal, users' individual access levels will determine which channels will be available to them; users will also be able to choose among the channels and where they want them on their computers' desktops.

ICON will divide users into **roles** based on their duty status and locations. Examples of role titles include "Anonymous Guest," "USAIC Permanent Party," and "Registered Guest." Most MI users outside USAIC will log in as Registered Guest users—this will allow them to access most of the portal information and to conduct collaboration with other MI professionals. The portal will determine the privileges and level of access to information for each user based on his or her login-role.

ICON's initial implementation will be on the Nonclassi-

(see CG's Forum, continued on page 4)

# CSM Forum

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



This past March, we had to postpone our Worldwide Command Sergeants Major/Sergeants Major (CSM/SGM) Military Intelligence (MI) Conference. However, we still selected the 2003 CSM Doug Russell Awardee, Sergeant (SGT) Andrew C. Rapp—a counterintelligence (CI) special agent assigned to 3d Special Forces Group (Airborne)—as the Third Annual Doug Russell Award recipient. The Army's top Special Forces leaders as well as representatives from the military intelligence community attended the ceremony on 7 March 2003 at Headquarters, U.S. Army Special Operations Command, Fort Bragg, North Carolina. CSM (Retired) Sterling McCormick, our Honorary MI Corps CSM, presented SGT Rapp with the Knowlton Award during the ceremony. CSM (R) McCormick said,



*SGT Rapp is the perfect example of the type of soldier for whom the award committee was looking....To win, it takes a soldier who distinguishes himself within the Military Intelligence community but it also takes a soldier who has demonstrated professionalism in his or her military occupational specialty.*

Again, congratulations to SGT Rapp, the 2003 CSM Doug Russell Award recipient.

As we continue to fight the Global War on Terrorism ("GWOT") in Afghanistan and Iraq, our operations tempo (OPTEMPO) does not appear to be slowing down. I ask you all to try to find the time to think about next year's CSM/SGM conference. Please bring to the table those lessons learned from your formations involved with "GWOT." Your lessons learned will assist the schoolhouse in developing a better-trained intelligence professional. Again, if there are any briefings, issues, or speaking presentations you would like for next year's conference, please E-mail me at [lawrence.j.haubrich@us.army.mil](mailto:lawrence.j.haubrich@us.army.mil). Our conference's success will depend on what we, the

senior noncommissioned officers (NCOs) of our Military Intelligence Corps, want to accomplish.

In May, we were fortunate to have the 12th SMA, Sergeant Major of the Army Jack L. Tilley, visit Fort Huachuca. He spoke with initial entry training (IET) students attending the unmanned aerial vehicle (UAV) operator's course, human intelligence (HUMINT) collection course, and CI course, as well as the NCO Academy. SMA Tilley commented, "*The technology our Army has is what separates us from the rest of the world,*" ...and "*the information Military Intelligence gives us saves soldiers' lives on the battlefield.*" SMA Tilley also visited the Garrison, Health Clinic, and the U.S. Army Network Enterprise Technology Command/9th

Army Signal Command, where he expressed his appreciation for what all the soldiers do for the nation.

SMA Tilley shared with the soldiers some of his experiences from his recent trips to Baghdad and Walter Reed Army Medical Center. "*Since the war on terrorism began, we have had 150 plus soldiers killed and over 300 injured,*" SMA Tilley stated. "*We won't allow ourselves to forget what we stand for. What we stand for is to protect the Constitution of the United States.*" He talked about visiting the wounded soldiers who came back from Iraq—his strong emotions visible on his face—and he praised their commitment to the Army and the nation. Team Huachuca thanks the SMA for taking care of soldiers, his continuing mentorship, and for his visit to the U.S. Army Intelligence Center and Fort Huachuca.

During the past few months, I visited our great MI career and assignment managers at MI Branch, U.S. Total Army Personnel Command. I also traveled to Fort Bragg, and visited MI soldiers assigned to the 3d and 7th Special Forces Groups (Airborne), 525th MI Brigade (Airborne), and the 313th MI Battalion (Airborne), 82d Airborne Division; these units all have soldiers who had just recently returned from deployments and prepared to deploy in support of the worldwide war on terrorism. In Utah,

*(see CSM's Forum, continued on page 4)*

(CG's Forum, continued from page 2)

portal channels and will consider your ideas and add them into our plan for future expansion of ICON. The point of contact is Major Tito Martinez, Director, Digital Training Office; you may contact him via E-mail at [erasmo.martinez@hua.army.mil](mailto:erasmo.martinez@hua.army.mil) and by telephone (520) 533-0981, or DSN 821-0981).

In addition to developing the ICON, we have also published for the first time a "Commandant's Recommended Reading List" for MI professionals. I believe you will find it visionary with decidedly futuristic and

information-based orientations. The list includes readings for the Balkans and the Middle East as well as some old favorites borrowed from traditional military-theory reading lists. The vast majority of the books, however, are something quite new and different. They complement the tremendous changes we are witnessing in the way we view information and how it will continue to affect the future of military conflict. I challenge you to work through these readings, as I am sure they will change the way you view our world, our profession of arms, and the future of our Branch.

## ALWAYS OUT FRONT!

### U.S. Army Intelligence Center Commandant's Reading List for MI Professionals

**The Lexus and the Olive Tree: Understanding Globalization** by Thomas L. Friedman

**Unleashing the Killer App: Digital Strategies for Market Dominance** by Larry Downes, Chunka Mui, and Nicholas Negroponte

**In Athena's Camp: Preparing for Conflict in the Information Age** edited by John Arquilla and David F. Ronfeldt

**Stray Voltage: War in the Information Age** by Brigadier General (Retired) Wayne M. Hall

**The Age of Spiritual Machines: When Computers Exceed Human Intelligence** by Ray Kurzweil

**War and AntiWar: Survival at the Dawn of the 21st Century** by Alvin and Heidi Toffler

**Complexity: The Emerging Science at the Edge of Order and Chaos** by M. Mitchell Waldrop

**The Dancing Wu Li Masters: A Overview of the New Physics** by Gary Zukav

**Being Digital** by Nicholas Negroponte

**The Social Life of Information** by John Seely Brown and Paul Duguid

**Bridge on the Drina** by Ivo Andric, Lovett F. Edwards (Translator)

**Yugoslavia—Death of a Nation** by Laura Silber and Allen Little

**An Introduction to Islam** by Frederick M. Denny

**What Everyone Needs to Know About Islam** by John L. Esposito

**The Islamic Threat: Myth or Reality?** by John L. Esposito

**Unholy War: Terror in the Name of Islam** by John L. Esposito

**A Peace to End All Peace: The Fall of the Ottoman Empire and the Creation of the Modern Middle East** by David Fromkin

**The Reckoning: Iraq and the Legacy of Saddam Hussein** by Sandra MacKey

**On War** by Karl von Clausewitz

**The Art of War** by Sun Tzu, translated and with an introduction by Samuel B. Griffith

**The Transformation of War** by Martin Van Creveld

**The New Face of War: How War Will Be Fought in the 21st Century** by Bruce Berkowitz

(CSM's Forum, continued from page 3)

I visited the 300th MI Brigade, attended the language conference, and visited the Joint Language Training Center. At Fort Hood, Texas, I visited the 312th MI Battalion, 1st Cavalry Division, where many soldiers were on deployment orders to, or had just returned from, Iraq. The bottom line is that all of us are soldiers, we are warriors,

all doing our parts fighting this Global War on Terrorism no matter where we are. We are a nation at war, so stay focused, embrace each other, and do not become complacent.

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!

# Visualizing the Information Environment

by Marc J. Romanych  
(Major, U.S. Army, Retired)

*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 Departments of the Army and Defense, or the U.S. Government.*

Although the Army recognizes the existence of the information environment and its importance to armed conflict, there is little consensus as to its composition and character. Perhaps, because of its abstract nature, the information environment eludes definitive description. Regrettably, this lack of a common view hinders our understanding of this new operating environment and its potential effects on military operations, especially during operational planning when the information operations (IO) staff is attempting to visualize the information environment as part of the command's battlespace.

This article discusses the application of emerging information theory to the problem of describing the information environment's effects on military operations and proposes a way to apply intelligence preparation of the battlespace (IPB) to the problem of defining the information environment.

## What is the Information Environment?

Doctrine defines the "information environment" as "the aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is information itself."<sup>1</sup> Unfortunately, this definition focuses on the information environment as a physical entity composed of information systems. The very reason for the exist-

ence of the information environment, information, is often a mere afterthought, while we completely disregard decisionmaking (the ultimate target of IO). The result is a definition that neither presents a useful picture of the information environment nor expresses its true nature.

Fortunately, recent work by the Department of Defense (DOD) Command and Control Research Program (CCRP) provides a model of the information environment that battle staffs can use. CCRP's publication, **Understanding Information Age Warfare**, describes the battlespace as having three distinct, but related, domains—physical, information, and cognitive.<sup>2</sup> Together, these domains represent the nature of the information environment and are central to understanding the impact of information on military operations.<sup>3</sup> We can describe the domains as shown in Figure 1.<sup>4</sup>

The **physical domain** is the tangible world. It is the material part of the information environment that

overlaps with the physical operating environments of land, sea, air, and space. This domain is where military maneuver and combat operations occur. It is also where the physical elements of information systems and the networks that connect these systems reside and operate.<sup>5</sup> Essential characteristics of the physical domain include those typically important to maneuver operations: geography (terrain), weather, populace, and civil infrastructure (to include communications networks and media). These characteristics affect the employment of information system assets and the linking of information systems into networks. For IO, this is the domain in which we attack and defend information systems.

The **information domain** is where information exists. It is an abstract construct based upon theory.<sup>6</sup> The information domain has a dual nature, consisting of information itself but also serving as the medium

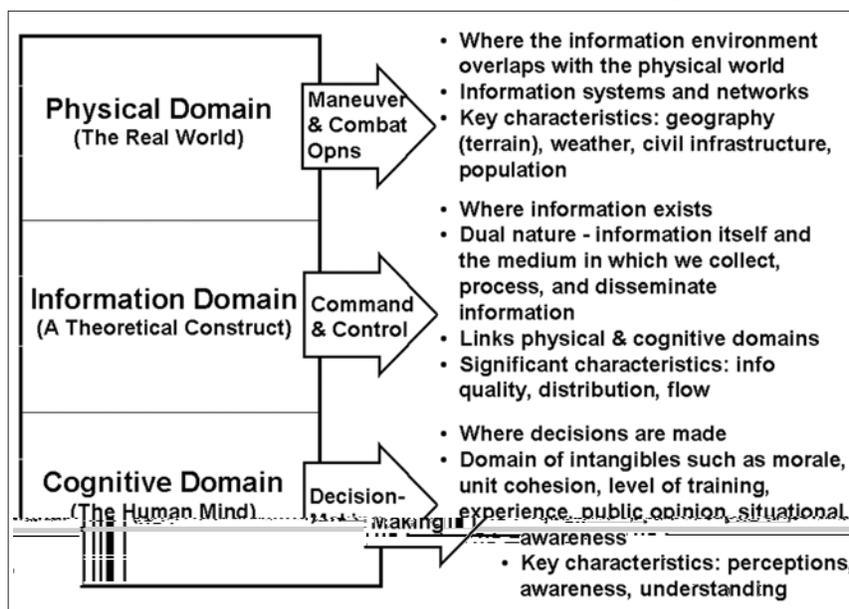


Figure 1. Information Environment Construct.

Domain	Significant Characteristics	Effects on Operations
Physical	Geography – Info environment compartmentalized by mountains	Info infrastructure concentrated in urban areas and along roads
	Info Infrastructure: •Telecom system—Used by military •Media – Govt controlled, reaches 90% of populace	•Primary means of C2 •Collateral damage concerns •Populace’s primary info source
	Demographics – >70% of populace concentrated in urban areas	Populace can hinder or tie down military forces
Information	•Info flow – follows ground LOCs •Media – content is anticoalition propaganda	•Info flow easily interdicted •Local media has influence on populace perceptions
Cognitive	Divide populace support for government regime	•Can influence populace to support or oppose military operations
Key: Govt – Government Info – Information LOCs – Lines of communication Telecom – Telecommunications		

Figure 2. Example Info Environment Effects.

by which we collect, process, and disseminate information (i.e., the functions of information systems). Conceptually, the information domain fits between the physical and cognitive domains or, perhaps more accurately, at the intersection of the two domains.<sup>7</sup> As such, the information domain links the reality of the physical domain to the human consciousness of the cognitive domain. Crucial characteristics of the information domain include those essential to information management and command and control (C2): information quality (completeness, accuracy, timeliness, relevance, and consistency), distribution (range, sharing, and continuity), and interaction (exchange or flow of information).<sup>8</sup> These characteristics affect information content and the functions of information systems. In this domain, IO seeks to affect the content and flow of information.

The **cognitive domain** is also abstract. However, unlike the information domain, which is purely theoretical, the cognitive domain exists in the minds of human beings and in the collective consciousness of groups and organizations.

This domain includes intangibles such as morale, unit cohesion, level of training, experience, public opinion, and situational awareness.<sup>9</sup> Most importantly, the cognitive domain is where we make decisions. Therefore, vital characteristics of this domain are those that affect individual and collective (organizational) decisionmaking: perceptions (attitudes), awareness (opinions, beliefs, and values), and understanding (knowledge). In the cognitive domain, IO seeks to affect the interpretation and use of information to make decisions.

### The Relationship of the Domains

Together, the three domains comprise the information environment. As previously noted, the physical domain is where information systems and networks reside and operate. The employment of these systems and networks in the physical domain influences the collection, processing, and dissemination of information in the information domain, which in turn affects human decisionmaking in the cognitive domain. As a result, effects in one domain generate consequent effects in the other domains.

To conduct IO, our view of the information environment must extend from the physical domain through the information domain into the cognitive domain. To affect the cognitive domain (the ultimate objective of IO), effects must first occur in the physical and then the information domains. Thus, staffs cannot base planning solely on the characteristics of friendly and adversary information systems (i.e., the physical domain); rather, it must include the desired higher order of effects in the information (information content and flow) and cognitive (decisionmaking) domains.<sup>10</sup> For this reason, when conducting IPB, it is necessary to analyze and visualize all three domains and their interrelationships.

### Applying Theory—The Combined Information Overlay

The information environment, in contrast to the other environments in which armed forces operate—land, sea, air, and space—is largely nonphysical and abstract. As a result, battle staffs often have difficulty expressing the information environment’s character and effects in a manner useful to the commander. One possible solution is a “combined information overlay” (CIO). Analogous to the modified combined obstacle overlay (MCOO) produced by the intelligence staff to portray the battlespace’s effects on military operations, the CIO is a graphic product that depicts the information environment’s effects.

The IO staff derives the CIO from analysis conducted during the first two steps of IPB: *Define the Battlefield Environment* and *Describe the Battlefield’s Effects*. To construct a CIO, first examine the battlespace to identify significant characteristics of each information environment domain (Step 1 of

IPB).<sup>11</sup> Such an analysis is comparable to the G2's evaluating the battlefield in terms of OAKOC (obstacles, avenues of approach, key terrain, observation and fields of fire, and concealment and cover). The difference is that this analysis attempts to "map" the battlefield's information environment based upon the generic characteristics of the information environment model:

- ❑ **Physical Domain:** What aspects of the geography (terrain), weather, populace, and the civil infrastructure impact on the employment of information systems and the linking of information systems into networks?
- ❑ **Information Domain:** What information and its quality, flow, and distribution affect information system functions (i.e., collection, processing, and dissemination of information)?
- ❑ **Cognitive Domain:** What populace and third-party perceptions, awareness, and understanding influence decisionmaking?

The next step is to analyze the identified significant characteristics in detail to determine the effects on military operations (Step 2 of IPB) (see Figure 2). Then the staff combines the domain's individual characteristics and effects to develop an aggregate view of the information environment. They plot the result on a map of the area of operations to depict where and how the information environment's effects will influence military operations.

Keep in mind that the CIO is a guide, not a rigid template. Because the information environment is not uniform in its composition and character, every CIO will be unique. Significant characteristics can vary widely depending on the assigned operational area, the type of military operation, and mission. Therefore, few analyzed information environments will incorporate all elements

of the template. However, whatever form the CIO takes, the product must show the aggregate effects of all three domains on military operations (see Figure 3). Some considerations for developing CIOs include—

- ❑ The CIO is an overview of the information environment. The degree of detail displayed varies depending on the type of operation, capabilities of the friendly and threat forces, and the relative significance of the information environment to the mission. Typically, analysis of the information environment results in a series of templates—based on the time available, perhaps one for each significant characteristic—that support the conclusions of the CIO and provide the details needed to plan the IO.
- ❑ When plotting significant characteristics of the information environment, it is possible that the battlespace will contain distinct "sub-information" environments. These environments are geographic areas in which the significant characteristics are notably different from those in adjacent areas. IO staffs may have to analyze subenviron-

ments separately to determine their composition and character.

- ❑ Inclusion of an entire information infrastructure on the CIO may be impractical; in which case, it should at least comprise key information nodes.

## Conclusion

As an operating environment for military forces, the information environment is difficult to visualize. It is complex, abstract, and ever changing. The CCRP's theoretical work and its application as discussed in this article only scratches the surface of what is necessary for battle staffs to characterize the information environment accurately. As our understanding of the nature of the information environment increases, changes in doctrine and tactics, techniques, and procedures (TTPs) are sure to follow. However, to start this process of change, we must first develop a common understanding of the information environment.



## Endnotes

1. Joint Publication 1-02, Department of Defense Dictionary of

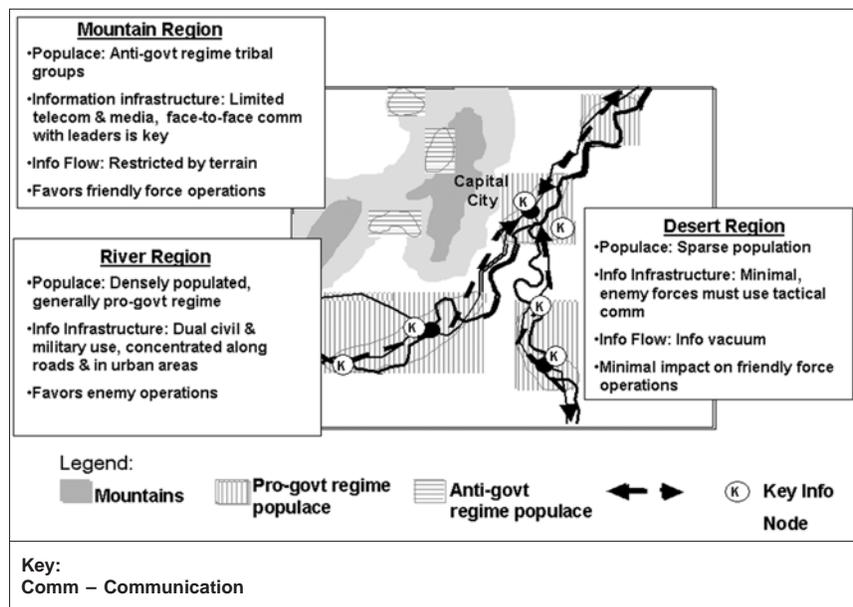


Figure 3. Example of a CIO.

**Military and Associated Terms** (Washington, D.C.: U.S. Government Printing Office, 12 April 2001), page 203.

2. Alberts, David S., Gartska, John J., Hayes, Richard E., Signori, David A., **Understanding Information Age Warfare** (Washington D.C.: DOD Command and Control Research Program, August 2001.) This book examines the information environment in a way that is very useful to IO. Anyone seeking to understand the relationship between information and information superiority is encouraged to read this work.

3. Ibid, page 10.

4. For another, albeit similar model of the information environment, see **Toward a Functional Model of Information Warfare** by L. Scott Johnson (*Studies in Intelligence*, Volume 1, Number 1, 1997). Although somewhat dated as well as technology-centric, it complements Under-

**standing Information Age Warfare** well.

5. Ibid. page 12.

6. There are two generally accepted theories of information. First—information as message (or meaning)—regards information as an immaterial message or signal that contains meaningful (or at least recognizable) content that a sender can transmit to a receiver. Second—information as medium—relates information to the message but also views information as a system or conduit that transmits a message from sender to receiver. See Arquilla, John, and Ronfeldt, David, **In Athena's Camp: Preparing for Conflict in the Information Age** (Santa Monica, CA: RAND, 1997), pages 145-152.

7. Sparling, Bryan, **Information Theory as a Foundation for Military Operations in the 21st Century** (Fort Leavenworth, KS: School of Advanced Military Studies, U.S. Army

Command and General Staff College, AY 01-02, 14 May 2002).

8. Alberts, et al, page 78.

9. Ibid, page 13.

10. Johnson, ID at 4.

11. Significant characteristics are those aspects of the battlespace that may influence military operations.

*Marc Romanych (Major, U.S. Army, Retired) works as a contractor with the U.S. Army 1st Information Operations Command (Land). Since 1998, he has deployed with IO field support teams to Bosnia and Kosovo, and numerous joint and Army warfighter exercises. Mr. Romanych teaches courses on information operations and information superiority for the American Military University. He holds degrees in Chemistry, Geology, History, and International Relations. Readers may contact him via E-mail at marc.romanych@us.army.mil.*



Order Processing Code \*6489

# MIPB Subscription

Subscription Order Form



Please send the subscription for \_\_\_\_\_ years to **Military Intelligence Professional Bulletin (MIPB)**. \$21.00 (Domestic, APO, and FPO); \$29.40 (Foreign) per year. You can E-mail us at [misty.simpkin@us.army.mil](mailto:misty.simpkin@us.army.mil) or [ernesto.alonso.bolanos@us.army.mil](mailto:ernesto.alonso.bolanos@us.army.mil).

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

**Address**

\_\_\_\_\_  
(Company or Personal Name)

\_\_\_\_\_  
(Street Address)

\_\_\_\_\_  
(Additional Address/Attention Line)

\_\_\_\_\_  
(City, State, ZIP Code)

**Please choose method of payment:**

Check payable to the **Superintendent of Documents**

GPO Deposit Account No. \_\_\_\_\_

MasterCard  VISA  Discover

\_\_\_\_\_  
(E-mail Address and Telephone Number)      \_\_\_\_\_  
Expiration Date

**Please include your E-mail address to confirm Receipt of payment.**      \_\_\_\_\_  
Authorization Signature

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

# Information Operations in Support of Demonstrations and Shows of Force

by Lieutenant Colonel  
Arthur N. Tulák

*A version of this article by then Major Tulák previously appeared in the Center for Army Lessons Learned (CALL) Training Techniques, 2nd Quarter, Fiscal Year 2003 (TQ2-03) at <http://call.army.mil/products/trngqtr/tq2-99/showforc.htm>. Reprinted with permission.*

The U.S. Army conducts shows of force and demonstration operations to influence key decisionmakers and audiences to support U.S. objectives. Information operations (IO) leverage the effectiveness of these operations across the pillars of IO by informing targeted audiences of friendly force capabilities and intent. Shows of force and demonstrations are military operations conducted by combat forces to protect U.S. and allied interests, give warning and pause to hostile groups, persuade neutrals, and encourage friendly groups.<sup>1</sup> Shows of force and demonstrations are military activities that support preventive diplomacy,<sup>2</sup> one of the three diplomatic-led activities of peace operations in which military activities play a supporting role.<sup>3</sup>

The North Atlantic Treaty Organization (NATO)-led Stabilization Force (SFOR) conducting peace operations in the former Republic of Yugoslavia (FRY) conducted a show of force 25 March to 17 April 1998 to demonstrate SFOR's rapid reinforcement capability. Military activities appropriate for shows of force and demonstrations in support of peacekeeping and peace enforcement include multinational training exercises demonstrating coalition military capabilities, interoperability, unity of effort, and resolve.<sup>4</sup>

The show of force exercise, dubbed Dynamic Response (DR) '98, com-

menced with an amphibious landing at Ploce on the Croatian coastline on 26 March 1998.<sup>5</sup> The culmination exercise of DR '98 was a combined arms live-fire exercise (CALFEX) demonstration called Dynamic Strike '98, held at the Glamoc firing range in Multinational Division-Southwest (MND-SW). Both the show of force and its concluding demonstration were intended to show to the people of FRY and their military and political decisionmakers the SFOR's ability to insert additional combat forces into the theater rapidly to reinforce SFOR.

As SFOR reduced its on-the-ground force structure in Bosnia-Herzegovina, the requirement for a reliable rapid-response capability took on increased importance. SFOR needed to retain the capability of responding to a renewal of hostilities or increased tensions in order to maintain the peace imposed upon the former warring factions (FWFs) during the initial peace-enforcement operations conducted in Operation JOINT ENDEAVOR. The creation of a European-based Strategic Reaction Force (SRF) for the Bosnia arena allowed SFOR to continue on-the-ground force reductions without compromising its credibility to enforce the military provisions of the Dayton Peace Accord through lethal combat power. This force, while not based in theater, had the mission of serving as both a deterrent to renewing hostilities and a viable reinforcement option to support one or more SFOR sectors in a period of heightened tension. The purpose of the show of force and demonstration was both to demonstrate visibly that despite reductions of on-the-ground forces, SFOR still had the capability to respond to escalation and remained committed to enforcing the peace, and to train the SRF to execute tasks

associated with rapidly reinforcing a deployed peace-operations force.

---

**IO can enhance the impact of informational, diplomatic, economic, and military efforts, and forestall or eliminate the need to employ forces in a combat or crisis situation**

---

IO provide the U.S. Government with the capability to influence the perceptions and decisionmaking of the FWFs while improving the deterrent value of power-projection options.<sup>6</sup> Political concerns dominate shows of force and demonstrations, as the objective is to dissuade adversaries from interfering with the enforcement of international law, United Nations Security Council Resolutions (UNSCRs), and internationally recognized peace accords.<sup>7</sup> At the operational level, IO employed in conjunction with shows of force and demonstrations supports deterrence of the resumption of hostilities and reassures allies and the international community that the peace-operations force remains capable of implementing the peace agreement. In peace-enforcement operations, maintaining security involves demonstrations of inherent military capability and preparedness, and the overt presence of uncommitted mobile combat power in the form of a reserve.<sup>8</sup>

SFOR leveraged the deterrent effects of DR '98 by incorporating IO with the lethal combat power components into a fluid exercise that was extremely successful in showing its

resolve in maintaining unbroken enforcement of the Dayton Peace Accord. Used in this manner, IO can enhance the impact of informational, diplomatic, economic, and military efforts, and forestall or eliminate the need to employ forces in a combat or crisis situation.<sup>9</sup> Demonstrations and shows of force, supported by effective information operations, can deter adversaries from interfering with the peace-operations force or its objectives or from resuming the hostilities with the other FWFs.<sup>10</sup> The objective is to demonstrate resolve and commitment to a peaceful resolution while underlying the readiness and ability to use force if required.<sup>11</sup>

An effective show of force or demonstration must be demonstrably mission-capable and sustainable.<sup>12</sup> That is, the execution of the show of force or demonstration must convincingly demonstrate to the targeted audience that the peace-operations force has the necessary combat power; command, control, and communications (C3); intelligence; international liaison; and ready and responsive forces required to use military force to enforce compliance. The SFOR SRF in DR '98 included military forces from four NATO countries (Italy, The Netherlands, Turkey, and the United States) and two NATO Partnership for Peace (PFP) nations (Poland and Romania). The SFOR planned for an SRF of more than 5,000 soldiers comprised of a wide range of military capabilities to include light, airborne, and mechanized infantry, as well as armor, artillery, and both fixed- and rotary-wing attack aircraft.<sup>13</sup> Peace-operations doctrine notes that armored forces and attack helicopter assets can play major roles in deterrence or function as a mobile reserve.<sup>14</sup>

The DR '98 show of force took the form of a training exercise in which the SRF practiced combat operations such as amphibious assault; air assault; fire and maneuver; and such peacekeeping tasks as oper-

ating checkpoints, patrolling, and inspecting weapons storage sites. During the exercise, the participating forces became familiar with the area of operations and command and control procedures among the participating nations of the SRF and of SFOR.<sup>15</sup> The culmination point of the exercise was the CALFEX demonstration conducted in front of an audience of major political and military leaders of the FWFs. The message that SFOR wanted to send was that although they would lessen the military force structure in the future, they still had the capability and means to deploy a potent military force in the event of heightened tensions.

The Public Affairs (PA) component of IO was the primary vehicle to inform the regional and international media covering the events. The Deputy Commander Supreme Allied Commander-Europe (SACEUR) aboard the USS Wasp in the Adriatic at the commencement of the exercise himself held press conferences at the culminating CALFEX demonstration at the Glamoc firing range. The SFOR Coalition Press Information Center (CPIC), essentially a Joint and Multinational Information Bureau, provided a steady stream of press releases before, during, and after the exercise. CPIC press kits on the exercise ensured that the regional and international media knew the SACEUR's intent. It is essential that the commander's intent for the military operation be clearly communicated and correctly interpreted by potential adversaries.<sup>16</sup> As open sources to foreign countries and the United States, the Army can use PA channels to disseminate international information.<sup>17</sup>

Dynamic Strike, the culminating CALFEX demonstration of Exercise Dynamic Response '98, featured a force-projection scenario of a multinational SRF encountering a hostile force about to attack a village situated on the Barbara Range at Glamoc. During the demonstration,

the SRF responded to the hostile force with organic weapons, supported by 81-millimeter (mm) mortar fires; Cobra gunships from the 26th Marine Expeditionary Unit (MEU), and Apaches from the Task Force Eagle 4th Aviation Brigade fired on "adversary" armored personnel carriers. U.S. and Italian Marines conducted amphibious assault and helicopter air assault operations onto the coast. A reinforcing multinational ground force, composed of mechanized and armored forces, linked up with the amphibious and air assault forces. During the demonstration, the SRF maintained an impressive rate and volume of fire from 120-mm tank guns, automatic weapons and cannon fire, TOW and MILAN<sup>18</sup> missiles, and mortar and artillery fire. In the last wave of the onslaught, attack helicopters eliminated remaining targets, while NATO air assets, including Harriers from the USS Wasp, Jaguars, and F-16s, were ready to intervene and deliver 2,000-pound bombs on target if necessary.<sup>19</sup>

General Wesley Clark (SACEUR) declared at a press conference following the live-fire demonstration,

*Maintaining a strategic reserve force outside the region that is ready to respond quickly to any crisis, and help restore stability, is important to SFOR's ability to maintain peace throughout the region.*<sup>20</sup>

He further added,

*An action is worth a thousand words. By demonstrating its capabilities, SFOR nations have made a very powerful judgement, peace will be kept, the Dayton Peace Agreement implemented, and Bosnia and Herzegovina will become a normal country in Europe.*<sup>21</sup>

The opening amphibious landing and air assault operations of Exercise Dynamic Response attracted large press attention from local, regional, and international media.<sup>22</sup>

That interest was cultivated with a well-organized and rehearsed “Media Day” on 24 March 1998 at the commencement of the Exercise.<sup>23</sup> That media interest subsequently continued throughout the Exercise by ensuring media awareness of and access to exercise events and through the use of press releases given to the press and posted on the Internet.<sup>24</sup> The SFOR CPIC, the Supreme Headquarters Allied Powers Europe (SHAPE) Public Information Office, the U.S. Forces Press Service, and the United States European Command (EUCOM) all provided press releases documenting the preparation and execution of the show of force and its culminating fire-power demonstration.

The show of force exercise with the culminating CALFEX demonstration and the attendant local, national, and international media coverage had a profound impact on the FWF political and military leadership. According to the unit after-action reviews (AARs) and interviews conducted by the SFOR Public Information Office with prominent FWF military and political leaders, those FWF leaders in attendance, and those watching the event through the media, received the intended message loud and clear.



#### Endnotes

1. **FM 100-20, Military Operations in Low-Intensity Conflict** (Washington, D.C.: Headquarters, Department of the Army, 5 December 1990), page 1-11.
2. **FM 100-23, Peace Operations** (Washington, D.C.: Headquarters, Department of the Army, 30 December 1994), page 2.
3. *Ibid.*, pages 2, 111.
4. **FM 100-7, Decisive Force: The Army in Theater Operations** (Washington, D.C.: Headquarters, Department of the Army, 31 May 1995), page 8-9.
5. SFOR Coalition Press Information Center, Press Release “Exercise Dynamic Response 98—Images From Deployment,” Sarajevo, 26 March 1998, downloaded from <http://www.nato.int/sfor/dyn-resp/p980326n.htm>.
6. **FM 100-6, Information Operations** (Washington, D.C.: Headquarters, Department of the Army, 27 August 1996), page 2-2.
7. **FM 100-20**, page 5-4.
8. **FM 100-23**, page 17.
9. Office of the Chairman of the Joint Chiefs of Staff, **Joint Publication 3-13, Joint Doctrine for Information Operations**, Preliminary Coordination Draft, 28 January 1998, pages I-2 and I-3.
10. **FM 100-23**, page 17.
11. *Ibid.*, page 2.
12. **FM 100-20**, page 5-4.
13. Coalition Press Information Center, Sarajevo, 23 March 1998, Press Release “Operation Joint Guard, Exercise Dynamic Response 98,” downloaded from <http://www.nato.int/sfor/dyn-resp/dyn-resp.htm>.
14. **FM 100-23**, page 40.
15. Kozaryn, Linda D., American Forces Press Service, Department of Defense, Press Release 98167, “NATO Strategic Reserve to Train in Bosnia,” American Forces Press Service downloaded from <http://www.dtic.mil/afps/news/9803243.htm>.
16. Air Command and Staff College Research Project 95-053, “Planning and Executing Conflict Termination,” Chapter 3, Case Study Analysis (Maxwell Air Force Base, AL: ACSC, 1995), page 9.
17. **Joint Publication 3-53, Joint Doctrine for Psychological Operations** (Washington, D.C.: Chairman of the Joint Chiefs of Staff, 10 July 1996), page vi.
18. The expansion of TOW is tube-launched, optically tracked, wire-guided and MILAN is Missile d’Infanterie Leger Antichar.
19. Arnold, 2LT David, “Dynamic Strike 98 Opens Fire,” Coalition Press Information Center, Sarajevo, 3 April 1998, downloaded from <http://www.nato.int/sfor/dyn-resp/p980403a.htm>.
20. Supreme Headquarters Allied Powers Europe, News Release 98-09-02, “INITIAL EXERCISE PRESS RELEASE Exercise Dynamic Response 98,” 9 February 1998, downloaded from: <http://www.shape.nato.int/Press/980902.htm>.
21. Arnold, ID at 19.
22. Coalition Press Information Center, Sarajevo, 25 March 1998, Press Release “Strategic Reserve Force Arrives For Exercise Dynamic Response 98,” downloaded from <http://www.nato.int/sfor/dyn-resp/p980325a.htm>.
23. Coalition Press Information Center, Sarajevo, 24 March 1998, Press Release “Operation Joint Guard, Exercise Dynamic Response 98—Media Day,” downloaded from <http://www.nato.int/sfor/dyn-resp/p980324a.htm>.
24. SFOR CPIC press releases included instructions to journalists on coordination of air and ground transportation (provided by SFOR) to the exercise events and offered assistance to journalists wanting to cover the scheduled events. The SFOR CPIC press kit issued in advance of the exercise laid out the entire exercise plans for journalists to plan their coverage.

*Lieutenant Colonel Arthur Tulák is currently serving at the J39 Information Operations Cell at U.S. Army Pacific Command (PACOM) Headquarters at Camp Smith, Hawaii. His previous assignment was as the Division Information Operations Officer for the 82d Airborne Division in Bagram, Afghanistan, as part of a 1st Information Operations (Land) Command Field Support Team supporting Operation ENDURING FREEDOM. LTC Tulák served in the IO Cells of the 1st Infantry Division and 1st Cavalry Division in Operations JOINT GUARD and JOINT FORGE in Bosnia-Herzegovina. His Infantry assignments include tours with the 87th, 8th, 27th, and 29th Infantry Regiments. LTC Tulák earned a Bachelor of Science degree in Business Administration with an emphasis in Marketing from the University of Southern California at Los Angeles; a Master of Science degree in Defense and Strategic Studies from Southwest Missouri State University, Springfield Missouri; and a Master of Military Arts and Sciences from the U.S. Army Command and General Staff College in General Studies with an emphasis on Information Operations in 1999. Readers may contact the author telephonically at DSN 305-477-3110.*

### Have You Moved Recently?

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

# Measures of Effectiveness in the Information Environment

by Lieutenant Colonel David C. Grohoski, Steven M. Seybert (Major, U.S. Army, Retired), and Marc J. Romanych (Major, U.S. Army, Retired)

Assessing the effectiveness of an information operation is one of the greatest challenges facing a staff. Despite the evolution of information operations (IO) doctrine and the refinement of supporting tactics, techniques, and procedures (TTPs), the Army has not solved the problem of IO assessment methodology. The question remains: lacking physical evidence, how can we quantify the intangible attributes of the information environment to assess the effectiveness of IO?

This article addresses the matter of quantifying the effectiveness of IO. Then it presents a methodology for developing measures of effectiveness (MOEs) to ascertain IO effects on friendly and enemy forces.

## Statement of the Problem

Why is assessing the impact of IO so difficult? First, the information environment is an abstract construct, and IO operates within that construct. According to *Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms*, the “information environment” is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information. Also included in the information environment is information itself. Thus, the information environment is a combination of physical assets (e.g., information systems) and nonphysical concepts (e.g., information, information-based processes, and human decisionmaking processes). IO attacks and protects the physical assets of information

systems to affect the nonphysical aspects of the information environment. Transitioning from visible effects resulting from destruction of tangible assets such as command posts (CPs) and radar systems to abstract effects such as disrupted information flow and degraded decisionmaking is a challenging task.

Second, not all of IO’s capabilities reside in the physical world. While physical destruction is tangible enough, many capabilities include nonphysical aspects—operations security (OPSEC), electronic warfare (EW), military deception, psychological operations (PSYOPs), etc. For IO purposes, the effects ultimately produced by these elements should occur in the intangible domain of ideas, perceptions, and attitudes. Capturing data or information to measure such nonphysical effects is difficult and often time-consuming, requiring a depth of analysis that seems impossible during high-tempo operations.

Third, an integrated IO campaign achieves a complex, tiered hierarchy

of effects (see Figure 1). The attack on or protection of physical assets (information systems) yields what one can call “**first-order effects**,” such as the destruction, degradation, and disruption of enemy signal nodes and CPs, or perhaps the presentation of false observables for collection by enemy intelligence systems. We direct these first-order activities against the enemy’s information system to achieve **second-order effects** on the enemy’s information and information-based processes, which in turn, seek a **third-order effect** on the enemy commander’s decisionmaking (i.e., the ultimate target of IO). Defensively, first-order effects may be the protection of friendly force information system assets; second-order effects may be the maintenance of situational awareness or an uninterrupted information flow; and third-order effects may be the preservation of effective decisionmaking. Each level of effects will likely yield corresponding enemy and friendly reactions, resulting in a complex, tiered set of causes and effects, which require interpretation to determine the

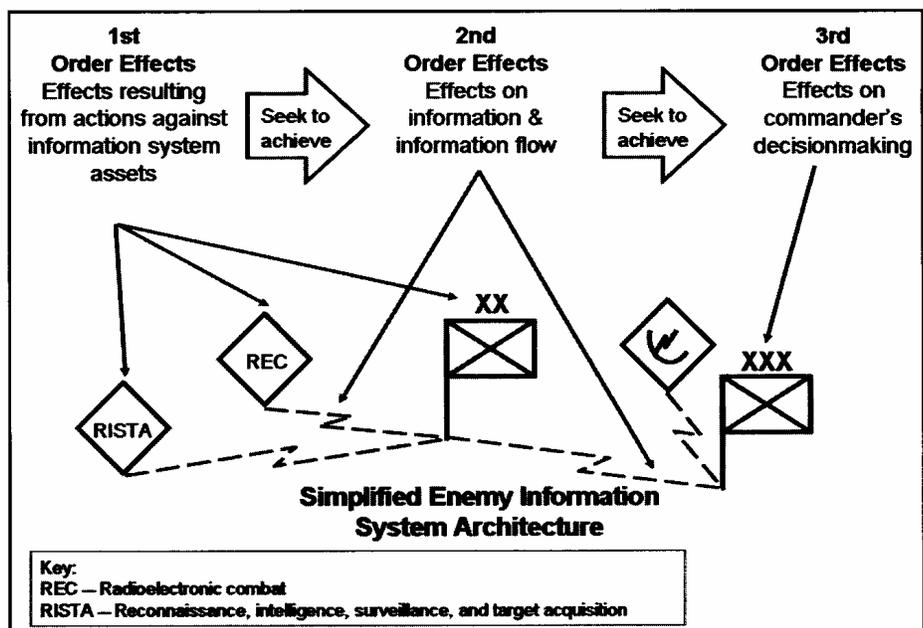


Figure 1. IO Effects Hierarchy.

overall impact of the IO. This maze of causal relationships requires something more than traditional battle damage assessment (BDA).

## Assessment and the Hierarchy of Effects

Measurement and analysis of effects resulting from the attack of enemy information systems and protection of friendly information systems make an IO campaign assessment possible. However, to do this, it is necessary to understand the hierarchy of effects resulting from IO activities (e.g., first-, second-, and third-order effects).

First-order effects result from those actions directed against the enemy's information system and those measures taken to protect the friendly information system. Generally, one deduces first-order effects by using information derived from unit reporting and BDA.<sup>1</sup> This assessment determines if planned IO tasks have occurred, and the direct result of these actions and activities. Generation of second- and third-order effects are by the aggregate of actions directed against enemy and friendly information systems. These effects are subtle and less quantifiable than first-order effects. At these levels, assessment seeks to determine if the aggregate of executed IO tasks have achieved the desired result:

- ❑ What were the effects on the enemy and friendly information systems (second-order effects)?
- ❑ Were the enemy and friendly commanders affected (third-order effects), and if so, how and to what extent?

Determination of second- and third-order effects is usually through inductive analysis of intelligence reporting and assessments.

## Establishing Cause and Effect

The only way to assess cause-and-effect linkages is to acknowledge—

- ❑ Military conflict consists of interactions among humans and technologies.
- ❑ Linkage of physical assets of a military force and the intangible aspects of military operations, such as morale, leadership, will, and cohesion.

Thus, attacking physical assets—CPs, target acquisition systems, intelligence collection and processing systems, and communications systems—will adversely impact a military force's ability to make and act upon decisions and consequently will have a detrimental affect on those intangibles that provide the military force with the ability to conduct operations.

Correlation exists when the value of an action (e.g., number of occurrences, degree of the effect, etc.) increases (or decreases) while the value of the effect also increases (or decreases). For example, if as the number of PSYOP leaflets dropped on enemy formations increases so do the number of enemy soldiers surrendering, or if as the number of jamming attacks against a command and control (C2) net increases, the traffic on that net decreases, then a probable correlation exists. This deductive reasoning forms the basis of determining first-order effects.

However, the apparent relationship between action (cause) and effects may be coincidental because the occurrence of an effect is accidental, or perhaps caused by the correlation of multiple actions executed to achieve the effect. For example, if friendly forces are successfully engaging enemy formations with fires and maneuver at the same time PSYOP activities are urging enemy soldiers to surrender, then correlating an increase in surrendering soldiers to PSYOP activities alone may not be possible. Furthermore, because an IO will often employ multiple elements to engage the enemy's information system, the cumulative effect of IO

support to friendly combat actions may make the impact of individual IO activities indistinguishable. Since there will rarely be enough time to rule out definitively coincidental relationships, the only possible antidote is an in-depth knowledge of the enemy and information environment that facilitates the development of an informed estimate through inductive reasoning.

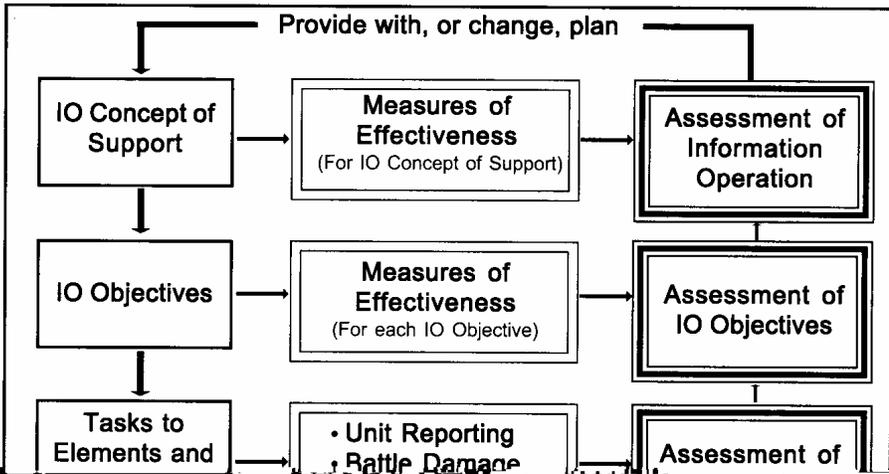
## What Are Measures of Effectiveness?

Unfortunately, the emerging joint definition of "MOEs" (e.g., tools used to measure results achieved in the overall mission and execution of assigned tasks<sup>2</sup>) provides little clarity as to what MOEs and how we can MOEs or them to assess IO. Therefore, for this discussion, we propose the following definition: measures of effectiveness are standards of reference used as the basis of comparison to evaluate the success or progress of an operation.

MOEs are a means to determine second and third-order effects by establishing a cause-and-effect linkage between the usually observable and quantifiable first-order effects and the abstract and subjective second- and third-order effects. MOEs do not constitute the assessment itself but are an evaluation means to determine if the individual IO tasks are achieving the IO objectives and whether accomplishment of the IO objectives is fulfilling the concept of IO support (see Figure 2).<sup>3</sup>

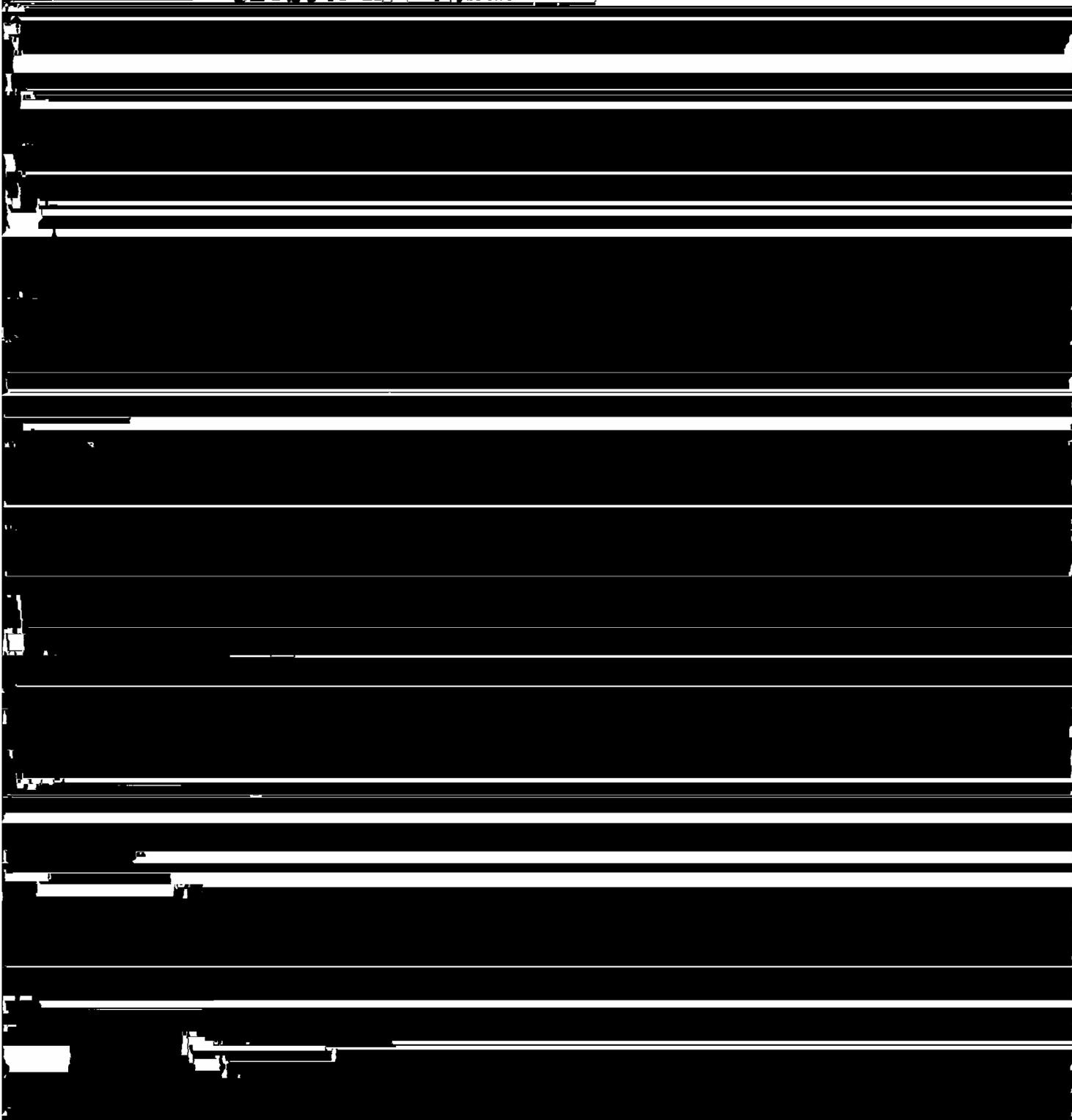
## Developing MOEs

The staff develops MOEs as part of the planning process to determine the effects of both offensive and defensive IO. To be meaningful, MOEs must link friendly and enemy actions and activities (cause) to enemy and friendly capabilities to make and act upon decisions (effect).<sup>4</sup> Therefore, MOE development begins with the IO mission statement and objectives.



- No reserve divisions committed against II Corps' main effort.
- No blockage of II Corps' main supply routes by the civilian populace.
- No instances of local leaders inciting the populace to interfere with II Corps' operations.

MOEs for third-order effects seek to determine if we affected the enemy and friendly commanders as planned. These MOEs should determine if the decisionmaker has



IO Objective	1st Order MOE (BDA)	2nd Order MOE	3rd Order MOE
Disrupt Northland 1st Army commander's synchronization of corps- and army-level operations	<ul style="list-style-type: none"> <li>• Destruction of corps &amp; army headquarters</li> <li>• Destroyed or captured reconnaissance teams</li> <li>• Decreased corps-level and above C2 communications traffic</li> <li>• Increased division C2 net communications traffic</li> </ul>	<ul style="list-style-type: none"> <li>• No synchronized fires and maneuver above division level</li> <li>• No reserve divisions committed against II Corps' main effort</li> </ul>	No counterattack by the Northland 1st Army against II Corps' main effort

Figure 3. Example IO Objective and MOE.

nate units report much of this information to their higher headquarters. Maneuver units, tactical PSYOPs teams, and civil affairs tactical support teams, as well as tactical human intelligence (HUMINT) teams (which traditionally include counter-intelligence personnel), and other intelligence collection assets all provide information with which to gauge IO success. Additionally, on-going intelligence analysis, including analysis of media and other open sources, supports assessing whether an IO campaign is achieving its objectives and if the IO concept of support is successful.

To receive information, the IO staff must actively monitor the operational situation and aggressively pursue information through unit reports and debriefings, IO working group (IOWG) meetings, and other venues. Commanders' battle update briefings, conference calls, and other meetings also facilitate monitoring IO execution by providing forums from which to receive information for subsequent analysis. Some other actions the IO staff can do include—

- ❑ Submit requests for information (RFIs) based upon the assessment plan.
- ❑ Develop IO input to the commander's critical information requirements (CCIRs).
- ❑ Coordinate with the deep operations coordination cell (DOCC)

and targeting board for BDA reporting.

- ❑ Review assessments at each IOWG meeting.
- ❑ Monitor G2 and G3 incident databases and analyze trends.

Ultimately, an assessment is successful when it is possible to decide when to proceed with the plan, when to reengage a target, when to execute a branch of the plan, or when to execute a sequel. MOEs fit into this effort by facilitating the organization and assessment of the information needed to support these decisions.

### Conclusion

Developing MOEs to assess the effectiveness of the information operation is a difficult task. In many respects, MOE creation is much more art than science. However, through development of proper MOEs and an effective assessment plan as discussed in this article, we can link the science involved in achieving and assessing first-order effects to the more subjective assessments of accomplishing second- and third-order effects. Thus, the staff can make an informed estimate of the effects resulting from execution of a command's IO tasks and establish the progress of the information operation campaign.

Clearly more work is necessary. However, as IO practitioners continue to work with MOEs and other as-

essment methodologies, they will continue to refine and validate successful techniques and procedures.



### Endnotes

1. Unit reporting and BDA address the success or failure of planned IO tasks to attack enemy and defend friendly information system assets. This information helps determine which enemy and friendly assets our actions affected and yields an estimate of the immediate results. The purpose of this first-order assessment is to determine if current IO tasks and the level of effort applied to the IO are adequate.

2. Joint Publication 3-60, *Joint Doctrine for Targeting*, 17 January 2002, page GL-8.

3. We may develop MOEs to measure the accomplishment of individual IO tasks. Doing so is largely dependent upon the importance of the task, as well as the availability of resources and time to plan and conduct an assessment to that level of detail.

4. Murray, William S., "A Will to Measure," *Parameters*, Autumn 2001, page 135.

5. A well-crafted IO objective specifies an effect, an object of the effect, and a purpose for the effect. Normally, offensive IO objectives are in terms of causing an adversary to do or not do something. Defensive IO objectives are in terms of protecting and defending friendly force's information and information systems.

6. It is important to note that doctrine does not provide specific effects for IO. Typical effects used in the field are deny, destroy, degrade, disrupt, deceive, exploit, and influence. Some of these effects are taken from targeting and therefore have specific definitions, while we use other effects simply because they seem appropriate to IO. Having well-defined effects will certainly assist the planning and development of IO objectives and MOEs. Another noteworthy aspect of IO doctrine is the lack of terms for describing defensive IO effects.

7. This MOE assumes that the enemy commander's predicted decision (as determined by the G2's intelligence preparation of the battlespace), was either to block or counterattack the II Corps' ground offensive.

*Lieutenant Colonel (Promotable) David C. Grohoski is currently the Deputy Director of Operations for the U.S. Army 1st Information Operations Command (Land). A career Infantry officer, his previous assignments include Battalion Senior Observer/*

Controller at the Joint Readiness Training Center (JRTC), Exchange Officer with the British Army, Executive Officer of the 3d Infantry Regiment (The Old Guard), as well as assignments in light infantry and airborne ranger units. He was a Distinguished Military Graduate of Michigan State University with a Bachelor of Arts degree in Social Science and earned a Master of Public Administration degree from the University of Oklahoma.

Major Steven Seybert (U.S. Army, Retired) has provided contract support for more

than six years to the U.S. Army 1st IO Command (Land) in planning and conducting IO. He has served with IO field support teams on deployments to various levels of military command from joint task force to division. He performed as an IO targeting officer while deployed to Operation JOINT GUARDIAN and as an IO planner during Operation IRAQI FREEDOM. He is a graduate of the U.S. Military Academy at West Point, New York, and the Command and General Staff Course. Readers may contact him via E-mail at [steve.seybert@us.army.mil](mailto:steve.seybert@us.army.mil).

Major Marc Romanych (U.S. Army, Retired) is a former Air Defense Artillery Officer. He works as a contractor with the U.S. Army 1st IO Command (Land). Since 1998, he has deployed with IO field support teams to Bosnia-Herzegovina, Kosovo, and numerous joint and Army warfighter exercises. Mr. Romanych teaches two courses on IO for American Military University. He holds degrees in Chemistry, Geology, History, and International Relations. Readers may contact him via E-mail at [marc.romanych@us.army.mil](mailto:marc.romanych@us.army.mil).

### Joint C4I Staff and Operations Course

What is in your future? Are you or will you soon be serving at a corps- or theater-level G2 or G6 staff in support of a joint task force (JTF) or working with a JTF Joint Communications Control Center (JCCC) executing requirements associated with an information management plan? Or are you looking at an assignment to one of the theater signal com-

# Reserve Support to IO: The 3431st MI Detachment (USAR) at NGIC

by Sherwin H. Terry, Jr.

The 3431st Military Intelligence Detachment (MID), U.S. Army Reserve (USAR), is one of 16 Army Reserve MIDs WARTRACEd to the National Ground Intelligence Center (NGIC) and supporting the Global War on Terrorism and Operation IRAQI FREEDOM. The 3431st MID is different from the usual MID, however, because it is a 45-person production group, rather than the classic 9-person detachment. Through this enlarged structure, the unit is providing support to NGIC and the U.S. Army Intelligence and Security Command (INSCOM) in the realm of intelligence support to information operations (IO) and computer network operations (CNO).

## MIDs Augment NGIC Support

NGIC is the Army's intelligence production activity located in Charlottesville, Virginia. The Center produces all-source ground-forces intelligence for a long list of custom-

ers that range from military research and development organizations, weapons developers, and senior Department of Defense decision-makers to the operational forces in the field. Assisting in this daunting task are 16 MIDs WARTRACEd to the Center. The many talents they bring expand the specialized expertise and skills available among the almost 800 civilian and military employees of the Center. For example, some of these MIDs boast members with expertise in chemical and nuclear weapons, small arms, radar systems, or skills in assessing foreign national military infrastructures. During the last 18 months, the Army called these MIDs to active duty to add their talents to NGIC's expertise in support of the Global War on Terrorism and Operation IRAQI FREEDOM.

## Structure of the 3431st MID

Among the 16 MIDs supporting NGIC is the 3431st MID, a produc-

tion group that differs from other MIDs in that it actually comprises five integral 9-person detachments. In August 2001, the Department of the Army (DA) authorized a reorganization of the 3431st MID to an expanded composition resulting from earlier direction by Lieutenant General (LTG) Thomas Plewes, then Chief of the USAR. Learning that the mission of the 3431st is to assist NGIC's intelligence production in response to customers' IO and CNO requirements, LTG Plewes seized on the opportunity to reinforce that support with an enhanced Reserve unit tailored especially for the task.

In September 2001, in the midst of beginning to reorganize and to recruit the necessary personnel to outfit its new structure, the 3431st MID became embroiled in the Global War on Terrorism resulting from the terrorist attacks of September 11. Twenty-seven strong, the unit began a tour of active duty in October 2001 for one year. Unit members provided personnel for the IO mission at the 1st Information Operations Command (Land) (formerly called the Land Information Warfare Activity, or LIWA) at Fort Belvoir, Virginia, and for IO intelligence production support to meet NGIC customers' needs. During their period of active duty, those members of the 3431st MID assigned to the 1st IO Command prepared assessments for IO Field Support Teams deployed with the U.S. Forces in Afghanistan, and those at NGIC published intelligence assessments addressing the command, control, and communications (C3) capabilities of transnational terrorist groups.

The period of unit activation all but halted the retailoring of the 3431st MID. Under the leadership of the Production Group Commander, Colonel Leslie Purser, that effort was reinvigo-



The front of the National Ground Intelligence Center building.

Courtesy of NGIC.



**NGIC employee Thomas Nelson, on a detail supporting Operation ENDURING FREEDOM, and Sergeant Christopher Newsome, 3431st MID, preparing an IO assessment at 1st IO Command (Land).**

rated. The Army is actively recruiting new members, particularly individuals with specific specialized skill sets in computer forensics; computer networking; network security; physics, math, and basic sciences; foreign area studies; and above all, an intelligence background. The personnel resourcing structure for each of the five detachments lists three commissioned officers (military occupational specialty [MOS] 35D, All-Source Intelligence Officer), a senior warrant officer (MOS 350B, All-Source Intelligence Technician), and five enlisted soldiers (MOS 96B, Intelligence Analyst) ranging in grade from E5 to E8. Due to the delayed restructuring, the production group has until September 2004 to reach full strength.

The Army tailored constitution of each of the five detachments of the 3431st to present a unique approach to the IO intelligence problem and how it will help NGIC to support customers' needs:

- ❑ One detachment will examine the telecommunications systems of potential adversaries' ground forces and assess the capability of those networks to support computer network at-

tacks that they might direct against the U.S. Army.

- ❑ Another detachment is supporting NGIC's intelligence research and reporting about the technologies underpinning foreign IO and projecting where those technologies will lead in the next 5 to 15 years.
- ❑ A third detachment is looking at adversaries' tactics, techniques, and procedures to assess a nation's or transnational group's intent to use CNO for insurgency or terrorism against the Army.
- ❑ The fourth detachment, in addition to performing the functions of the Group headquarters, can provide a flexible production surge capability for the other detachments in the event that NGIC experiences an overload of IO tasking.
- ❑ The fifth detachment has a unique role in approaching the IO problem: it is projecting NGIC production support to other INSCOM subcommands that will require IO intelligence production. Members of this detachment are currently drilling at Fort Belvoir, where they are augmenting the 1st IO Command (Land).

## IO Products from the 3431st MID

The 3431st MID has produced a number of IO-related intelligence documents supporting the efforts of NGIC and the Army. The publications span the gamut from the short, directed assessments on particular aspects of C3 or CNO, like those described above, to comprehensive IO country studies addressing the entirety of IO. The U.S. Army Training and Doctrine Command (TRADOC) has used one particular series of country studies to develop scenarios for IO segments of wargames for the Army of the future. Members of the 3431st MID also made a major contribution to the IO section of a study assessing the threat to the Army's Future Combat System (FCS). Due to these two efforts alone, the 3431st MID has made a significant impact in helping to design the Army of the future. More recently, their publications in support of Operation IRAQI FREEDOM include assessments on Iraqi weapons and technologies and the urban defense prospects of the Iraqi forces.

## Conclusion

As the 3431st MID Production Group approaches full strength, it will continue to expand its formidable presence in the IO and CNO intelligence production capabilities of the National Ground Intelligence Center. The MID will permit the Center to address the needs of its customers better, with a broader and more talented base than would otherwise be available.



*Sherwin Terry (Lieutenant Colonel, U.S. Army Reserve, Retired) is currently an electronics engineer with the National Ground Intelligence Center. He holds a Bachelor of Arts degree in Mathematics and a Bachelor of Science degree in Electrical Engineering from Bucknell University and a Master of Business Administration degree from James Madison University. He is a graduate of the Command and General Staff College and has served as a CGSC Instructor. Among his duties at NGIC, he is the NGIC point of contact for the 3431st MID.*

# Intelligence Support to Information Operations: Staff Chaplains

by Major Norman Emery

*A version of this article previously appeared in the Center for Army Lessons Learned (CALL) Training Techniques, 2nd Quarter, Fiscal Year 2003 (TQ2-03),<sup>1</sup> Reprinted with permission.*

*IPB supports IO by identifying the IO capabilities and vulnerabilities of friendly, adversary, and other key groups. It portrays adversary and other key group leaders/decision-makers, command and control (C2) systems, and decisionmaking processes.*

—FM 3-13, Information Operations:  
Doctrine, Tactics, Techniques,  
and Procedures

Throughout the past ten years, U.S. peace and combat operations in Bosnia-Herzegovina, Africa, Haiti, Kosovo, and Afghanistan have involved influencing the population to achieve specific military objectives. Those “influence operations,” which were part of an information operations (IO) campaign, required a thorough understanding of a country or region’s religious and social culture. The planning process often overlooks or underdevelops this understanding. The staff chaplain, an oft available but underutilized asset, can be a crucial person in the analysis of culture in information operations. The Chaplain Corps recognizes, and is responding to, this need.

## Importance of Understanding Culture

In military planning and operations, culture is a broad term that encompasses a country’s history of its peoples, religions, and hierarchal structure, religious and social customs and observances, and defines social relationships and structure. A command’s failure to recognize or respect a country’s culture can undermine or impede the command’s

mission, or otherwise affect its ability to influence the information environment through IO. Below are some examples of how knowledge of the culture impacts IO planning in—

- ❑ Coordinating with shuras, mullahs, and other trusted members in rural and small urban communities to distribute humanitarian assistance to the local populace.
- ❑ Recognizing and acknowledging important holidays to gain the populace’s respect.
- ❑ Preventing a faux pas in observation of customs.
- ❑ Creating a nodal analysis of religious leaders who possess few degrees of separation from key leaders.
- ❑ Understanding tribal relations, concepts, and traditions, which often can differ from those of U.S. forces’ own experiences and conceptions.

## Integrating Staff Chaplains

Ideally, a unit would deploy with a well-developed culture database. With or without such a tool, the optimal time to integrate the analysis of culture is during the mission analysis (MA) of the military decisionmaking process (MDMP). This responsibility generally falls upon the G2/J2 Plans section, the analysis and control element (ACE), or both. Often the initial cultural analysis is very shallow due to collection and analysis prioritization; therefore, it requires emphasis by the IO section. Since sections can be small and limited in time and knowledge resources, ad hoc members are necessary to develop the cultural analysis requirement. Although having foreign area officers (FAOs) may be ideal, their actual inclusion on staffs is

rare and may be entirely absent during the critical initial planning phases. It is here that a staff chaplain can contribute significantly. During the mission analysis, the IO section develops the IO intelligence preparation of the battlespace (IPB). Essential elements of IO IPB include—

- ❑ In-depth analysis of religion.
- ❑ Important religious and cultural dates and observances.
- ❑ Religious and social structure.
- ❑ Leaders and their probable influence.

Identifying religious leaders can help the G2/J2 develop a link analysis. Additionally, religious leaders are often very influential with the local population, which can support accomplishing IO objectives. The staff chaplain involvement in the MA should go beyond reporting of “Blue” assets (e.g., how many chaplains and resources are necessary for operations at subordinate level). The staff chaplain should also conduct his own form of IPB; his knowledge is essential in the development of the IO campaign plan. Several leaders learned the value of knowing and understanding local religious practices in Bosnia, and the lack of knowledge at times hampered U.S. efforts.

Chaplain (Colonel) Albert Smith, Third Army and Combined/Joint Forces Land Component Command (C/JFLCC) Chaplain, supports the concept of using staff chaplains for this purpose but emphasizes that commanders and their staffs must understand that staff chaplains have a different role than ground chaplains (those assigned to combat and support units). While commanders can

expect staff chaplains to provide their contribution to IO IPB, research databases, and possibly assist in culture analysis, these chaplains cannot be part of an intelligence collection plan. Generally, chaplains of any faith can gain access to local religious leaders since religion and a profession of faith are the common bonds. As an unwritten professional courtesy, that trust cannot be diminished due to perceptions that chaplains are intelligence gatherers! If that bond of trust is ever compromised, it is not just distrust of that particular chaplain. Therefore, we must follow these unwritten rules and protocols.

### Challenges and the World Religion Program

Chaplains must have proper development to succeed in this suggested role. There still exist some challenges. Foremost is the fact that the majority of U.S. chaplains are Christian or Jewish, while the dominant religions in the current and foreseeable majority of operational areas are Muslim (or other

faiths). The Chaplain Corps recognizes this fact, and has expanded its training through its World Religion Program. World Religion instructors research, develop databases, and teach the complexities of various regional religious beliefs and social cultures. Instructors are at four locations: Defense Language Institute Foreign Language Center (DLIFLC) in Monterey, California; the Chaplain Advanced Course at Fort Jackson, South Carolina; the psychological operations (PSYOPs) school at the John Fitzgerald Kennedy (JFK) Special Warfare Center at Fort Bragg, North Carolina; and the Command and General Staff College at Fort Leavenworth, Kansas.

The other significant challenge is ensuring the staff chaplain has current, accurate, and detailed information once deployed. The Chaplain School created a “reach” back capability (a centralized information support system) to provide support not only to staff chaplains but also to planning staffs in general. A well-researched World Religions website ([wrc.lingnet.org](http://wrc.lingnet.org)) provides the first

link to critical cultural information. According to Chaplain (Major) Larry Closter, former World Religion Chaplain at DLIFLC:

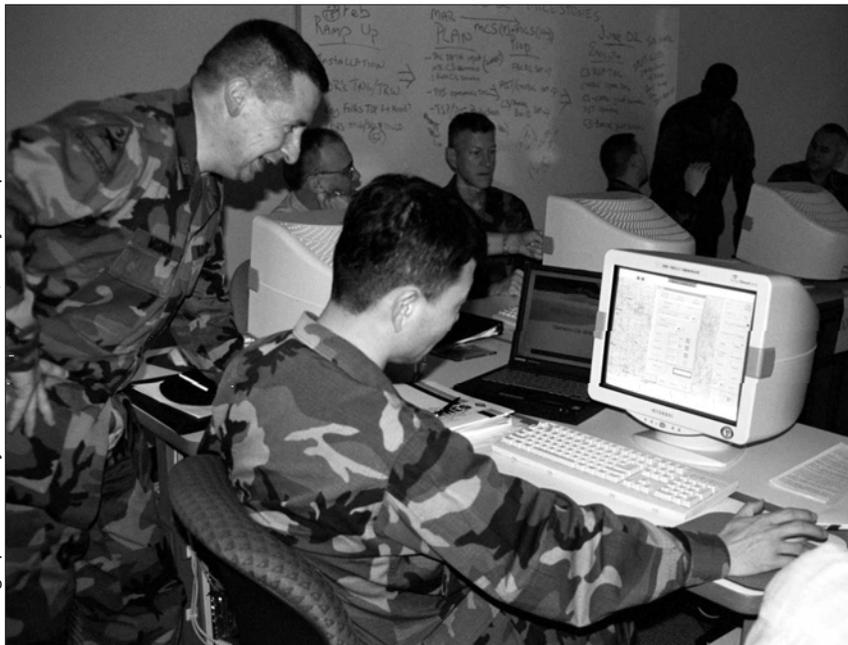
*General comments on culture are not very helpful to the process, since each religion has its own nuances. A good example is the Kurds. They have a great variety in their structure because of isolation due to the mountainous region they live in.<sup>2</sup>*

A command needs a chaplain on the staff who knows the system and structure. Chaplain Closter states that commanders frequently ask questions about indigenous religions, history of religions, burial rituals, and major holidays that may clog main supply routes (e.g., pilgrimages). If scouts or human intelligence (HUMINT) collectors are unable to obtain this information, the website is there to support chaplains with a database containing tiered layers of information. For example, it explains Islam in general, then the website goes into more details such as the Sunni and Shiite sects, etc. The site is also organized by region and then narrows to local levels (major areas), addressing the known power structure and how they practice religion. The challenge is building the database for areas where few after-action reports (AARs) exist. Chaplain Closter says the State Department has an excellent database and there is discussion concerning how to combine the two databases.

The staff chaplain’s preparation to be a valuable member of the IO planning team consists of one or more of the following resources:

- That chaplain’s own faith and training.
- The World Religions website ([wrc.lingnet.org](http://wrc.lingnet.org)). The website is the most referenced capability. Part of the database is books developed to inform language students, which chaplains also

Photograph courtesy of Nella Hobson, Army Chaplain School.



**The Army Chaplain School set up a special classroom in 2002 with seventeen Force XXI Battle Command Brigade and Below systems to train chaplains and chaplain assistants in tactical religious support using digital technology.**

find useful. The books currently cover North Africa, Asia, East Europe, and South America, largely due to the efforts of Chaplain (Lieutenant Colonel) Ken Sampson. The goal is to eventually have a "religious map" of the entire world.

- ❑ World Religion instructors. All instructors have earned at least a master's degree in world religion or an aspect of world religion, and planners may contact them directly for their expertise.
- ❑ The Chaplain Basic and Advanced Courses and World Religion course. Instruction at these courses integrates chaplains just out of the seminary who generally have little knowledge of other world religions apart from their own; most chaplains are open to learning about or understanding other religions.

### Staff Chaplains Are Planning Multipliers

In summary, staff chaplains are a valuable but underutilized re-

source in developing the analysis of an adversary's culture for the MDMP. Many IO missions can begin before combat operations, and failure to understand the complexities of culture can negatively impact those operations. At that point it is too late. Commanders and operations staff officers should understand that staff chaplains can be a valuable multiplier in the total planning process by assisting in developing the reverse IPB for MA, the IO Working Group (IOWG), and targeting boards, and should insist on their participation. Their products are critical for intelligence support to IO, which requires an in-depth understanding of culture for operations involving humanitarian assistance, civil affairs, PSYOPs, deception, and integrated IO. The doctrinal organization of the IOWG should change to reflect this greater role. The Chaplain Corps is making great strides to prepare its chaplains better for this role.



*I would like to thank Lieutenant Colonel Scott Kiefer, 1st IO Command, for his generous time and comments leading to this article.*

#### Endnote

1. The CALL TQ2-03 is available on the Internet at <http://call.army.mil/Products/TRNGQTR/TQ2-03/emery/emery.htm>.
2. Personal conversation with Chaplain (Major) Larry Closter, 7 June 2002.

*Major Norman Emery is a Functional Area 30 (Information Operations) officer and was a member of the Center for Army Lessons Learned (CALL) Operation ENDURING FREEDOM Combined Arms Assessment Team (CAAT) sent to Kuwait and Afghanistan in March 2002. His past assignments include Battalion S2, 1-187 Infantry, and company commands and Battalion S3 at the Presidio of Monterey. He is currently enrolled in the Special Operations and Low-Intensity Conflict/IO (SOLIC/IO) Program at the Naval Postgraduate School. You may contact MAJ Emery via E-mail at [nemery@nps.navy.mil](mailto:nemery@nps.navy.mil) and telephonically at (831) 372-0954.*

## Updated FDIC Websites on the Way at Fort Huachuca

The Futures Development Integration Center at the U.S. Army Intelligence Center is breathing new life into its elements' web sites by bringing all the sites under a centralized umbrella to maintain continuity and to improve the sites' appearance. Each site has a unique address in the form of **https://www.futures.hua.army.mil/<site>**, **http://<site>.futures.hua.army.mil**, or **http://secure.futures.hua.army.mil**.

#### FDIC Sites

<b>www</b>	Central launching point	<b>nsto</b>	New Systems Training Office
<b>abio</b>	Army Broadcast Intelligence Office	<b>tencap</b>	Tactical Exploitation of National Capabilities
<b>bcbl</b>	Battle Command Battle Lab-Huachuca	<b>tmmasas</b>	TSM All-Source Analysis System
<b>car</b>	Concepts, Architectures & Requirements	<b>tsmjstars</b>	Joint Surveillance Target Attack Radar System
<b>dcd</b>	Directorate of Combat Developments	<b>tsmprophet</b>	TRADOC System Manager (TSM), Prophet
<b>forcedesign</b>	Force Design Division	<b>tsmuav</b>	TSM Unmanned Aerial Vehicle
<b>kaps</b>	Knowledge and Program Services	<b>weather</b>	Army Weather Support Team

**Current Secure FDIC Sites** (password controlled software) <https://secure.futures.hua.army.mil>. These sites will be active soon.

<b>secure</b>	secure site with doctrine and web enabler sites (uses Army Knowledge On-Line login/password)
<b>weather</b>	(on the <a href="https://secure.futures.hua.army.mil">https://secure.futures.hua.army.mil</a> site)

# LIKE ADDING WINGS TO A TIGER— CHINESE INFORMATION WAR THEORY AND PRACTICE

by Timothy L. Thomas

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

During the past five years, numerous Chinese military and civilian scholars published significant works on information war (IW) and related issues. An analysis of their works yields several interesting results.

- First, the Chinese feel compelled to develop a specific Chinese IW theory, in accordance with the Chinese culture, economic and military situation, perceived threat, and their military philosophy and terminology.
- Second, Chinese military art strongly influences Chinese IW theory. China is quickly integrating IW theory into its People's War concept. It is also considering the development of an independent "net force" branch of service (to supplement the Navy, Army, and Air Force), and applying the 36 stratagems of war to IW methods.
- Third, Chinese military science dictates division of IW into subelements very different from those studied in the United States. These include the forms, nature, features, distinctions, principles, types, and levels of IW. These subdivisions are similar to Russia's IW methodology.

While a theory of Chinese IW is developing, turning theory into practice has proven more difficult since China is still developing the civilian and military infrastructure to support its philosophy.<sup>1</sup> This article will highlight crucial aspects of the specific Chinese approach to IW. It will begin by discussing how the

information age has affected China's attitude toward warfare and the specific Chinese historical factors affecting this interpretation. Finally, it will discuss Chinese IW definitions, and investigate the training courses and organizational structures needed to teach IW.

## IW with Chinese Characteristics

The major change of the information age was a reassessment of how to evaluate and conduct warfare. China realized that although it cannot currently threaten other countries as a superpower might, it can do something with its IW force, such as theoretically threaten U.S. financial stability. The characteristics of information (global reach, speed-of-light transmission, nonlinear effects, inexhaustibility, multiple access, etc.) control the material and energy of warfare in a way that nuclear weapons cannot.<sup>2</sup> IW attempts to beat the enemy in terms of promptness, accuracy, and sustainability.<sup>3</sup> It thus makes complete sense to put a significant effort into developing an information-based capability in both the civilian and military sense. From the Chinese point of view, IW is like adding wings to a tiger, making the latter more combat-worthy than before.

Recent reports of hacker attacks on U.S. labs indicate that China is moving from theory to practice in security matters as well. *The Washington Times* reported on 3 August 2000 that hackers suspected of working for a Chinese Government institute broke into a Los Alamos computer system and took large amounts of sensitive but unclassified information. Los Alamos spokesperson Jim Danneskiold stated that "an enormous amount of Chinese activity" occurs continuously.<sup>4</sup>

The targets of Chinese IW include information sources; channels; destinations;<sup>5</sup> command, control, communications, computers and intelligence (C4I); and electronic warfare (EW) assets. First attack objectives will be the computer networking system linking the political, economic, and military installations of a country and the ability to control decisionmaking to hinder coordinated actions. This IW focus implies that not just soldiers will conduct warfare in the future but civilians too. Some Chinese theorists have recommended organizing network special warfare detachments and computer experts to form a shock brigade of "network warriors" to accomplish this task.

Chinese IW experts recognize a need to reconsider how to compute the correlation of forces. The Chinese believe one can no longer calculate military strength using the number of armored divisions, air force wings, etc. In the information age, studies must include "invisible forces" such as computing and communications capabilities and system reliability.<sup>6</sup>

A second reevaluation of warfare was more traditional in nature. Chinese theorists believe that the capabilities and qualities of the information era enhance and breathe new life into Mao Zedung's theory of a People's War.

Electronics, computer, and information engineering experts are likely to become the genuine heroes of a new People's War, much like the warrior class of the past.<sup>7</sup> In addition to the economic factors, this may explain why China is willing to reduce its Army—China can "keep up" with other countries by employing a multitude of information engineers and citizens with laptops instead of just soldiers. China clearly has the

people to conduct “take home battle,” a reference to battle conducted with laptops at home that allow thousands of citizens to hack foreign computer systems when needed. China has a number of superior software writers and much untapped potential in the information field. The problem is how to find more information space and equipment for all of these people.<sup>8</sup>

Ideas for uniting a People’s War with IW are finding fertile ground in the 1.5 million-person reserve force of China. The People’s Liberation Army (PLA) is turning reserve forces in some districts into mini-IW regiments. For example, in the Echeng District (about 700 miles due south of Beijing) in Hubei Province, the People’s Armed Forces Department (PAFD) organized 20 city departments (power, finance, television, medical, etc.) into a militia or reserve IW regiment. The PAFD had a network warfare battalion, as well as EW, intelligence, psychological warfare (PSYWAR) battalions, and 35 technical “*Fenduis*” (squad to battalion units). The PAFD also set up the first reserve IW training base for 500 people. The Echeng District PAFD even gave a website at <http://ezarmy.net>.<sup>9</sup>

Echeng is not the only district with reserve or militia units conducting IW training. The Fujian Province held a meeting at Xiamen in December 1999 that had reserve and militia forces. The report cited militia high-technology *Fenduis* that carried out electronic countermeasures, network attack and defense, and radar reconnaissance operations. They conducted these operations as part of an enforced blockade of an island—which may have implications for Taiwan. The Xiamen area is a special economic zone and attracts a higher-than-usual number of science and technology clients to the area;<sup>10</sup> thus, it is a prime area for IW-related activities. There are also reports of reserve IW

activity in Xian PAFD, and in the Datong military subdistrict (MSD).

In Xian, the PAFD IW *Fendui* acted as the opposing forces (OPFOR) for a military district exercise in the Jinan Military Region. They listed ten information operations (IO) methods: planting information mines, conducting information reconnaissance, changing network data, releasing information bombs, dumping information garbage, disseminating propaganda, applying information deception, releasing clone information, organizing information defense, and establishing network spy stations.<sup>11</sup>

A third way the information age affected China’s attitude toward warfare is an updating of historical strategies. Some 300 years ago, an unknown scholar compiled **The Secret Art of War: The 36 Stratagems**, and emphasized deception as a military art that can achieve specific military objectives. In the information age—characterized by anonymous attacks and uncertainty (e.g., uncertain origins of viruses, the existence of “back doors” in programs, etc.)—the stratagems may be revitalized as a tactic. It should therefore be easier to deceive or inflict perception management injuries (“guidance injuries” in Chinese). For example, one of the 36 stratagems is “*besiege Wei to rescue Zhao*.” This means when the enemy is too strong to attack directly, then attack something he holds dear. The IW application is that if you cannot afford a direct (nuclear) attack, then attack the servers and nets responsible for Western financial, power, political, and other systems stability. The journal **China Military Science** published an article about IW stratagems in 2001 indicating the IW-stratagem tie remains important. The information age is developing into the age of anonymous persuaders.

A May 2000 Chinese article on Internet War offered the logic behind “why” military leaders might use such stratagems today. China is currently

a relatively weak IO power and must use tricks and strategy to compensate for the shortage of material assets.<sup>12</sup>

A “net force,” if developed, would protect net sovereignty and engage in net warfare, a technology and knowledge-intensive type of warfare. Net technology would include—

- ❑ **Scanning technology** to break codes, steal data, and take recovery (anti-follow-up) actions.
- ❑ **Superior offensive technology** capable of launching attacks and countermeasures on the net, including information-paralyzing software, information-blocking software, and information-deception software.
- ❑ **Masquerade technology** capable of stealing authority from the network by assuming a false identity.
- ❑ **Defensive technology** that can ward off attacks, serve as an electronic gate to prevent internal leaks, and block arbitrary actions, much like an electronic policeman.<sup>13</sup>

### Chinese IW Definitions: Focus on Network and Cognitive Processes

Studying Chinese IW definitions consecutively by year offers clues to the developing nature of Chinese IW theory. In 1996, the definition of IW offered by Shen Weiguang stated it is a war in which both sides strive to hold the battlefield initiative by **controlling** the flow of information and intelligence. Instead of protecting friendly information systems and attacking enemy systems, as the United States defines the term, Shen emphasized protecting oneself and **controlling** the enemy.<sup>14</sup> Wang Pufeng stated the central issue in achieving victory in IW is **control** of information. Thus, in 1996, the emphasis was clearly on *control*.

In 1997, author Liang Zhenxing stated that IW includes all types of war-fighting activities that involve the exploitation, alteration, and paraly-

sis of the enemy's information and information systems, as well as all those types of activities that involve protecting one's own information and information systems from similar enemy actions. Liang added that the Chinese definition of IW should take cognizance of Chinese characteristics but be in line with the definition prevailing internationally.

Another 1997 author, Wang Baocun, covered the forms, nature, levels, distinctions, features, and principles of IW. He listed **forms of IW** as peacetime, crisis, and wartime; the **nature of IW** as reflected in offensive and defensive operations; **levels of IW** as national, strategic, theater, and tactical; and **other distinctions of IW** as command and control (C2), intelligence, electronic, psychological, cyberspace, hackers, virtual, economic, strategy, and precision. He enumerated the **features of IW** as complexity, limited goals, short duration, less damage, larger battle space and less troop density, transparency, the intense struggle for information superiority, increased integration, increased demand on command, new aspects of massing forces, and the fact that effective strength may not be the main target. He stated that **principles of IW** include decapitation, blinding, transparency, quick response, and survival.<sup>15</sup>

In 1998, one analyst defined IW as the ability to hinder an opponent's decisionmaking while protecting friendly **decisionmaking** abilities. Note that the Chinese emphasis is not on attacking enemy information or information systems but on "hindering" an opponent's **decision-making**.

In 1999, Chinese analysts returned to serious debate over IW issues. Shen Weiguang defined IW this time more broadly as involving two sides in pitched battle against one another in the political, economic, cultural, scientific, social, and technological fields. The fight was over information

space and resources. He defined IW narrowly as the **confrontation of warring parties in the field of information**. The essence of IW is to attain the objective of "*forcing enemy troops to surrender without a fight*" through the use of information superiority.<sup>16</sup> This definition echoes historical Chinese thoughts on warfare, and implies information superiority is more of a **cognitive-** than **systems-**related process. Yuan Banggen, the head of a General Staff Directorate, stated that IW is "*the struggle waged to seize and keep control over information*," and the struggle between belligerent parties to "*seize the initiative in acquiring, controlling and using information*." This is accomplished by capitalizing on and sabotaging the enemy's information resources, information system, "informationized" weapon systems, and by using and protecting one's own information resources, information systems, and "informationized" weapon systems. Yuan thus substitutes "*capitalizing and sabotaging*" for the U.S. term "attacking" while simultaneously emphasizing control. He also noted that IW is a kind of knowledge warfare.<sup>17</sup>

In late December 1999, Xie Guang, the Vice-Minister of the Commission of Science, Technology and Industry for National Defense, stated that IW:

*...in the military sense means overall use of various types of information techniques, equipment, and systems, using disturbance, misinformation or destruction of the enemy's information systems, particularly his command systems, to shake the determination of the enemy's policymakers, and at the same time the use of all means possible to ensure that one's own information systems are not damaged or disturbed.*<sup>18</sup>

In 2000, Wang Pufeng offered a deeper explanation of information war, distinguishing it from information warfare. In Wang's opinion, an **in-**

**formation war** refers to a kind of **war** and a kind of **war pattern**, while **information warfare** refers to a kind of **operation** and a kind of **operational pattern**. The new operational pattern refers to operations in a computer network space. IW embraces information detection systems, information transmission systems, information and weapon strike systems, and information processing and use systems. **Information war includes information warfare**. Both integrate information and energy and use an information-network-based battlefield as their arena.<sup>19</sup>

Few Chinese authors attempted to define IO but one who did was Yuan Banggen in 1999. Yuan stated that IO are specific IW operations. IW is the core of "informationized warfare," whereas IO are the manifestation of information warfare on the battlefield. IO's theoretical system develops from two levels, fundamental and application. Basic theories consist of fundamental concepts about IO, its organizational structure and technological equipment, C2 for IO, etc. One can categorize application theories into offensive IO and defensive IO; strategic, operational, campaign, and tactical levels; and into peacetime, wartime, and crisis-period IO. All IO activities center upon C2. IO's two missions are preparation and implementation; its principles are centralized command, multilevel power delegation, multidimensional inspection and testing, timely decisionmaking, and the integration of military and civilian actions with a focus on vital links.<sup>20</sup>

Author Qi Jianguo suggested uniting the network with a People's War. He recommended that the PLA establish a *People's War organ* that is an authoritative, centralized, and united network. It would control IO and networking activities, and allow for the conduct of mobilization exercises and education on People's War on the network. Laws and regulations need formulation in

order to standardize the preparations and development of a network People's War.<sup>21</sup> China must uphold the principle of combining the establishment of networks for both wartime and peacetime use, setting up networks for both military and civilian use, and developing Internet service in a limited manner.<sup>22</sup>

Wang Baocun also believes strongly in the union of IW and cognitive processes. He described perception structures, perception systems, and belief systems as IW components. He defined a perception structure as:

*...all things that an individual or a group considers correct or true, regardless of whether these things that are considered correct or true have been obtained through perception or belief.*

His definition of perception structures says they comprise perception systems, as those...

*systems which are established and operated in order to understand or observe verifiable phenomena by turning such phenomena into perceptible realities and subsequently to make decisions or take action on the basis of intuitive understanding of such realities.*

Belief systems are "systems which guide testable empirical information and such information and consciousness that cannot be tested or are hard to test."<sup>23</sup>

## **Chinese Organizations and Training Needed to Conduct IW**

There are several organizations charged with IW instruction for the PLA. The lead organization is the **Communications Command Academy**. The Academy is in Wuhan, the capital of central China's Hubei Province. In 1998, the Academy announced the publication of two books, **Command and Control**

**in IW** and **Technology in IW** that became the leading Chinese IW texts. The Academy is well respected for its IW curriculum that analyzes strategic, operational, and tactical IW requirements.<sup>24</sup> Interestingly, the Academy is not far from the reserve component IW regiment in Echeng district.

A second leading PLA IW institute is the **Information Engineering University**, established by combining the Institute of Information Engineering, the Electronic Technology College, and the Survey and Mapping College. Located in Zhengzhou, the capital of Henan Province, the University will help cultivate professionals for high-technology warfare involving the use of information, according to President Major General Zhou Rongting, and will create a number of new specialties such as remote-image information engineering, satellite-navigation and positioning engineering, and map databanks. The major specialties include information security, modern communications technology, and space technology.<sup>25</sup>

A third PLA IW location is the **Science and Engineering University**, established by combining the Institute of Communications Engineering, the Engineering Institute of the Engineering Corps, the Meteorology Institute of the Air Force, and the 63d Research Institute of the General Staff headquarters. It trains new military personnel in fields such as IW, communications and command automation, and other subjects.<sup>26</sup> There are more than 400 experts and professors at the University teaching IW theories and technological subjects.<sup>27</sup>

A fourth PLA IW-related institute is the **National Defense Science and Technology University** in Changsha. Directly under the supervision of the Central Military Commission, it is where China develops the "Yin He" series of supercomputers.<sup>28</sup> From April to

June 1999, some 60 senior officers (average age 53) studied high-technology warfare at the University during the war in Kosovo.

The **Navy Engineering College**, headed by President Shao Zijun, is a PLA Navy institute studying IW. The general orientation of the College is to combine arms and information. It hopes to help adapt the Chinese Navy to the combat needs of IW.

The system of training advanced in 1996 to handle this problem involved first laying a sound strategic foundation, then improving everyone's knowledge about IW by studying the experiences of foreign armies. Then it stressed expanding basic IW skills, especially in electronic and PSYWAR, and in information attack and defense. Finally, the training would emphasize converting knowledge to ability through the conduct of IW exercises. Press reports indicated that China followed this plan.<sup>29</sup>

## **Conclusions**

What conclusions do we draw, first about Chinese IW and then about recommendations for the U.S. Armed Forces? First, Chinese military theorists have found a relatively cheap and malleable methodology in IW, one that can enable China to catch up with the West in both strategic military and international status. These areas could lead China to play an important strategic role in the Asia-Pacific region and to emerge gradually into an economic competitor.

Second, China has an unusual emphasis on the emerging role of new IW forces. These various groups include the potential development of a net force (separate armed forces branch, although no evidence to date has confirmed the existence of such a separate branch), a shock brigade of network warriors, information protection troops, an information corps, electronic police, and a united network *People's War organ*, among

other units. Interestingly, Western nations are currently the most capable of instituting such a concept, since computers reside in so many homes and offices but the concept of forming an army from society is absent in these countries. Chinese theorists believe the side mobilizing the most computer experts to participate in take-home battle will very likely determine an IW victory. These forces would employ a strategy such as net point warfare, attempting to take out important information nodes and junctions. The Chinese believe in the power of network stability, and focus greatly on the protection of the network.

Third, Chinese IW emphasis reflects a mixture of Western and Chinese thinking that is moving away from the former. It is a Chinese proclivity to stress control, computerized warfare, network warfare, and knowledge warfare in addition to information superiority and "system of systems" theories, which have become the Western norm. Chinese thinking is closer to that of the Russians due to a common frame of reference (military art and the Marxist dialectic). There has also evolved a Chinese specific IW lexicon that is different from that used by Russia and the West.

Fourth, Chinese IW often looks to Chinese military history to find answers to today's problems, such as **The Secret Art of War's** 36 stratagems. IW appears to fit well with these stratagems. Yet China recognizes the capabilities inherent in Western IW and will think twice before engaging.

Thus for the U.S. military, a study of Chinese IW methods would be not only advisable but also required. Such a study might uncover inherent IW weaknesses in the U.S. system when analyzed through the thought process of another ideological prism or framework. The worst mistake that the United States

can make is to use its own process for uncovering vulnerabilities exclusively, since there are other problem-solving schemes (e.g., the dialectic) available. As the Chinese have said, losers in IW will not just be those with backward technology but those who lack command thinking and the ability to apply strategies. It is worth the time of the U.S. analytical community to scrutinize a variety of IW strategies and tactics.



#### Endnotes

1. To some Chinese theorists, the cornerstone of IW's operational theory involves preserving the integrity and stability of the infrastructure of one's side to perform these functions. Infrastructure stability is more important than survivability of units. See Wang Jianghuai and Lin Dong, "Viewing Our Army's Quality Building from the Perspective of What Information Warfare Demands," Beijing *Jiefangjun Bao*, 3 March 1998, page 6, as translated and downloaded from the FBIS website on 16 March 1998.
2. Shen Weiguang, "Focus of Contemporary World Military Revolution—Introduction to Research in IW," *Jiefangjun Bao*, 7 November 1995, page 6, as translated and reported in FBIS-CHI-95-239, 13 December 1995, pages 22-27.
3. Wang Jianghuai and Lin Dong, ID at 1.
4. Bill Gertz, "Hackers Linked to China Stole Documents from Los Alamos," *The Washington Times*, 3 August 2000, page 1.
5. Wang Jianghuai and Lin Dong, page 6.
6. Hai Lung and Chang Feng, "Chinese Military Studies Information Warfare," Hong Kong *Kuang Chiao Ching* (Hong Kong), 16 January 1996, Number 280, pages 22, 23, as translated and published by FBIS-CHI-96-035, 21 February 1996, pages 33, 34.
7. Shen Weiguang, pages 22-27.
8. Wang Xiaodong, "Special Means of Warfare in the Information Age: Strategic Information Warfare," *Jianchuan Zhishi*, 30 June 1999, as translated and downloaded from the FBIS website on 27 July 1999.
9. *China National Defense News*, 24 January 2000, provided by Mr. William Belk via E-mail. Mr. Belk is the head of a skilled U.S. Reservist group that studies China.

10. *China National Defense News*, 15 December 1999, page 1, provided by Mr. Belk via E-mail.
11. *Qianjin Bao*, 10 December 1999, provided by Mr. Belk via E-mail.
12. Qi Jianguo, "Thought on Internet War," Beijing *Jiefangjun Bao*, Internet version, 16 May 2000, page 6, as translated and downloaded from the FBIS website on 16 May 2000.
13. Ibid.
14. Shen Weiguang [no title provided], Beijing *Zhongguo Guofang Keji X*, September-December 1996, No 5/6, pages 87-89, as translated and reported in FBIS-CHI-98-029, insert date 30 January 1998.
15. Wang Baocun, "A Preliminary Analysis of IW," Beijing *Zhongguo Junshi Kexue*, Number 4, 20 November 1997, pages 102-111, as translated and downloaded from the FBIS website on 20 November 1997.
16. Shen Weiguang, "Checking Information Warfare-Epoch Mission of Intellectual Military," *Jiefangjun Bao*, 2 February 1999, page 6, as translated and downloaded from the FBIS web site on 17 February 1999.
17. Yuan Banggen, "On IW, Digital Battlefields," Beijing *Zhongguo Junshi Kexue*, 20 February 1999, pages 46-51, as translated and downloaded from the FBIS website on 17 July 1999.
18. Xie Guang, "Wars Under High Tech," Beijing *Renmin Ribao*, 27 December 1999, page 7, as translated and downloaded from the FBIS website on 30 January 1999.
19. Wang Pufeng [no title provided], Hong Kong *Hsien-Tai Chun-Shih (Conmilit)*, 11 April 2000, pages 19-21, as translated and downloaded from the FBIS website on 3 May 2000.
20. Yuan, ID at 17.
21. Qi Jianguo, ID at 12, page 6.
22. Ibid.
23. Wang Baocun, "New Military Revolution in the World, 'Subduing Enemy Force without Battle' and Informationized Warfare," *Zhongguo Junshi Kexue*, 4 May 1999, pages 60-63, as translated and downloaded from the FBIS website on 23 August 1999.
24. Lei Yuanshen, "New Breakthrough in the Study of Information Warfare," *Jiefangjun Bao*, 21 July 1998, page 6, as translated and downloaded from the FBIS website on 12 August 1998.
25. "University to Foster Talent for High-Tech Warfare," *Xinhua*, 17 November 1999, as translated and downloaded from the FBIS website on 17 November 1999.

26. Ma Xiaochun, "PLA Sets Up Four New Academies," Beijing *Xinhua*, 2 July 1999, as translated and downloaded from the FBIS website on 7 July 1999.

27. "PLA Trains Personnel for Information Warfare," Hong Kong *Tai Yang Pao*, 15 September 1999, page A17, as translated and downloaded from the FBIS website on 15 September 1999.

28. Guo Hao, "Chinese Military Prepares to Fight Digital Warfare," Hong Kong *Kuang Chiao Ching*, 16 March 2000, Number 330, pages 19-21, as translated and downloaded from the FBIS website on 16 March 2000.

29. Cheng Bingwen, "Let Training Lean Close to Information Warfare," *Jiefangjun Bao*, 12 November 1996, page 6, as translated and reported in

FBIS-CHI-96-230, inserted on 29 November 1996.

*Timothy Thomas (Lieutenant Colonel, U.S. Army, Retired) is an analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He was a U.S. Army Foreign Area Officer who specialized in Soviet and Russian studies and his military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an Inspector of Soviet Tactical Operations under the Commission on Security and Cooperation in Europe (CSCE); and as a Brigade S2 and Company Commander in the 82d Airborne Division. He earned a Bachelor of Science degree from the U.S. Military Academy at West Point,*

*New York, and a Master of Arts degree from the University of Southern California. Mr. Thomas has done extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low-intensity conflict, and political-military affairs. He is the Assistant Editor of the journal **European Security**; an Adjunct Professor at the U.S. Army's Eurasian Institute; an Adjunct Lecturer at the U.S. Air Force Special Operations School; and a member of two Russian organizations, the Academy of International Information and the Academy of Natural Sciences. Mr. Thomas' articles also have appeared in Russian publications and **Czech Military Thought**; and he has co-authored several articles with Russian military officers. Mr. Thomas speaks and reads Russian.*

## U.S. Army Reserve Command MI Augmentation Detachment

Military Intelligence (MI) soldiers are a critical U.S. Army asset. The nation has a real interest in preserving and employing these skills, especially as the MI soldier gains experience in using these hard-won skills. To retain these soldiers and their skills for the nation, the U.S. Army Reserve Command established the Military Intelligence Augmentation Detachment (MIAD) directly subordinate to the USARC. The MIAD's mission is to facilitate life-cycle management of MI soldiers in the Reserve Component (RC). The Detachment accomplishes its mission by assigning USAR enlisted, warrant, and company-grade soldiers to USARC high-priority MI units with vacancies. The MIAD enables MI-qualified soldiers who do not reside near a USARC Tier 1 unit to be productive members of the U.S. Army Reserve (USAR). The primary MIAD focus is the retention of soldiers leaving active duty, soldiers displaced by unit reorganizations or inactivation, and USAR soldiers relocating to an area without a USAR MI unit.

After joining the MIAD, MI soldiers have funding to attend a minimum of six 3-day trips in active-duty-for-training (ADT) status each fiscal year. These normally occur during the unit's weekend training periods. During these six ADT periods, the MIAD funds the soldier's transportation and lodging expenses. The soldier also must perform a minimum of 24 mutual training assemblies (MUTAs) either at a unit close to his home or through other means such as performing intelligence-related work using the World Basic Information Library. The MIAD will also fund travel and base pay for the soldier's annual training period (normally two weeks each year) if it is more than normal commuting distance of the soldier's home. Some USAR MI personnel perform their AT as overseas deployment training (ODT).

### Languages Needed

Currently the MIAD needs soldiers with language skills in Arabic, Chinese-Mandarin, French, Korean, Persian-Iranian, Spanish, Russian, Serbo-Croatian, Thai, Turkish, Urdu, and Vietnamese. Soldiers not skilled in critical languages may be eligible for attendance at the Defense Language Institute (DLI).

### Additional MIAD Opportunities

The MIAD also manages soldiers in two other types of units. A limited number of MIAD soldiers can serve as Technical Intelligence Analysts with 203d MI Battalion at Aberdeen Proving Ground, Maryland. The 203d is a multiple-component (MultiCompo) unit and the only technical intelligence battalion in the Army. To be eligible for this assignment, soldiers must be qualified Technical Intelligence Analysts. Most of these positions are at the Sergeant, Staff Sergeant, and Sergeant First Class levels. MI NCOs can also serve with one of the five Army Reserve Total Army School System (TASS) units as MI Instructors. These soldiers have the important job of instructing RC soldiers in MI subjects.

### Contacting the MIAD

Active duty soldiers leaving the Active Army who are interested in an MIAD assignment can obtain more information from their post transition counselors. Additional information on the MIAD is available from the Army Knowledge Online (AKO). Go the Army Communities/Army Reserve/Direct Reporting Units and click on the MI Augmentation Detachment. You can also contact the MIAD via E-mail at MIAD2@usarc-emh2.army.mil or by telephoning 1-800-359-8483, extensions 9546/8896.

# Determining Battlefield Effects in an Urban Environment: MOUT Terrain Analysis

by Lieutenant Colonel  
Alfonso J. Ahuja

*The increased population and accelerated growth of cities have made the problems of combat in built-up areas an urgent requirement for the U.S. Army. This type of combat cannot be avoided.*

—FM 90-10-1<sup>1</sup>

Military operations in Panama, Somalia, Kuwait, Bosnia-Herzegovina, and Iraq demonstrate the current and future requirements for U.S. forces to be able to operate effectively in an urban environment; the need for an urban warfare capability will not diminish in the future. Operations in an urban environment will present unique and complex challenges for all of our Battlefield Operating Systems (BOSs). The increasing focus on stability operations and support operations—to include Peacekeeping Operations, Combating Terrorism, Noncombatant Evacuations, Nation Assistance, Civil Disturbance Operations, Humanitarian Assistance, etc.—merely reinforces that more attention must be given to operations in an urban environment. In-

telligence doctrine must address these needs.

The most recent version of **FM 34-130, Intelligence Preparation of the Battlefield**, dated 8 July 1994, added a chapter to address the various considerations of the IPB process when conducting stability and support operations. The number of this type of operation has increased, and the Army increasingly conducts these operations in an urban environment.

The current **FM 34-130**, Chapter 6, IPB for Operations Other than War, does not adequately address the focus of the IPB process in the urban environment. The previous version of **FM 34-130** (May 1989) had Appendix B, IPB in the Urban Battle, which addressed in detail the special considerations for conducting the IPB process in an urban environment. The current **FM 90-10-1, An Infantryman's Guide to Combat in Built-up Areas**, has a chapter on Urban Analysis and an appendix on Urban Building Analysis that contains some of the material that was in the 1989 version of

**FM 34-130**. While this is a good source of doctrinal information, unit S2s should not need to go to an infantry manual to find doctrine on the IPB process.

*Doctrine Note: Although the Infantry Center and School promulgates this manual, in fact the Intelligence Center and Fort Huachuca wrote those intelligence annexes and appendixes, not just for FM 90-10-1 but also for FM 3-06, Urban Operations. A Special Text (ST) on Intelligence Support to Military Operations in Urban Terrain (MOU) is emerging; however, the Doctrine Division's subject matter expert recently left, and most of our military personnel are deployed in support of on-going operations. As time and resources permit, work will continue.*

While operations in an urban environment affect all steps of the IPB process, the focus of this article is on terrain analysis as part of Step 2, Describe the Battlefield Effects. To succeed in battle in built-up areas, commanders and leaders at all levels must understand the nature of the environment. To assist commanders, S2s must analyze the effects of urban terrain on enemy forces, unaligned elements, and friendly forces.

Terrain analysis in an urban environment differs from that of open terrain in many respects. The analysis of the five military aspects of terrain—obstacles, avenues of approach, key terrain, observation and fields of fire, concealment and cover (OAKOC)—still applies. This analysis, however, must be in the context of urban battlefield characteristics. A standard modified combined obstacles overlay (MCOO) developed from a military map and done in accordance with the current **FM 34-130** will not be of much use to leaders at the company level and below.

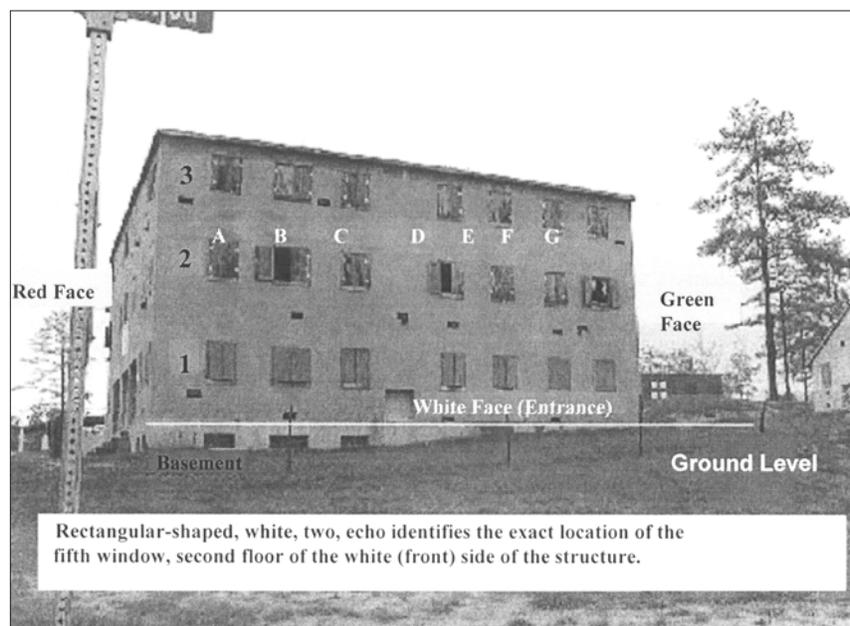


Figure 1. An Example of Structural Labeling.

*Doctrine Note: Emerging doctrine, to include production of STs, is already aggressively pursuing many of the issues raised by the author, and we are making efforts to incorporate existing, combat-tested methodologies. An example, taken from (Draft) ST 2-01.103, Intelligence Support to Urban Operations, follows:*

*There is, however, no standardized Army protocol to assist unit leaders (all echelons) in identifying key structural elements. Rather than enforce a position that may not allow the necessary flexibility, policy allows mission leaders and organizations to develop their own formats. This may include the Ranger Numbering standing operating procedure (SOP) or the Marine Corps Sniper Guide. Without being unduly restrictive, the objective continues to be standardization only at the mission letter. Figure 1 is provided only as an example of structural labeling although it does reflect all critical points. Figure 2 outlines procedures that may be followed and explains structural labeling.*

Standard military maps do not have the detail required to allow S2s to conduct a thorough analysis of urban terrain. Many standard military maps are old and do not reflect the more recent buildings, streets, and sometimes even significant urban growth. In addition, standard maps do not show the subsurface aspects of the urban environment: sewers, subways, and underground water systems. While these military maps show key public buildings and areas such as hospitals, clinics, stadiums, and parks, they do not clearly identify the water facilities, communication facilities, fuel supply, storage facilities, and temporary conditions (e.g., construction sites).

The S2's analysis of these unique aspects of urban terrain is crucial to the commanders' appreciation of the nature of this terrain.

- ❑ Sewer and subway systems can provide infiltration routes.
- ❑ Elevated railways and mass transit routes provide mobility on which the urban residents depend; if operations destroy or disable these facilities, congestion will occur.
- ❑ Utilities such as electrical, gas, or water facilities may be key targets.
- ❑ While forces cannot attack hospitals and clinics when not under use for military purposes, they may be a source of medical support for all factions and elements.
- ❑ Stadiums, parks, and sports fields may serve as holding ar-

reas, enemy prisoner of war (EPW) facilities, or landing and pickup zones.

- ❑ Construction sites and other commercial operations may be a source of Class IV<sup>2</sup> materials.

S2s must obtain maps or other imagery that contains this information so that they can analyze it and provide that product to maneuver commanders.

The Army must somewhat alter analysis of the five military aspects of terrain (OAKOC) to consider fully the unique aspects of urban terrain. More than any other environment, the urban battlefield is dynamic. Depending on the street layout patterns, people can create or improvise manmade obstacles quickly to block narrow streets or these obstacles may not be a significant factor where streets are wider. Natural obstacles arguably pose less of a problem in urban terrain than in open terrain. Rubble caused by direct or indirect fire may impede both mounted and dismounted movement. In relatively rare circumstances, rubble may actually aid movement, such as when a building collapses across a canal, thereby providing access to the other side. These are the types of factors that make the urban environment dynamic.

S2s must analyze avenues of approach from all dimensions—air, ground, and subsurface—which generally requires separate overlays depicting air, ground, and subsurface avenues of approach. From these overlays, analysts should be able to

determine what size forces they can support, and advise the commander appropriately. This analysis should also allow the commander and the remainder of the staff to answer certain vital questions like:

- ❑ Are the avenues of approach linked?
- ❑ If so, where?
- ❑ What is the possible impact on enemy or friendly courses of action (COAs)?

Key terrain will vary based on the composition of the urban area and the nature of the threat. If the enemy prefers using snipers, then buildings providing good observation and fields of fire may be key terrain; if the enemy prefers strongpoints, then highly reinforced buildings (e.g., banks) that dominate intersections may become key terrain, and so forth.

Observation and fields of fire will be much more restrictive in an urban environment and the use of photos and imagery will be invaluable. The ability of the S2 and his section to do photographic and imagery analysis will be a significant factor in the quality and quantity of information they are able to provide.

Analysis of cover and concealment is also vital to success on the urban battlefield. Building characteristics, masonry, wood, brick, and even glass can all provide varying degrees of protection from observation, as well as the effects of weapons and munitions.

S2s, especially at battalion level, must be able to provide analysis of

Step	Concern	Details
1	<b>Structural Shape</b>	Structural shapes will be identified as square, rectangular, T-shaped, L-shaped, U-shaped, H-shaped, X-shaped, and irregular.
	Square	Designed so that all four sides are of equal size. Such designs are normally found in inner-city construction, smaller family dwellings, and in utility company maintenance buildings.
	Rectangle	Designed so that opposite sides are of equal size. The most commonly used shape in building construction.
	T-shaped	A modification of a square or rectangle with a wing extending from the center of the front or back of the building.
	L-shaped	A modification of a square or rectangle with a wing extending from one end or the other of the front or back of the building. A common design for family dwellings.
	U-shaped	A modification of a rectangle with a wing extending from each end of the front or back of the building. A modification of a U-shape is the multiple U, with more than two wings extending from the front or back. The U-shape is common to larger official buildings and hospitals.
	H-shaped	A modification of a rectangle with a wing extending from each end to the front and back. A modification of the H-shaped is the multiple H. The multiple H has more than two wings extending to the front and back.
	X-shaped	A center common area with T-shaped wings extending from the center of each side. X-shaped designs are found in some apartment complexes.
	Irregular	Buildings that do not fit traditional designs such as the Pentagon, religious structures, sports arenas, and permanent fortifications.
2	<b>Structural Face Designation</b>	Once the shape has been determined, the structure's main entrance is located and designated "white." If none of the building faces are identifiable as the main one, the commander will designate a face as white. Once done, the other faces will be color-coded in a clockwise manner with the white face serving as the base. While facing the white face, progressive faces will be designated as red, black (rear face), and green. For irregularly shaped structures the white face will be designated and the remaining faces color-coded. Any report addressing this structure will include the direction the sides take relative to each other. An example of color-coding and shape follows. <b>EXAMPLE:</b> "Irregular, white face one, white face two right, red face, black face, green face." This describes a pentagon-shaped irregular design.
3	<b>Measurement of Side Lengths</b>	Once the structural faces have been color-coded the shape, face color, and dimensions of the respective sides will be given. For irregularly shaped structures the same procedure is used with the addition of direction the sides take relative to each other. Send measurements as feet, length first followed by height. <b>EXAMPLE:</b> "Rectangle, red face 20 by 30."
4	<b>Numbering of Floors</b>	Floors will be numbered from "1" beginning with the ground floor. (Basements and other subterranean areas are addressed later.) Roofs, floors, attics, porches, balconies, chimneys, stairs, fire escapes, and other substructures will <b>not</b> be numbered but designated as what they are. Once the structural shape, face, and measurements are reported, then report using face, floor, and any additional information. <b>EXAMPLE:</b> "Black face, three, patio and fire escape."
5	<b>Numbering of Windows or Openings</b>	Windows will be designated "window," doors as "door," and all other openings as "opening." Designate from left to right as "Alpha, Bravo, Charlie, etc." <b>EXAMPLE:</b> "Window Alpha"; "Opening Delta."
6	<b>Numbering of Basements and Other Subterranean Levels</b>	Sub-basements, tunnels, or vaults may be dug deep into the earth and provided multiple subterranean levels. Such structures will be designated one at a time and given an alpha designation (first level = Alpha, second level = Bravo, third level = Charlie). Additionally, the type of structure or equipment on a given level must be identified as in the example below. <b>EXAMPLE:</b> A basement will be designated basement. "Sub-basement 'Alpha' parking garage." "Tunnel 'Charlie' gas pipeline." "Vault 'Delta' with electrical conduit tunnel." (Reflects a vault on the 4th level below the street level and that it has electrical conduits or lines running through it.)

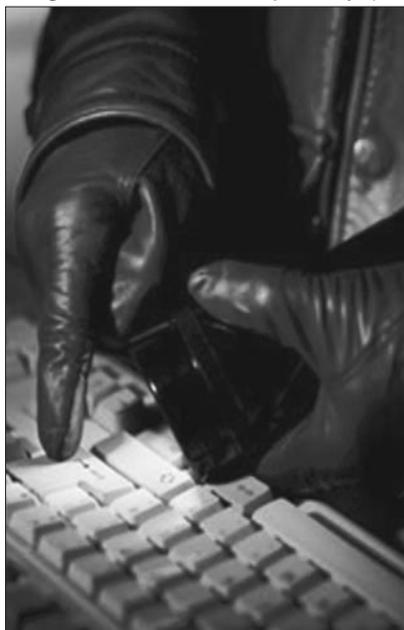
Figure 2. Details of Structural Labeling.



**by Chief Warrant Officer Two  
Bobby Allen**

*The views expressed in this article are those of the author and do not reflect the official policy or position of the 902d Military Intelligence Group, U.S. Army Intelligence and Security Command, the Departments of the Army and Defense, or the U.S. Government.*

U.S. counterintelligence (CI) elements must refocus to defend against the rapidly expanding cyber-intelligence collection threat. The cyber-revolution in military affairs has already started, before even a consensus on its definition has been reached. Earlier policies of risk-avoidance and placing too much emphasis on personal privacy at the expense of national security have degraded intelligence potency and hampered traditional CI efforts. After 11 September 2001, however, U.S. citizens now seem more willing to concede that privacy matters less than an aggressive and effective intelligence collection capability (in-



cluding CI activities) to combat the new face of terrorism. If the cultural and legal trend of returning to a national security focus continues, aggressive human intelligence (HUMINT) collection that goes after real secrets, and CI operations that genuinely exploit foreign intelligence and security services (FISS) may return.

### **The Threat Is Sophisticated**

Today's spies practice much more sophisticated methods and employ the latest technologies to gather and transmit massive volumes of our most sensitive information on a much wider variety of targets. FISS can and do leverage distributed cyberattacks routed through many countries using a wide variety of tactics and techniques, making it nearly impossible to state with certainty that any particular attack originated from a particular threat. Over time, computing power will completely overwhelm our ability to comprehend, let alone protect against, the exponentially expanding vulnerabilities created with new technologies. It is imperative that CI stays ahead and avoids technological surprise—

*...the unilateral advantage gained by the introduction of a new weapon (or the use of a known weapon in an innovative way)...against an adversary who is either unaware of its existence or not ready with effective countermeasures....<sup>1</sup>*

The intelligence community must embrace new technologies, carefully selecting those that best suit strategic intelligence purposes. Perhaps the best method to maintain compartmentalization and still

maximize the use of new technologies is to recruit small groups of highly specialized technicians to explore each technology potential from both a defensive perspective (what can the threat do to us?) and for possible offensive operations (how can we use this against the threat?).

### **The Insider Threat**

The greatest threat is from trusted insiders with placement and access to highly sensitive classified information. It is a relatively simple task to plug in a miniature data-storage device and save hundreds of megabytes of classified data they can easily smuggle out. It is equally easy for an insider to save this data to floppy disks, compact discs with read-only memory (CD ROMs), or even to another hard drive they brought in themselves. Unlike most other crimes, it is technically possible for a spy to encrypt, hide evidence using stenography, or both, and even completely delete all traces of evidence that was once on media.<sup>2</sup>

CI can conduct operations to invent new ways of detecting and responding to this type of attack. Modern security devices cannot replace traditional security practices such as background checks, awareness training, physical security, and internal investigations. A dramatic demonstration can be had by any company willing to hire a person or agency to attempt to infiltrate and discover information about their own company. Within days, an individual can gather information from the Internet, use fake identification to gain employment, observe passwords, and access sensitive information.<sup>3</sup> There is no easy solution to preventing

this kind of threat; enforcing strict security policies and providing awareness training with random spot-checking appears to be the best compromise solution for now.

## **We Are Our Own Worst Enemy**

Political policies and social beliefs since the Reagan Administration have resulted in a win-win situation for FISS. The policy of recklessly declassifying information, along with our cultural penchant for sharing sensitive but unclassified information, combined with our institutional migration to put everything on the Internet for ease of data dissemination, have combined to make collecting on the United States terribly easy. The hampering of HUMINT and CI operations and investigations in the name of privacy have permitted untold numbers of FISS agents to operate unimpeded for years.

## **The Networked Vulnerability**

Isolating secure systems from nonsecure systems, enforcing evolving “best practices,” using strong physical security, and constantly monitoring networks for anomalies can reduce the networked threat. *“The head of the Computer Emergency Response Team (CERT) once estimated that well over 90 percent of all reported break-ins were made possible because hackers could exploit known but uncorrected weaknesses of the target system.”*<sup>4</sup> Wherever there is the possibility of crossing unclassified with classified networks through negligence or willful intent, the remote attack is possible. Like criminals, FISS will continue to seek ways of gaining unauthorized access to sensitive networks simply because there is very little to lose in trying.

The Federal Bureau of Investigation (FBI) is investigating a record number of espionage cases because *“if there is a way to make a criminal’s job easier and safer, he*

*is going to use it.”*<sup>5</sup> Although it may be a better method to spot, assess, and recruit insiders, the novel methods to access information remotely have much greater potential than just having a spy steal files. The *“use of cryptographic hardware tokens to authenticate users when logging into systems and networks”*<sup>6</sup> would tremendously increase security when implemented with subnetting to isolate internal access to networked information.

Often networks are very complicated and require a great deal of time and understanding to evaluate their vulnerabilities properly. We should only permit the people with the right training to do this job, essentially creating a specialty within a specialty. Random, unannounced spot-checking would ensure that administrators and users have not changed configurations, compromising security for convenience or reliability. Here CI can play a role in detecting network intrusions by creating systems or networks that appear attractive to a networked attacker to learn their methods of intrusion, or other technical detection operation. However, even with the latest network firewalls, intrusion detection systems, virus scanners, encryption, compartmentalization, and security policies, vulnerability exists anywhere there is a connection to the outside world.

## **What To Do**

The Army must quickly define the role of CI in combating the cyber-intelligence threat and implement policies. Neither the U.S. Government nor its civilian experts alone can stymie the terrorist and FISS cyberthreat. The task of protecting U.S. information systems and other critical infrastructures requires the combined effort of the best minds of civilian industry, military, government, think-tanks, and academia. The National Infrastructure Protection Center (NIPC) has the responsibility to protect critical infrastructure from

all threats; CI is only a portion of that responsibility. The current reorganization underway of the FBI by its Director Robert Mueller, III, is an excellent model for Department of Defense (DOD) CI assets to define and implement changes necessary to thwart the ever-increasing cyberthreat.

The U.S. Army Intelligence and Security Command (INSCOM) created the Land Information Warfare Agency (LIWA)—now redesignated the 1st Information Operations Command (Land)—to support the ground commander in information operations (IO) and information warfare (IW). The mission of 1st IO Command (Land) is broad and overarching, and often conflicts with that of other agencies providing similar services. However, the creation of LIWA and now the 1st IO Command demonstrates the migration toward a more comprehensive assessment and defense of our information systems, in which CI will play a vital role. The 1st IO Command is still in the formative stage and requires time to carve its niche in the much larger IW landscape.

The trend toward increasing the number of special access programs (SAPs), highly sensitive projects that require exceptional security measures, is perhaps the best approach. CI personnel assigned to support a SAP could call upon the collective resources of highly skilled teams of area-specific cyber-CI specialists to protect these most sensitive projects. As the scope of what needs protection and the number and complexity of technologies increase, so should the number and specificity of cyber-CI assets increase to deter, detect, and potentially exploit threat FISS activities. According to Bruce Schneier, *“...as more and more aspects of our lives move into cyberspace, the demand for cyberspace security (and hence the demand for these experts) increases.”*<sup>7</sup> This “flex-up” concept maximizes the use of currently avail-

able CI resources and provides for economy of force during the continuous expansion of technology and threat.

Another approach to consider would be to centralize cyber-CI assets in regional centers. We could collocate them with other national cyberintelligence investigative and operational units.

To cope with the emerging cyberthreat, the CI program will have to reorganize to meet this new demand. First, an immediate infusion of CI personnel is necessary to fill the traditional positions neglected for many years. Secondly, CI agents should first serve in assignments at lower echelons to indoctrinate them into the system in which they will serve. This entry-level period is necessary to evaluate and assess the agents, as well as to provide them an opportunity to develop the vocabulary and organizational understanding to run investigations more effectively. Lastly, CI must task-organize to concentrate on the skills and techniques necessary to accomplish a particular type of highly specialized mission to counter the evolving threat. Each CI assignment should last many years, and units should tailor them to their particular missions. The role of HUMINT collector should not be a responsibility of CI agents. These changes would go a long way to refocus CI to take up the new task and forge a new path in the cyber-landscape but many other changes will also be essential.

Once we implement policy, the next basic building block is training. Therefore, the Army should implement cyber-CI training as a core competency of CI at all levels. CI agents must be as familiar with cyber-methodologies as they are with traditional FISS methods. Fundamental skills, such as properly imaging media for forensics or network analysis, should be taught to all agents. The basics of networking

and media storage should be understood and updated regularly. Today, CI has a few very specific areas of responsibility in the cyber-realm. Unfortunately, most CI agents lack the degree of computer savvy needed to conduct beyond-user-level forensics and lack even a fundamental understanding of networks.

Generally, system administrators are the only ones with the necessary skills to monitor networks and keep a lookout for indicators of cyber-espionage but, sadly, with many this is merely an implied secondary function. Most typically, a system administrator who suspects there has been a compromise of classified information will call the regional CI field office, then that office in turn will forward the media to a CI cyberlab for analysis. The lab uses tools and techniques that the CI field office could employ with minimal resources and training. "*Most learning is incidental*"<sup>8</sup> and people learn by doing without intentionally planning to do so. Pushing the basic cyber-investigations back down to field offices whenever possible better reserves the lab for unique or the more technical cyber-investigations, and keeps the field offices' abilities viable.

Defining the difference between system administrators, information security officers and CI agents can be relatively simple. Units should call in CI once they discover indicators of FISS involvement. Through traditional institutional and education methods (e.g., Subversion and Espionage Directed Against the Army [SAEDA] briefings), CI can continue to be instrumental in educating Army units on what these indicators look like, and foster a relationship encouraging communication. CI should continue to evaluate all reported incidents and try to prioritize these threats to best deploy assets and identify deficiencies in the program. A unit could assign a CI agent to a SAP to provide continuity and immediate evaluation of all anomalies discovered.

CI cannot support the intelligence community in a vacuum; we must instead wire it in to the latest security products, vulnerabilities, and even the techniques used by hackers. Institutionally, the Army must develop a higher level of connectivity to improve collaboration with other agencies focused specifically on the cyber-CI threat. It is not possible for any one agency to know about all possible cyber vulnerabilities, let alone pre-



pare an adequate response to all of them. The very essence of cyber-vulnerabilities and special tactics is the degree of secrecy they maintain. Once a vulnerability is known, CI must quickly develop countermeasures to eliminate or reduce its potency. Liaison is critical to establish a baseline of best practices and to ensure the countering of a recognized vulnerability at one agency throughout all other agencies. Finally, we should simplify sharing the specifics of special collection techniques, applications, and products.

### Final Thoughts

The bottom line is that the basic model of espionage remains the same, only the methods of collection, transmittal, and communication have changed. CI agents today must confront spies that potentially might never physically meet with their FISS handlers, as shown by the case of Robert Hanssen, one of the top CI agents for the FBI, who successfully spied for the Soviets and later the Russians. During this time, he continually sought ways to improve his electronic methodology. He used a Palm III personal digital assistant (PDA) to store and encrypt information that he would later give to his handlers. He used a simple technique to transmit *“data hidden on tracks not usually read by a computer.”*<sup>9</sup> Robert Hanssen combined this effort with many traditional non-electronic techniques, such as

markings, surveillance detection, and dead drops.

He even checked his own classified computer systems for his name, to include references made by Russia’s military intelligence agency, the Glavnoye Razvedyvatelnoye Upravlenie (commonly known as the GRU), and the *Foreign Intelligence Surveillance Act*<sup>10</sup> (FISA) court (the US court through which all surveillance’s must be approved) for indicators that he was under investigation. *“Hanssen was inventive, suggesting at one point that he trade in his Palm III for a wireless Palm VII, which he could use to send encrypted messages.”*<sup>11</sup> He had unique placement and access to a broad range of highly damaging information, and his knowledge of the methods to detect his espionage activity were unmatched. We can see that his basic methods of gathering and transmitting data are only the foreshadowing of the degree of sophistication to come.



### Endnotes

1. Campen, Alan D. and Dearth, Douglas H., Contributing Editors, **Cyberwar 2.0: Myths, Mysteries and Reality** (Fairfax, VA: AFCEA International Press, 1998), page 192.
2. Ibid, pages 168 and 169.
3. Schwartau, Winn, **Information Warfare**, Second Edition (New York, NY: Thunder’s Mouth Press, 1996), page 537.
4. Campen, Alan D., Dearth, Douglas H., and Goodden, R. Thomas, Contributing Editors, **Cyberwar: Security, Strategy, and Conflict in the Information**

**Age** (Fairfax, VA: AFCEA International Press, 1996), page 96.

5. Schwartau, Winn, **Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption** (New York, NY: Thunder’s Mouth Press, 2000), page 45.

6. Campen, Alan D. and Dearth, Douglas H., Contributing Editors, **Cyberwar 3.0: Human Factors in Information Operations and Future Conflict** (Fairfax, VA: AFCEA International Press, 2000), page 132.

7. Schneier, Bruce, **Secrets and Lies** (New York, NY: Wiley Computer Publishing, 2000), page 368.

8. Campen, Dearth, and Goodden, page 148.

9. McCullagh, Declan, “Old Spy, New Tricks” (Wired, 2001) at <http://www.wired.com/news/politics/0,1283,41950,00.html>.

10. Ibid.

11. Ibid.

*Chief Warrant Officer Two Bobby Allen is a Counterintelligence (CI) Special Agent assigned in investigative status and is the Information Assurance Security Officer for the Cyber-CI Activity. He received cyber-investigations training with the DOD Computer Investigations Training Program and is a Certified Information System Security Professional (CISSP). Following his nine years enlisted service as a CI Special Agent, some of his assignments as a CI technician have included Operations Officer for the CI section of the Joint Military Intelligence Battalion, Bosnia-Herzegovina, and Team Leader for the CI detachment at Eskan Village, Saudi Arabia. He is currently working toward completion of his Master of Science in Strategic Intelligence (MSSI) degree with American Military University. Readers can reach him via E-mail at [bobby.allen@us.army.mil](mailto:bobby.allen@us.army.mil) and by telephone at DSN 622-4875.*

## Errata for “The Case for the MI Ranger”

**MIPB** regrets editorial changes that impacted the intended meaning of Captain Thomas Spahr’s article in the April-June 2003 issue. In the **Change in DA Policy Needed** section, we printed: “...The exception to this policy is soldiers in the 96R and 98G MOSs. Some 96R soldiers can qualify for Ranger school; also, 98G soldiers can qualify if they sign up for the Special Forces.” This was incorrect; 96R soldiers *cannot* currently attend Ranger school, which was one of the major points of the article.

Also, the introductory paragraph should have read: “MI troops, in particular 98G Low-Level Voice Interceptor (LLVI) teams and 96R Ground Surveillance Radar (GSR)/Remotely Monitored Battlefield Sensor System (REMBASS) teams, can be an essential part of these combined arms reconnaissance efforts.”

We apologize to the author for these errors.

—The Editorial Staff

# CI in Information Operations: Enabling Operators and Defining Emerging Roles for CI in Army IO

by Chief Warrant Officer Two  
Jason L. Morton

*The opinions expressed herein are those of the author and do not reflect the official position of the 902d MI Group, U.S. Army Intelligence and Security Command, U.S. Army Intelligence Center and Fort Huachuca, Doctrine Division, Department of the Army, Department of Defense, or the U.S. Government. The author provided this article to provoke thoughtful discussion on counterintelligence and human intelligence activities and operations as they may pertain to information operations.*

Army counterintelligence (CI) awareness briefings have long identified espionage as the “second oldest profession.” Criminal trades have embraced 21st century technologies to further their efforts, as have the practitioners of espionage and intelligence. CI, the intelligence discipline charged with identifying, detecting, exploiting, and neutralizing foreign intelligence collection efforts, has begun to make strides into the 21st century information technologies. However, we are behind the other elements of Army information operations (IO) in defining roles, missions, and tactics, techniques, and procedures (TTPs) for how to operate in cyberspace, the newest military operating environment. Many talented and innovative CI Agents have begun developing ways CI can provide value and additional depth to Army IO and technical CI. Senior intelligence and CI operators, managers, and leaders must now further define, capture, and formalize these efforts into policy, doctrine, TTPs, missions, and the necessary support areas to bring CI fully into the 21st century and meet the threat in the new battlespace and operating environment.

Army CI and human intelligence (HUMINT) functions and elements exist at all operational levels; our thoughts and actions on support to IO should be no different. HUMINT is part of this discussion since CI and HUMINT use similar methodologies despite a distinct difference in mission and implementation. Many of the efforts in CI support to IO have crossed discipline lines and involve HUMINT missions, such as document exploitation (DOCEX) and machine language-translation technologies. From a HUMINT perspective, we have only scratched the surface. Therefore, one can challenge the HUMINT community to analyze its tasks and missions and provide input on how it can apply what it does to IO, in terms the IO community understands, and leverage technology to enhance mission efficiency. Currently, CI elements involved in IO only exist at a few of the U.S. Army Intelligence and Security Command (INSCOM) theater intelligence brigades and groups (TIBs/TIGs), and a few other separate elements. Most of these elements focus on investigations and investigative methodologies to support DOCEX of computer media. The Army should analyze and appropriately mature all functional areas of CI and HUMINT to take full advantage of technology and fully identify exploitable information in whatever environment or medium our adversaries operate.

Intelligence and CI are both vital support functions to IO under current doctrine as defined in **FM 3-13, Army Information Operations Tactics, Techniques, and Procedures**, but are not defined to the level of other “pillars” of IO. CI and HUMINT professionals working in IO and technology have developed very progressive and solid methodologies and TTPs to

accomplish emerging mission areas. The 902d MI Group’s Continental United States (CONUS) Sub-Control Office (SCO) Handbook has addressed computer investigations and Category 6 (Automation) Subversion and Espionage Directed Against the Army (SAEDA) incidents for several years. The Army is rolling most of that guidance into its G2 CI Investigative Handbook, with some additions from other theater SCOs and Department of Defense (DOD) Law Enforcement Counterintelligence (LECI) agencies.

The 513th MI Brigade and Defense Intelligence Agency (DIA) both have methodologies to support DOCEX of computer media. These references cover the “how” of investigations and operations at the most fundamental level—their existence is the basis for defining the requirements. These references have grown from a need by units in the field to document best practices for a recurring mission or task. Therein lies the requirement. Our adversaries are presenting a threat or operating in a new environment in which we need to enter and operate to accomplish our respective intelligence disciplines’ missions



Although agents in the field have developed some great TTPs, current doctrine, policy, and guidance are scarce concerning CI and HUMINT as they relate to IO. We must fill in the gaps to ensure these TTPs can be effective. Without policy, doctrine, and the senior- and executive-level programs and staff officers to support these efforts, they will suffer. Mission efficiency degrades while operators are working to synchronize missions, define standards across commands, and the other tasks normally handled by program offices and staffs.

Once we have defined the basic requirements, the Army must think them through fully in terms of doctrine, training, leader development, organizations, materiel, personnel and facilities (DTLOMS-PF), perhaps using an integrated concepts team (ICT) to do so.

*Doctrine Note: A working CI and HUMINT ICT has existed for years; the author intended merely to explain the process to the readership.*

Personnel issues are the cornerstone to all other factors regarding this issue. A critical component for success of technology-based IO is a program to identify, recruit, train, retain, and provide career management for operators. Additionally, such a program must include the identification of mission areas, elements, training, and other factors to develop these capabilities fully for overall benefit to the Army. We must identify and specially manage a core cadre of subject matter experts and technically qualified personnel outside the traditional Army models to explore and establish these processes. The reason for this special management is that most assignments are from 24 to 36 months, after which personnel rotate to different operational level assignments. For CI, this normally equates to a tactical-to-strategic-to-tactical cycle. Since there are no defined requirements for missions spanning the

operational levels, there is no real opportunity to allow the Army assignments model to “grow” or “spread the knowledge” of these soldiers. The Army is not optimally using the money for training and the soldiers’ experience, since 24 to 36 months out of the technology field renders one’s skills, training, and knowledge ineffective in the operating environment. The current trends in personnel rotations and transitions will continue to hinder the efforts of transformation and developing a set of programs to support commanders and operators at all levels. Stabilizing the right people (with the right skills and abilities) to develop the DTLOMS-PF considerations and follow-on recommendation documents is critical to providing relevant CI and HUMINT to the Army.

The use of technology enhances all four functional mission areas of CI—investigations, operations, collection, and analysis and production. We also need to take into account our adversaries’ use of these technologies. HUMINT, as well as CI, needs to embrace technology as a tool fully and be prepared to use and exploit the employment of technology by our adversaries. These technologies currently exist or are emerging at the national and strategic levels. However, CI and HUMINT soldiers trained in the operation and exploitation of technology and assigned at all levels of the Army will only enhance the quality of the intelligence we provide to commanders and operators at every level. The nature of the threat and the locations where we react to the threat and engage our targets are not supportable by small, centralized elements of specially trained operators.

With an understanding of technology, intelligence discipline fundamentals, supported unit mission, and their interrelations, both the technical CI agent and HUMINT specialist can conduct tasks in support of an all-source effort to support a local commander. The technical CI agent

could conduct a counterespionage investigation relating to foreign intelligence and security services’ use of digital methodologies and computer network operations. Meanwhile, a technical HUMINT specialist can execute digital media exploitation as a subdiscipline of DOCEX under existing DOCEX TTPs, authorities, and reporting procedures. At an appropriate time and after suitable analysis, this data may support efforts to protect our information and computer networks through Army Computer Emergency Response Team (CERT) computer network defense efforts, additional CI or HUMINT operations, or form the basis for computer network operations target development. To reach the point where this is a reality, we must challenge ourselves and change prohibitive mindsets, practices, and outdated policy. The Army must do all of this while maintaining security, need to know, and sight of who we are supporting and why.

The nature of the operating environment and the threat require us to ensure the new technical and administrative methodologies allow for speed. Espionage and other collection operations are very hard to investigate, because by their nature they are secretive and often applied with varying degrees of stealth. However, we cannot use this rationale as an excuse to spend two months on an investigative subject’s computer hard drive to determine if he was hiding information on it. A trained CI agent using media forensics technologies—coupled with the elements of espionage and known cases, incidents, and facts, as well as other intelligence—should be able to produce information in a matter of hours or days to be considered usable intelligence. In the realm of digital media exploitation, network incident investigations, and reactive CI operations, the timeline needs to be just

*(Continued on page 42)*

# Nonpassive Defense of the Army's Computer Networks

by Thomas G. King

Imagine bringing the most powerful nation in the world to its knees without firing a shot. Imagine rendering the most powerful military force in the history of the world impotent without crossing your own border. Far fetched? According to a federal government White Paper issued in 1998:

*The United States possesses both the world's strongest military and its largest national economy.... Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in nontraditional ways.... Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and nontraditional attacks on our infrastructures and information systems may be capable of significantly harming both our military power and our economy.<sup>1</sup>*

The Internet is a series of host computers that store information and relay communications. The Internet evolved from a United States Department of Defense program called Advanced Research Projects Agency Network (ARPANET) started in 1969. By the mid-1990s, the Army had discovered that the Internet was an excellent tool for conducting its business. Consequently, the Army developed multiple networks and systems containing routers and servers for electronic communications and provided desktop computers and Internet access to the vast majority of its workforce (military, civilian, and contractor). Since all of these computers can link to other computers literally anywhere in the world, anyone in the world has the ability to connect to Army computers.

Not only has the Army provided computers to its workforce but it has incorporated computers into its entire enterprise. Everything from weapons systems to payroll to morale, welfare, and recreation activities is dependent on computers. If these computers have access to the Internet, then potentially anyone in the world can access them. Before 1998, the Army did not have an effective method of detecting who was accessing these systems.

## Intruder Detection

The Army "got religion" in 1998 with an event that has been labeled "Solar Sunrise." In February 1998, the United States was facing a military confrontation with Iraq. Although that confrontation did not occur, during the period of preparation for war, hackers launched an attack against computer systems in the Pentagon. Although investigation ultimately discovered that the attack came from teenagers, the incident revealed that the Army did not have any effective way to monitor outside activity within its systems and networks.

The Army assigned the mission of creating an intruder detection system to what was then the U.S. Army Signal Command at Fort Huachuca, Arizona. The Army had already started to consolidate systems and networks, had created network operations security centers, and had just created a Computer Emergency Response Team (CERT) system to verify potential intrusions and protect against vulnerabilities. The Army Signal Command began to install intrusion detection systems, and set up organizations aimed at protecting the Army's networks and systems. The importance of network protection, among other things, has led to the creation of the Network Enterprise Technology Command/9th

Army Signal Command (NETCOM), the Army's single enterprise manager of telecommunications. Within NETCOM are the Army Network Operations and Security Centers (ANOSCs) and the theater NOSCs. The CERT system has also evolved under the 1st Information Operations Command (Land) to include the Army CERT (ACERT) and regional CERTs.

NETCOM has the mission of defending the Army's computer systems. It has installed and operates intrusion detection systems, and the ACERT works to protect against vulnerabilities to the system. This activity falls within the concept of passive defense. The Army has long ago accepted the fact that a passive defense is not an effective defense. The problem is to create a nonpassive defense of the Army's computer networks and systems within the constraints of the law.

## Nonpassive Defense Measures

What are nonpassive defensive measures? One possible measure is to use "honey pots." Honey pots are entities on a network or system that are likely to attract hackers or other intruders whose activities can then be monitored. There are many different types of honey pots, some purely defensive, while others are designed to gain information about the specific intruder. This type of honey pot is called a "research honey pot," and this function sounds suspiciously like counterintelligence and law-enforcement activity, not service provider activity.<sup>2</sup> Another method would be "attack sensing and warning." This practice involves detecting and identifying the characterization of intentional unauthorized activity within a network or a system, to include attack- and intrusion-

related intelligence collection. This attack sensing and warning could target both inside the Army's networks and systems or out in the Internet itself.

## Applicable Laws and Statutes

In considering a nonpassive defense, the Army needs to take into account a number of Federal statutes. The first is the so-called "Wiretap Statute," also known as the *Electronic Communication Privacy Act (ECPA)*.<sup>3</sup> Under the wiretap statute, the unauthorized interception of electronic communications and the use or disclosure of information obtained thereby is prohibited. This restriction applies to the content of communications. Exceptions have been carved out for law enforcement with proper authority and the intelligence community with proper authority. An exception has also been created for the provider of the computer service, who can intercept, use, and disclose information "incident to the rendition of his service or to the protection of the rights or property of that service."

The service provider exception does apply to parts of the U.S. Government but not to the entire federal government. In a 1999 memo to the Department of Defense General Counsel, the Department of Justice (DOJ) stated unequivocally that the DOD was a service provider. However, DOJ went on to say that components of DOD, such as law enforcement or intelligence, would not qualify as "service providers."<sup>4</sup> In other words, the job function within DOD would determine whether or not the activity or individual would qualify as a service provider. **AR 380-19, Information Systems Security**, sets up both the network and systems administrators and the CERTs as service providers. The next question would be whether the installation and operation of a honey pot would constitute a valid service provider mission. It does not. The pur-

pose of a research honey pot is to attract intruders so the administrator can track them and keep them under surveillance. Although one can argue that this activity is "necessary incident to" protecting the rights and property of the service provider, the author thinks this is a weak argument. Indeed, the DOJ has stated that "a Defense Department system administrator protecting his or her system may freely review both logs and content, and disclose the *initial* information reviewed to law enforcement..." [emphasis added].<sup>5</sup> Discovering and viewing initial hacker activity is within the scope of the service provider exception. A honey pot that did this could arguably be within the service provider exception. A research honey pot, which attracts hacker activity and monitors it, does not fall within this interpretation. It is therefore outside the protection of the service provider exception.

Another statute to consider at this point is the *Foreign Intelligence Surveillance Act (FISA)*.<sup>6</sup> Under FISA, a person is guilty of a criminal offense if he or she intentionally engages in electronic surveillance under color of law without a statutory exception or a court order. The statute contains a long and involved definition of what "electronic surveillance" is but the bottom line is that it means targeting individuals and watching them through electronic means. The statute applies to "any person" "acting under color of law." This includes government employees. There are exceptions for law-enforcement agents acting under court order or intelligence activities operating with FISA warrants or other statutory authority. Setting up research honey pots that target or watch specific individuals or activities or to monitor activity within the system could violate this statute. This statute is thus another factor to consider in a nonpassive defense.

If monitoring is to take place outside the system, then a third stat-

ute comes into play. This is the "Hacker Statute," the *Computer Fraud and Abuse Act*.<sup>7</sup> This statute would prohibit unauthorized access into a computer or computer system. If the Army seeks to carry on a nonpassive defense within another's computer or system, this would constitute a criminal offense by the Army. The service provider exception does not even contemplate this type of "defense."

## Conclusion

What should be clear at this point is that a service provider has a difficult job in clearing legal hurdles to carry on nonpassive defense. There are, however, organizations existing within the Army which have the ability to obtain legal authority. This would be law enforcement (specifically the Computer Crime Investigations Unit) and the Intelligence community. All of the cited statutes have exceptions for law enforcement and intelligence activities, provided they obtain the proper permissions. Therefore, as the Army looks to nonpassive defense, it needs to build an effective team between the service providers and the investigators, criminal and intelligence. It is this teamwork, exploiting the technical and legal capabilities of these different groups, that will lead to effective defense of the Army's computer networks.



### Endnotes:

1. "The Clinton Administration's Policy on Critical Infrastructure Protection," PDD 63, 22 May 1998.
2. Spitzner, Lance, **Honeypots: Tracking Hackers** (New York, NY: Addison-Wesley, undated).
3. *U.S. Code (USC), Title 18, Crimes and Criminal Procedure*, Sections 2510-2521.

(Continued on page 48)

# Intelligence in Support of Strategic Signal Units

by James R. Lint

*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 Departments of the Army and Defense, or the U.S. Government.*

The intention of this article is to foment discussion and debate to improve the MI Corps. It is not the author's intention to beat up soldiers stationed in S2 shops of signal units. By asking questions, we can often garner future improvements to doctrine and utilization of MI soldiers.

Most of us would admit that it is traditionally the S2, particularly in combat arms units, who brings intelligence to the commander, especially intelligence pertaining to the unit's mission. After all, it is normally the S2 who—

- ❑ Ensures intelligence readiness.
- ❑ Supervises the conduct of the intelligence tasks.
- ❑ Performs intelligence synchronization.
- ❑ Provides other intelligence support such as: orders production, products, updates, advising the command, and MI-unique deconfliction.
- ❑ Coordinates for counterintelligence (CI) activities.
- ❑ Supports security programs.

## Background

With most of the above responsibilities, those with experience in combat arms units would definitely state the S2 should provide that information to the supported commander. However, in a signal unit, especially a strategic signal unit, the responsibility seems to shift away from the S2. Some S2s might respond that “*we do not have the training, time, or people.*” More dip-

lomatic responses might include “*We are not staffed for this,*” or something similar. However, the military and moral responsibility remains; it is imperative that there be no retreat from the cyber-battlefield.

Many of us have often seen S2s become irritated when the G2 passed intelligence directly to a brigade commander. (They are often officers of equal rank who live in the same neighborhood and attend the same meetings.) This sometimes “blindsides” an S2 who did not have the information. Most would agree that the normal process is for intelligence—especially intelligence affecting the command—to flow through the command S2. However, often in computer network defense (CND) or cyber-matters, the S2s are not in the loop. Should they be the channel for cyber-intelligence or CND? Who should notify the commander that a node or router is under a hacker attack? Is the S2 in the “threat to systems” loop? Does the S2 provide the commander with an intelligence summary (INTSUM) that covers cyber-intelligence? Do military intelligence (MI) and S2s have the mission to conduct cyberthreat analysis in strategic (theater support) signal units? Are we actually ready to support a network-centric Army?

Many will also say that the outstanding work done by the regional computer emergency response teams (CERTs), Army CERT, and the 1st Information Operations (IO) Command (formerly the U.S. Army Land Information Warfare Activity, or LIWA) is an intelligence job, and is all the intelligence product needed, desired, or required for support to a signal brigade. Should that information go through the S2 or directly to the S3 or network operation center?

Should there be long-term analysis of cyber-indications and warning (I&W)? Should that information go to the S2 or S3? This author believes that there must be a change in the S2 office for the S2 personnel to support operations better, or a decision must be made to give up the fight at the Brigade S2 level and “hope” for success. S2 soldiers and personnel require more training specifically targeted to support cyber if they are to be effective in this fight. We see the Chinese military thought in a paper on “Information Warfare,” by Senior Colonel Wang Baocun and Li Fei published in *Liberation Army Daily*, 13 and 20 June 1995. The authors work at the Academy of Military Science, Beijing. There have been a few good papers translated and put in public domain about the Chinese “new ideas in waging war.” We must be prepared for new methods in future wars. Luckily, the Chinese have put their ideas in paper and it is in public domain.

*Editor's Note: See the article by Timothy L. Thomas on Chinese Information War Theory and Practice in this issue of MIPB.*

## Lack of Specialized Training

The lack of specialized training is not unique. Often, young intelligence analysts (military occupational specialty [MOS] 96B) arrive at aviation units, where they must suddenly learn about air mobility corridors. (This is not something taught in great detail in their basic courses; they must learn it through unit training for the unit's specific mission.) When the junior 96B reports to an engineer unit, he must learn about engineer-specific tasks, such as river crossings, also in greater detail. We also see young 96B soldiers

move to strategic signal unit assignments where they must then learn the cyber- and signal threat. The U.S. Army is a tactical and strategic Internet service provider (ISP); however, our junior intelligence analysts are not trained for supporting the signal or cyber missions.

In school, S2 personnel learn a bit about enemy electronic warfare (EW). They do not learn anything about prediction or I&W of a cyberattack on a strategic signal unit—mostly because there are no tracked indicators; the worldwide web facilitates global reach and anonymity with no advance notice of intent to perform malicious acts. If an infantry battalion in the 2d Infantry Division is attacked and there were no intelligence warning, that would be an “intelligence failure.” When a strategic signal unit is attacked and the systems administrations must take machines offline, reconfigure them, or reinstall all software with overtime costs and lost mission time, that is a cost not only in money but also in mission readiness and effectiveness. Given the intelligence resources and support dedicated to protect the unit, why should we view this event as anything other than an intelligence failure as well?

Many people question whether the S2 or intelligence analyst should be involved in the cyberthreat development work, which many often dismiss as “too hard to do.” Should we therefore withdraw from producing threat information? The S2 is doctrinally responsible for producing threat estimates and advising the commander on the types of threats that can attack the unit. Therefore, MI and the S2s in strategic signal units must undergo self-training to develop an understanding of the threat and to be able to discuss it intelligently with the supported commander. S2s often see this risky as when their raters are highly knowledgeable in cyber-matters. By fall-

ing back to the status quo, the S2s do not have to worry about making errors due to lack of knowledge about the cyber-world, and they have more than enough missions without adding a “new” threat dimension of cyber-warfare. Signal units do not have many MI personnel. Often the battalions have extra signal soldiers but few MI soldiers, so signal soldiers have to learn a new career field and do the best they can. Primarily, they must perform the security manager and physical security missions. The brigade-level S2s will be busy enough with personnel, information, and physical security, leaving no time to learn or develop tactics, techniques, and procedures (TTPs) aimed toward a significant threat to signal units: cyber-warfare. While the Army discusses Transformation, the computer and cyber-world have actually transformed. Has the U.S. Army kept up with the ever-changing technology and threats to that technology? Clearly not. More importantly, is it the responsibility of the signal unit S2, or is this level of detailed and specialized knowledge more appropriately the domain of the aforementioned strategic assets?

One must be realistic and consider that not every analyst needs this training; units’ training budgets are already strained and time spent in training is time that the analysts are not working in their field. Having discussed the issues, the next step is formulation of viable alternatives.

**Distance Learning.** Analysts and other personnel assigned to a field that is radically new for them (cyber-warfare), regardless of age, could obtain certification and training via distance learning from either the Intelligence or Signal Centers. This seems to be the most cost-effective method, as web-based learning sites can easily update with new technologies.

## Conclusion

Whatever method or combination of methods are chosen, it is vital that the Army deliberately addresses the threat of cyber-warfare and properly trains intelligence personnel on this

threat. At a recent briefing, the Deputy Commanding General, U.S. Army Network Enterprise Technology Command (NETCOM), discussed situational awareness for the commander. As MI professionals, we must always ask what we have done today to improve the commander's situational awareness of all threats. At the same time, plan on improving the commander's situational awareness in the future.



*James Lint (U.S. Marine Corps and U.S. Army, Retired) is an MI Corps Association (MICA) MI Corps Mentor. He has 25 years of MI experience, covering the*

*USMC, U.S. Army, contractor, and civil service. He is the moderator of two list-servers: S2\_online and the Army Counterintelligence Discussion Group ([http://groups.yahoo.com/group/S2\\_online/](http://groups.yahoo.com/group/S2_online/) and <http://groups.yahoo.com/group/ACIDG-L/>). He is currently the Deputy Director for Intelligence and Security, 1st Signal Brigade, and was the Korea Information Assurance Manager-Intelligence, with the U.S. Forces, Korea. J/G2 (USFK/8USA), Korea. His Military Assignments included Security Manager, 308th MI Battalion; Current Operations Noncommissioned Officer in Charge and S3 NCOIC, 524th MI Battalion; First Sergeant, Operational Support Detachment (OSD), 202d MI Battalion; CI Special Agent and Human Intelligence Assessment Team Chief, Joint Operational Support Element, J2, Joint Task Force 160, Guantanamo Bay, Cuba.*

---

## CI in Information Operations

---

*(Continued from page 37)*

as fast. Proactive CI operations may work on a more traditional timeline since they are not designed to respond to an immediate threat. However, the environment of these operations—cyberspace—epitomizes the asymmetrical and fast-moving field in which we must operate.

Technology is a small part of this speed. We must streamline administrative and management processes to enable the operators. The approval authority for most technical CI operations is the Secretary of the Army or higher. Dedicated staff sections that would rapidly staff operational plans would help, as would a cyber SCO to manage, deconflict, and synchronize streamline operations for the Army Central Control Office (ACCO) and the Army G2. The management is critical because there is no worldwide visibility on Army CI interests in cyberspace. Dedicated “tactical” analysis is also crucial. The Army Counterintelligence Center (ACIC) produces some great products concerning IO from a CI perspective. However, the ACIC is the Army's

strategic CI analytical shop. The Information Dominance Centers at the TIBs/TIGs are better suited to provide tailored, relevant analysis to a theater and lower echelon commander. Changing how we investigate and operate is important but we must also change the supporting elements. Changing how we provide analysis to and manage those investigations and operations further enhances investigations and operations in support of the overall intelligence effort.

The Army is at a critical decision point in CI and HUMINT concerning technology and support to IO. Do we continue the status quo or bring CI and HUMINT into the fold on senior- and executive-level visibility and guidance on IO and technology issues? Formally stating requirements and implementing new and innovative ways to conduct CI and HUMINT operations in cyberspace and in support of IO will provide true value to Army intelligence. This requires policy, guidance, and programs in these areas. Radical changes are not necessary. Simply analyzing what we do now and modifying how and where we do CI makes a much more vi-

able intelligence discipline in support of all-source intelligence to support the Army's operations.



*CW2 Jason Morton is currently assigned to the Saudi Resident Office, Field Office Southwest Asia, 202d MI Battalion, 513th MI Brigade. He previously served as the Chief of Network Investigations and Future Operations for the Cyber-CI Activity (formerly Information Warfare Branch), 902d MI Group. He has served several assignments in Europe and is a graduate of Advanced Foreign CI Training Course (AFCITC), Computer Investigations Course for Special Agents (CICSA), Advanced CICSA (ACICSA), and several DOD investigative and technology courses. Readers may contact him via E-mail at [jason.morton@us.army.mil](mailto:jason.morton@us.army.mil).*

### Please Share Your Photographs

**MIPB** is always looking for good photographs of MI professionals at work. We would like action shots where possible and no “happy snaps.” Please take at 600 dpi or better and send the photo, a caption with a full description, and identify the photographer. Thank you!

# Bridging the Intelligence Gap in the Heartland: Evolving MI Roles in Support to Domestic Criminal Threats

by Major James Klotz and  
Lieutenant Colonel  
Michael French

*The views and conclusions in this document are those of the authors and do not necessarily present the official policies or positions of the Fort Riley Criminal Investigation Division Battalion, U.S. Army Intelligence Center and Fort Huachuca, the Departments of the Army and Defense, and the U.S. Government.*

The modern battlefield now extends to the heartland of the United States and into our own backyards. Clear distinctions between acts of crime and acts of war blur in the wake of these ruthless terrorist attacks. As we in the various intelligence communities respond to these now very real threats to homeland security, our nation calls us to perform many of our wartime missions domestically in support to law-enforcement operations. Performance of these wartime intelligence missions inside U.S. borders has, of course, raised several concerns. These concerns are not altogether new, having previously arisen during the Civil War and Vietnam eras.

Domestic military intelligence (MI) operations are defined procedures detailed in regulatory guidance, such as **Army Regulation (AR) 381-10, U.S. Army Intelligence Activities**. Since 1975, Executive Orders (EOs) have been in effect to provide our intelligence professionals with guidelines on how to perform their missions consistent with the legal rights and protections guaranteed to all U.S. persons by our **Constitution**. President Ronald W. Reagan issued *Executive Order 12333, United States Intelligence Activities*, in 1981, which is still in

force today. **Department of Defense (DOD) Regulation 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons**, implements *Executive Order 12333* within the DOD and sets forth procedures governing the activities of DOD intelligence components that affect U.S. persons. It states:

*The purpose of these procedures is to enable DOD intelligence components to carry out effectively their authorized functions while ensuring their activities that affect U.S. persons are carried out in a manner that protects the constitutional rights and privacy of such persons.*

The terrorist attacks of 11 September 2001 did not cause a change in the *EO*; however, they have caused the intelligence communities to re-evaluate the limits imposed on domestic intelligence operations that affect their missions. Additionally, the ramifications of these attacks did prompt a clarification of procedures by the Army's Deputy Chief of Staff (DCS) for Intelligence (DCSINT) (now the DCS G2); in particular, whether MI capabilities and resources might, in some way, be brought to bear in support of domestic law-enforcement operations. This article chronicles the initiatives of one unit's effort to combine the talents and resources of the Army's MI community with those of the Army's law-enforcement community.

## Doctrinal Issues

The events of 11 September serve to identify a doctrinal "gap" between the roles, missions, and responsibilities of the MI and military law-

enforcement communities. Despite both communities' increased emphasis on resolving these "disconnects," there remain a number of shortfalls and gray areas within Army-approved doctrine relating to police intelligence operations (PIOs), especially as it relates to the formalized processes for the collection of information and conduct of the Police Information Assessment Process (PIAP), and development of police intelligence products (PIPs). Given that the Army only recently (within the last five years or so) assigned military police (MP) and criminal investigation division (CID) elements the wartime tasks of police and criminal intelligence operations, this weakness in our doctrine is understandable. Doctrine often captures the lessons of the last "war." However, in this area, doctrine is progressive and incorporates lessons learned while the Global War on Terrorism is still on-going.

*Policy Note: Although doctrine has not traditionally addressed it, the U.S. Army Criminal Investigation Command (USACIDC) has had responsibility to "collect, analyze, and disseminate to affected commands criminal intelligence pertaining to threat activities...." in all of the last three versions of **AR 525-13, Antiterrorism**.*

*Doctrinal Note: The introduction of Police Intelligence Operations was not intended to replace Military Intelligence, nor to subsume traditional MI functions, duties, or responsibilities, nor to become a separate stovepipe organization. A PIO pertains to strategic analysis of operational and tactical police operations provided to the commander and staff for decision-making.*

This is not to suggest there is **no** doctrine relating to MI's role with respect to police and criminal intelligence operations. MI and law enforcement have been collaborating and performing these missions (and doing them well) for many years. Instead, the evolution of modern warfare has forced the Army to recognize the relevance of PIOs (and MI's contribution to these operations) in modern military undertakings and not simply their **combat support** relevance. This recognition is now evident across the entire operational spectrum, whether in peace-enforcement operations (as in the Balkans), in domestic force protection (FP) operations (in which we are now fully engaged), or on the physical battlefield (as in Afghanistan). There remains the need for a coherent police intelligence doctrine that adds analytic rigor to our familiar processes, generates useful police intelligence products, and communicates in terms supported commanders are accustomed to hearing.

*Doctrinal Note: It is precisely with this in mind that **ST 2-91.2, Intelligence Support to Installation Commander's Handbook on Force Protection, is under development.***

The Fort Riley, Kansas, CID Battalion, is attempting to address some of these doctrinal issues through a local initiative. The Criminal Intelligence Management and Integration Center (CIMIC) may have far-reaching consequences.

*Doctrinal Note: The following is a local tactic, technique, and procedure (TTP), not an approved doctrinal solution.*

Following 11 September, and with the active sponsorship of the 24th Infantry Division (ID) (Mechanized), the Riley CID Battalion initiated an effort to "mend the seams" in MI and criminal intelligence doctrine and TTPs, both within and among the MI and MP communities. The CIMIC's aim is to improve the exchange of

information and gain greater synergy between critical FP functionalities including installation-level actors (e.g., G3s, directorates of plans, training, and security (DPTSs), provost marshals, etc.) and federal, state, and local law-enforcement agencies (LEAs). To help facilitate this effort, the 24th ID (M) is taking a bold step forward into new territory. In particular, the Division G2 has attached an MI major (the co-author of this paper) full time to serve as the Battalion's S3 for the specific purpose of providing support to law-enforcement operations (not the typical MI S2 function). The expressed purpose of this first-of-its-kind arrangement is to apply time-proven MI analytical methodologies and techniques (e.g., link analysis, intelligence preparation of the battlefield [IPB], etc.) to operational law-enforcement efforts. In so doing, the Division believes this effort will improve the ability of CID to gather, index, integrate, and analyze criminal intelligence information for the purposes of thwarting crimes and catching criminals.

### Battalion CIMIC

Here is how it works. The Riley Battalion's CIMIC focuses on pro-

viding support to local commanders by organizing and integrating national, regional, and local police and criminal intelligence information. It also seeks to provide enough quality information to enable installations to form a coherent, full-spectrum response to threats posed by terrorism, hate groups, extremism, gang activity, and a related lack of discipline, including illicit drug and firearms trafficking and use.

CIMIC objectives are to—

- ❑ Improve criminal and police intelligence support to installation-level commanders and help them tailor their FP activities.
- ❑ Provide all the Battalion CID elements with a common operational picture across the 13-state Fort Riley CID Battalion's area of responsibility (AOR) (see Figure 1).
- ❑ Foster closer cooperation among local and regional LEAs.
- ❑ Develop better intelligence relationships with the MI community at each supported installation and its higher headquarters while trying to help make each installation safer and more secure.

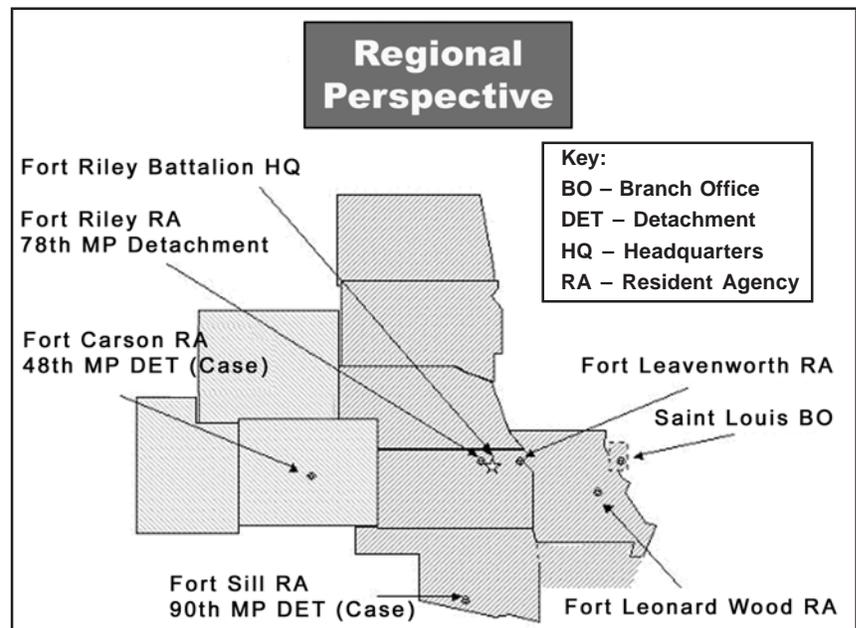


Figure 1. The Fort Riley CID Battalion's AOR.

Figure 2 depicts criminal intelligence relationships at the local, regional, and national levels. At the installation level, MP and CID operations are fairly well defined and practiced. Criminal intelligence operations at the national level are also reasonably well established and integrated. However, one cannot say the same of the regional police and criminal intelligence operations performed by the MPs and CID. The Fort Riley CID Battalion formed, equipped, and staffed the CIMIC to fill this regional intelligence gap.

After polling senior installation leaders across the Battalion's AOR, some common themes emerged. Among them was the view that although the CID provided excellent investigative support and was very well-connected to the local law-enforcement communities (provost marshal offices [PMOs], staff judge advocates, and local commanders), more work was necessary in

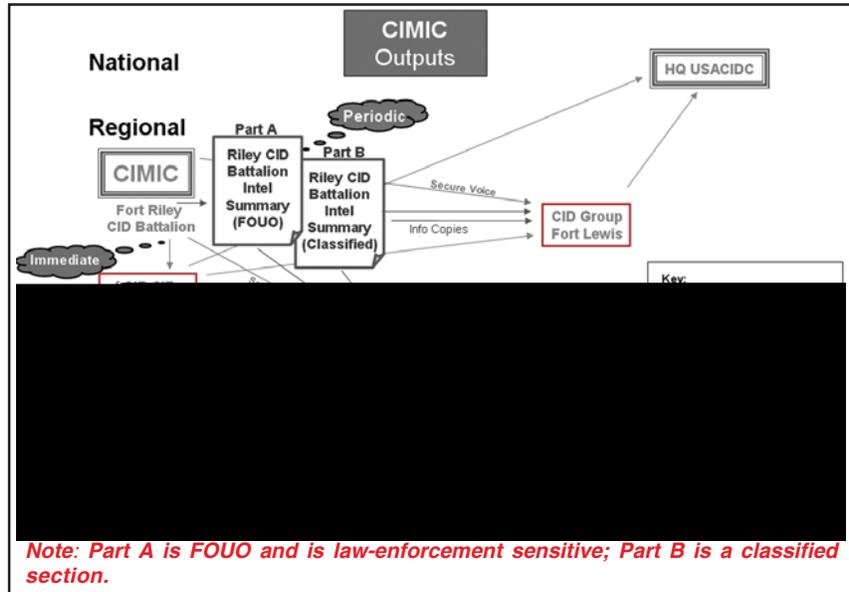


Figure 3. Information Flow.

the police and criminal intelligence-gathering and crime-analysis areas. Field commanders noted that they receive plenty of crime data but not enough useful information and analysis to support policy for-

mulation and decisionmaking. The CIMIC strives to provide the missing information and analysis.

Essentially, the CIMIC is an operations center for collecting, integrating, analyzing, and disseminating regionally tailored police and criminal intelligence information. By leveraging off-the-shelf technologies (e.g., personal computers, facsimile machines [FAXs], and Internet access) and local installation support—Fort Riley provides full-time Secure Internet Protocol Router Network (SIPRNET) access and MI manpower—the CIMIC acts as a CID regional criminal intelligence clearinghouse for the Midwestern United States. (To elaborate on this point, the CID directly distributes its criminal intelligence update to the FBI Joint Terrorism Task Force [JTTF], U.S. Bureau of Alcohol, Tobacco, and Firearms [ATF], and U.S. Drug Enforcement Agency [DEA] as well as the Kansas National Guard Bureau, highway patrol, and the Saint Louis Police Department. Indirectly, the installation CID Resident Agencies (RAs) distributed the update to each local community.)

The CIMIC enhances police and criminal intelligence support to installation-level commanders by

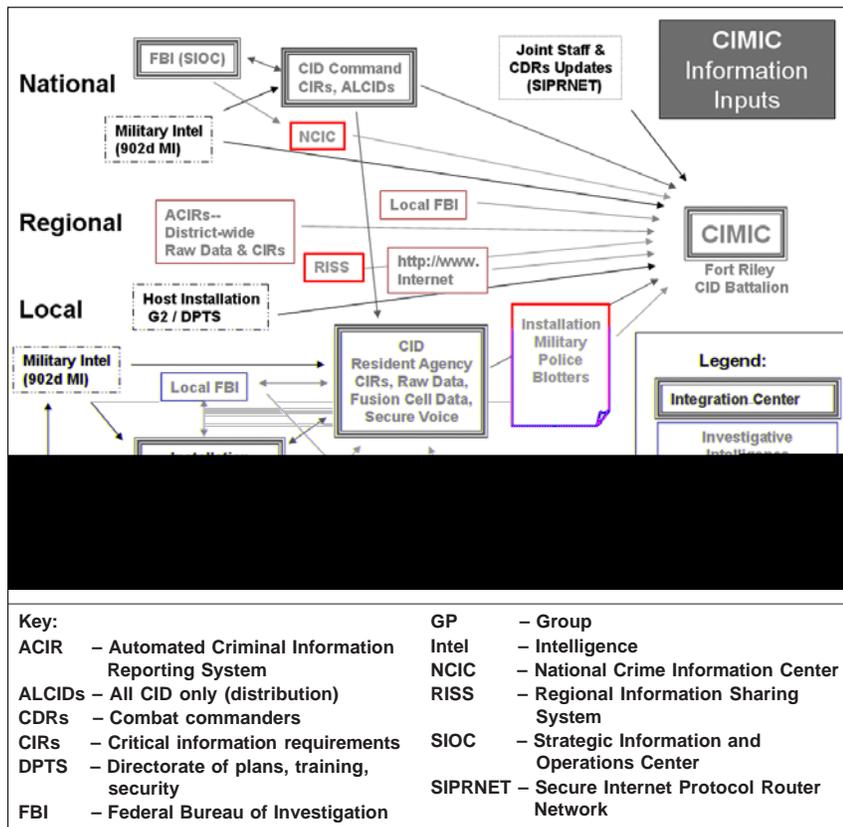


Figure 2. Criminal Intelligence Relationships at the Local, Regional, and National Levels.

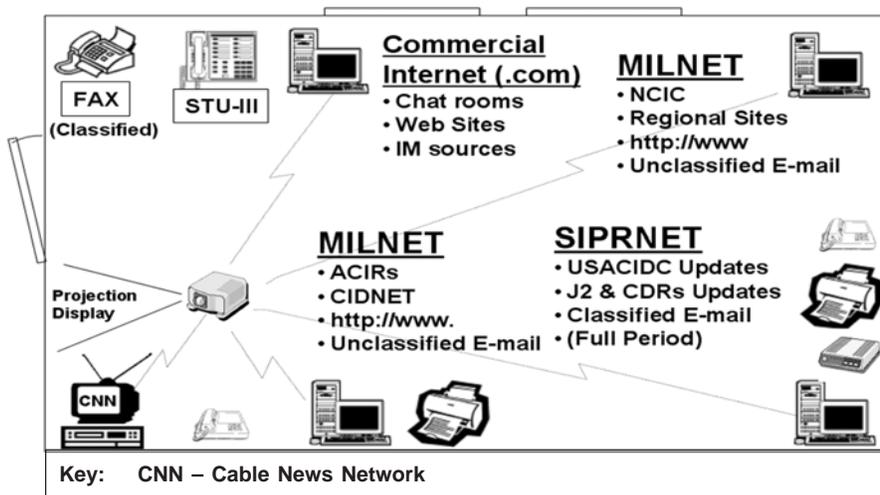


Figure 4. CIMIC Physical Layout.

publishing a two-part criminal intelligence digest three times a week. Figure 3 outlines the information flow.

The regional update section captures data relevant to the Battalion's AOR based on analysis driven by the commander's critical information requirements (CCIRs) and priority intelligence requirements (PIRs). The national update draws, from such diverse sources as the—

- ❑ Joint staff and combatant commanders' updates.
- ❑ 902d MI Group products.
- ❑ 24th ID (M) G2 summary products (U.S. Forces Command and III Corps input).
- ❑ CID secure Internet (CIDNET).
- ❑ U.S. Army Criminal Investigation Command (USACIDC) critical information requirements (CIRs).

The district update draws from reports provided by the RA criminal intelligence submissions and installation FP fusion-cell feedback, blotter reviews, local and regional FBI input, local 902d MI Group detachment input, and other raw-data analyses. Each intelligence entry cites the sources, and we generate and disseminate the product called the "criminal intelligence summary" (CRIM INTSUM) each Monday, Wednesday, and Friday.

The CRIM INTSUM goes to CID offices and group headquarters via

SIPRNET and secure-telephone-unit III (STU-III) facsimile (fax). CID offices use CRIM INTSUMs to "feed" installation FP fusion cells at their regularly scheduled meetings. At the same time, local CID representatives draw fresh intelligence information from local sources and forward it to the CIMIC to initiate its next collection, analysis, and integration cycle.

### Battalion CIMIC Configuration

Figure 4 depicts the CIMIC's configuration and capabilities including access to the SIPRNET, commercial Internet, and the installation's military network (MILNET). MILNET provides access to a usual host of capabilities, plus many essential Army information management (IM) systems to which the CID has obtained read-only access (e.g., Enlisted Distribution and Assignment System [EDAS], Total Officer Personnel Management Information System [TOPMIS], Defense Eligibility Enrollment Reporting System [DEERS], etc.). Access to other web-based systems is also available including the civilian Regional Information Sharing System (RISS) that provides a regional view of civilian criminal intelligence information. The CIMIC is currently connected to both the Middle-States Organized Crime Information Center (MOCIC) permitting access to, and information-sharing with, the other five regions

of the RISS network, and to the FBI's National Crime Information Center (NCIC) providing access to a computerized index of criminal justice information (including criminal-record historical information, fugitives, stolen properties, missing persons). Future capabilities may eventually include access to the Defense Finance and Accounting Service (DFAS).

### Conclusion

The Fort Riley Battalion's CIMIC is by no means a panacea for ameliorating doctrinal shortfalls in criminal intelligence operations. It does, however, serve to create conditions suitable for addressing some crucial challenges facing MI, MP, and CID elements as they respond to a rapidly changing battlefield environment. Through the CIMIC, the Fort Riley CID Battalion, in close cooperation with the 24th ID (M) G2, is striving to improve its criminal intelligence support to local commanders and to examine new directions for further improvement. Many issues remain, but the CIMIC's efforts serve to define them better and offer possible solutions.



*Major Jim Klotz is the S3 of the Fort Riley CID Battalion. He holds a Bachelor of Science degree in Physical Geography from the U.S. Military Academy. He has served in a variety of military intelligence assignments to include S2, 937th Engineer Group; Combat Operations Officer in the Battle Command Battle Lab-Fort Huachuca; and the U.S. Army Central Command (USARCENT) Intelligence Center during Operations DESERT SHIELD and DESERT STORM. Readers may contact MAJ Klotz via E-mail at james.klotz@us.army.mil and telephonically at (785) 239-8039.*

*Lieutenant Colonel Mike French is the Commander of the Fort Riley CID Battalion. He holds a Baccalaureate degree in Criminology from the University of Maryland, and Master of Business Administration and Finance degrees from Boston and Jacksonville State Universities. Readers may write to LTC French via E-mail at michael.french@us.army.mil.*

# Get Your Soldiers Ready For Deployment

by Command Sergeant Major  
Lori L. Brown

If you have been notified that you are deploying in support of one of the many operations in which our Army is currently engaged, welcome to the club. The companies busily prepare their units to load up their vans, jump on the "iron bird," and touch down in their new home away from home. Wait! What did the noncommissioned officer (NCO) support channel do to get the soldiers ready? Here are some ideas of how the 110th MI Battalion had our senior NCOs crack that nut.

## Promotions

All soldiers in our Army truly believe that they are going to get promoted. Every month before the 10th of the month, you process your semi-centralized promotion documents, turn in DA Form 3355, Promotion Point Worksheet, and every month you hold or participate in a promotion board. Each of our Sergeants (SGTs) and below put together their "I Love Me" books to hand-carry on deployment. The First Sergeants (1SGs) quality controlled (QC'd) each book to verify all pertinent data was there. This has saved our soldiers much pain and anguish. When the soldiers made the cut-off score, they knew that they made it. Their points are not suspended and they do not need to provide any documents to "prove" that they made their points after redeployment. We made sure that the soldiers would only have to go through this once. Our lower enlisted soldiers who compete for those ever-so-few waivers are also covered. Their 1SGs do not have to guess if they attended a school or completed correspondence courses, they **know**. Our commanders also know that they are selecting the best-

qualified and the right soldiers for promotion.

Equally important are the Centralized Promotion Boards. The odds of deploying during one or more of the centralized boards are pretty good. We ran into the Sergeant Major (SGM) and Master Sergeant (MSG) Boards during the 110th's deployment. We ensured that all the Staff Sergeants (SSGs), Sergeants First Class (SFCs) and MSGs had a Department of the Army (DA) photograph taken before deployment. We did this early on so that the senior NCOs had an opportunity to QC the photos and provide feedback to these NCOs. Then we turned in the photos to the Soldier Support Battalion.

The remainder of this process becomes easier as the U.S. Total Army Personnel Command (PERSCOM) gets all the Official Military Personnel Files (OMPFs) online. We were not this fortunate. The SSGs, SFCs, and MSGs reviewed and updated their DA Forms 2-1, Personnel Qualification Record (PQR), and Enlisted Record Briefs (ERBs). Each of our NCOs, from lowest to highest, received their OMPFs and brought them on deployment. The 1SGs made the OMPF an inspectable item with the soldier's readiness deployment file. We did run into the problem of having an antiquated microfiche reader but the process worked. We were confident that the NCOs would be able to process the required records and submit an accurate PQR.

The one thing we should have done differently is work with the SGTs and SSGs early on before deployment, as soon after notification as possible. Most of their OMPFs needed a lot of attention, and those NCOs are not really sure what documents the OMPFs should contain. We could have solved it

with an Noncommissioned Officer Development Program (NCO DP) and then one-on-one sessions with the junior and senior NCOs. This works very well when the unit is scheduled for a rotation in a theater such as Bosnia-Herzegovina, Kosovo, or the Sinai. However, we have also executed this model in support of Operation ENDURING FREEDOM activities as individual backfill and unit deployments. The command sergeant major (CSM) and 1SGs can certainly work the schedule with the local photographic support section on the installation to get this imperative fulfilled.

## Counseling Files

The company put the soldiers' counseling files on the orderly rooms' packing lists; it was vital during the deployment since the soldiers did not all deploy with their pre-deployment supervisors. There were so many instances where a soldier's previous counseling was critical to making decisions about that soldier's assignment within the task force or other decisions. We continued with our internal policy of providing monthly developmental counseling for the junior enlisted soldiers and quarterly counseling for the NCOs. The soldier's entire personal information file was essential to this success. The entire counseling file was also critical for those specialists and sergeants in the primary zone for promotion who did not receive recommendations. The counseling files assisted us in writing awards, noncommissioned officer evaluation reports (NCOERs), recommendations for Audie Murphy and Major General Aubrey "Red" Newman boards, promotions, and even disciplinary actions. The counseling file is a must for the company-packing list.

## NCOERs

This area can turn into a crisis-action team situation and spin out of control in a hurry. Close out the NCOERs in advance of deployment where possible. We task-organized the Battalion in August for our November deployment. This gave us not only three months to “team-build” but also some additional time at home station to close out the NCOERs. In the Battalion, we pretty much controlled our own destiny; however, we had more than 50 augmentees from seven different battalions. Not all of those NCOs received change of rater reports before departing their respective home stations. Needless to say chasing NCOERs down kept the Personnel Sergeant, the 1SGs, and CSM busier than we intended during the first weeks on the ground. The lesson learned here is for all of us to do the change-of-rater reports before NCOs depart for any deployment.

## Task Organizing

As I mentioned briefly above, we task-organized for the mission three months prior to hitting the ground in Kosovo. This greatly enhanced our team-building efforts. It was important for the company chains-of-command to learn the names and faces of their “new” companies. We resolved many administrative tasks early on by these efforts. Our task organization date preceded our mission readiness exercise (MRE) by approximately three weeks. After completing the MRE, we remained in our task-organized structure. Now halfway through our deployment, we are planning for the reorganization of the Battalion back at our home station.

The reorganization will be extremely turbulent. We have received more than 50 additional soldiers since our departure. We essentially have two additional platoons to stand up in our general support company. It was imperative to reorganize one of the two direct support companies to allow it to train for its upcoming Joint Readiness Training Center (JRTC) rotation. The Commander selected the reorganization date and the company commanders and 1SGs know the structure, by name, of their post-deployment companies. We worked it far enough in advance to allow for the planning of NCOERs and training events. The training piece is critical. Now that the rear detachment companies know what the post-deployment structure looks like, they can train those teams so we do not dive in training proficiency because the teams have not jelled. The Commander and I feel very confident that the mission-essential task list (METL) proficiency will not degrade.

## Training Files

Simply having a “soft copy” of the training files is insufficient. Although our electronic training database files are extremely useful in tracking date of rank, weapon qualifications, physical training (PT) data, clothing sizes, etc., the electronic files are **not** a substitute for some of the “hard copy” documents found in the training files, especially weapon qualification and Army Physical Fitness Test (APFT) Scorecards (DA Forms 705). Hard copy weapon qualification sheets and APFT scorecards are required for SGT and SSG promotion point computations. Each deployed

company continues to conduct APFTs, both record and diagnostic, so having the soldiers’ historical DA Forms 705 is essential. For the APFT-challenged soldier, the hard copy of the APFT scorecard is necessary to document multiple APFT failures in order to execute any type of administrative actions (bars to reenlistment, administrative reductions, etc.). When deployed, soldiers take APFTs, requalify on their assigned weapons, become Combat Lifesaver-certified and recertified, and so forth. The company simply places the results in the existing training files, rather than creating entirely new training records that they would have to reintegrate with home station records after redeployment.

## Final Thoughts

One more thing before I close. Get with your signal officer or network specialist and have that person download your E-mail and desktop files. We prevented much anguish by bringing home station E-mail personal folders with us. We also downloaded all of our relevant computer files on compact disc—this was an enormous help. Either transfer all of your files on a laptop or download them on disks; if you do not, you will be having someone from the rear send the files anyway.



*Command Sergeant Major Lori Brown is currently the CSM, 110th MI Battalion. She has held every leadership position from team leader to Battalion CSM. She previously served as the 501st MI Brigade S3 Operations SGM, 502d MI Battalion Operations Sergeant, and spent four years as a First Sergeant. CSM Brown completed five overseas tours. She holds a Bachelor of Science degree from Regents College. You can contact CSM Brown at lori.brown@us.army.mil.*

---

## Nonpassive Defense of the Army’s Computer Networks

---

(Continued from page 39)

4. Department of Justice Memorandum to DOD General Counsel, dated 11 August 1999.

5. Ibid.

6. Title 18 USC, Sections 1801-1811.

7. Title 18 USC, Section 1030.

*Tom King is a Department of the Army Civilian currently assigned to the Office of the Staff Judge Advocate, U.S. Army Network Enterprise Technology Command/9th Army Signal Command (NETCOM). Dual-hatted, he serves as both the Information Assurance Lawyer for the command and works computer law issues for the U.S. Army Intelligence Center and Fort*

*Huachuca as well. He holds a Bachelor of Science degree from the University of Rochester, a Juris Doctor degree from Albany Law School, and a Master of Arts degree in History from the State University of New York (SUNY) at Albany. Readers may contact Mr. King via E-mail at thomas.g.king@us.army.mil and telephonically at (520) 533-3197 or DSN 821-3197.*

# Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT)

by Captain Misty L. Martin

The Intelligence and Electronic Warfare Tactical Proficiency Trainer (IEWTPT) program evolved in response to the need that the Active Army and Reserve Component tactical Military Intelligence (MI) units had for a means to simulate an opposing force battlefield realistically. A Headquarters, Department of the Army-directed study in 1980 initially documented the inability to maintain the skills of Military Intelligence (MI) soldiers in tactical units. The study concluded that units were neither conducting effective training nor was the equipment available for the units to conduct training. In response to this need, the MI community produced a Training Device Need Statement (TDNS) and an Operational Requirements Document (ORD). The IEWTPT acquisition will address these needs and requirements.

## The Training Device

The IEWTPT is a “non-system” training device that provides realistic battle command training through an integrated, distributed intelligence information environment to primarily MI soldier operators who drive the intelligence systems as well as battle commanders and the battle staff. IEWTPT replicates the environment that commanders will find on the future battlefield in scope, fidelity, and information management requirements. It provides the ability for MI commanders to conduct individual, crew, collective, and unit training.

## IEWTPT Capabilities

The IEWTPT consists of three functional groupings of capabilities referred to as the technical control cell (TCC), the target signature arrays (TSAs), and a supporting constructive simulation. The TCC



consists of sensor stimulators and emulators that sample the environment generated by the constructive simulation. The TCC networks the TSAs, coordinates scenarios, and collects after-action data. The TSAs are embedded into or strapped on the intelligence and electronic warfare (IEW) operational equipment that allows receipt and translation of the TCC feeds.

**Technical Control Cell.** The TCC controls all IEWTPT training and communication between the constructive simulation and the operational intelligence processing systems. The control functions include the following:

- ❑ Segregating or linking the operational intelligence processing systems to provide individual, collective, and unit-level training.
- ❑ Collecting training data for after-action review (AAR).
- ❑ Providing the constructive simulation with the status of the operational intelligence processing systems.

Equally important, the TCC enhances the constructive simulation run-time state variables to provide the data (content) to the intelligence processing systems as if the intelligence processing system were actually operational. The TCC interfaces with the instrumentation systems as required to support the training requirements.

**Target Signature Arrays.** A TSA may be an embedded capability, a

strap-on capability, or some combination thereof, which injects the TCC-provided content into operational intelligence processing systems. The operator uses unit equipment to derive intelligence data context-sensitive to the battle command constructive simulation and publish and deliver realistic outputs to the same communications systems that would be used in time of hostilities or stability and support operations. The TSAs are dependent upon the successful development of the TCC to support connecting multiple TSAs for large MI scenarios. The IEW System Program Managers are responsible for the development of the TSAs. The IEWTPT will stimulate up to ten different TSAs.

**Constructive Simulation.** The constructive simulation provides run-time state variables from an integrated constructive training simulation. Run-time state variables at a minimum include the following:

- ❑ Platform position, velocity, vector, status, and state for all entities.
- ❑ Synthetic natural environment (SNE).
- ❑ Status of the command and control, communications, computers, and intelligence systems used to connect the constructive simulation to the training audience.

The run-time state variables describe the context for both the constructive simulation and IEWTPT to collect entity data from which they can derive intelligence.

## IEWTPT Development

The IEWTPT program comprises three blocks—Block I is the Initial Operational Capability (IOC), Block II is an interim capability, and Block III is the Final Operational Capability (FOC) (see Figure 1).



# CGS and Apache-Longbow Linkage— A 2d Infantry Division Initiative

by First Lieutenant Christine V. Fallon, Staff Sergeant Steven D. Jaime, and Sergeant Tony Donaldson

The Common Ground Station (CGS) is a receiver-processor of Joint Surveillance Target Attack Radar System (Joint STARS) data. The CGS provides a visual display of this data correlated against a map background. In addition, the ground station receives imagery, synthetic aperture radar (SAR) data, and video, allowing U.S. and allied maneuver forces an early look at the activity of the second, third, and follow-on enemy ground forces. By simultaneously receiving, processing, and displaying multiple intelligence sources on a digitized map background, the CGS system provides input to the “now battle picture” of the battlefield for commanders. Inherent in CGS is the flexibility to provide tailored intelligence collection for lethal targeting by field artillery and attack aviation assets. This unique system also provides battle management, surveillance, targeting, and interdiction support for development and execution of plans and orders with near-real-time correlated information.

## Background of the Initiative

Until recently, the system has had limited success supporting commanders' requirements in operations close to the forward line of own troops. This is primarily because Joint STARS is unable to discern enemy targets from friendly targets. The 2d Infantry Division (2 ID) in Korea recently experimented with radar data flow from the Apache Longbow to CGS. This information supplements the shortfalls of the Joint STARS. While attributed to the system during acquisition, this capability was not a reality until recently.

Through the 2 ID initiative, contractors rewrote the software, and the team achieved CGS information transmission to the Apache Longbow, a close-combat asset. The Common Ground Station's digital datalink with the Longbow will provide units throughout the division with more detailed intelligence of the close threat. This initiative also has the potential to increase survivability of the aircraft by providing the Longbow possible early warning of known enemy air defense artillery (ADA) emitters. The system complements information flowing from the Division Analysis and Control Element (ACE) through the unit Analysis and Control Team (ACT), increasing combat effectiveness by allowing the Longbow to plan ingress and egress routes to targets better.

## September 2002 Linkage Exercise

During an exercise on 26 September 2002, elements of the 102d Military Intelligence Battalion and 1st Battalion (Attack), 2d Aviation Regiment, successfully linked the CGS with software version CSB 1.B11.1, IDM 2.9H to an airborne Apache Longbow with software version LOT 6, IDM 2.9H. The first step was to establish voice communication using ultra-high frequency (VRC-83) and very-high frequency (VRC-92/RT-1523E), secure and nonsecure. The team accomplished this using the CGS' mounted vehicular antennas and both tail- and belly-mounted antennas on the Apache. External mast antennas were not necessary—as previously thought by contractors—to establish and maintain a successful two-way link between the CGS and the Apache Longbow.

During the initial phase of our trials, the CGS could only receive fire-control radar (FCR) targets and

digital plain text messages but could not send information to the Apache. Contractors then made permanent modifications to the CGS software based on controlled environment testing performed by two contract firms on 18 September 2002. On site, contractors extended the periodicity of the present position query (PPQ) from 30 seconds to 2 minutes. The PPQ allows the CGS to track the telemetry of the aircraft and is required for a successful link with the Apache. However, the CGS still could not establish a link. During our initial tests, we used plain text and single-channel data as per contractor guidance. However, the key to success was to switch from plain text to enciphered text as well as frequency-hopping mode.

Once all changes were complete, the CGS was able to communicate digitally with the Apache, sending free text and FCR messages, establishing a successful link. Testers initially achieved the link with the aircraft on the ground, providing controlled conditions (line of sight [LOS] and unobstructed communication). Once this was successful, we connected with an airborne Apache. This communication was the first between the CGS and an airborne Apache Longbow using the previously mentioned software configurations. After achieving success, we broke and reestablished the datalink several times to ensure consistency. The Apache was airborne for approximately one hour and traveled roughly two kilometers away from the CGS during the flight.

Having established a successful datalink, the CGS was able to send the Apache Longbow both FCR and digital plain text messages, as well as Airborne Reconnaissance Low (ARL) imagery previously archived in the CGS database. The datalink al-

lowed the aircraft's telemetry to be displayed, thus enabling the CGS operators to track the flight path of the Apache. The ability to track the aircraft's telemetry is vital to effective operations between the CGS and the Apache. If the CGS operator has the ability to see where the Apache is and what it is looking at through the FCR, then the operator can send additional target information the Apache's FCR is not showing.

The aircraft's combat effectiveness and survivability also increases due to the CGS operators' ability to identify and pass on suspected air defense artillery (ADA) and surface-to-air missile sites. The more information that we can provide to the aircraft, the better they will be able to plan future attack missions or alter ongoing operations. According to Colonel James E. Moentmann, 2d Aviation Regiment Commander, the greatest value to the Longbow and aviation brigade is in the pre-mission planning phase. For example, the CGS can provide updated site data before occupying an attack-by-fire position or before departure on a movement to contact.

Using the Apache Longbow to gather data while performing standard attack operations provides commanders with close-combat intelligence and increases the survivability of the aircraft. The most likely scenario is that the Longbows will pass data at the end of a mission as they are rotating off station and conducting a battle handover to another team, with the likely product being a "shot at" file or the last of very many radar snapshots. However, with the first attempt at an aerial link established using the current software, we identified some limitations. The greatest limitation is that the CGS is an LOS system. The Longbow does not have the standoff distance of ARL or the E-8 (Joint STARS) aerial intelligence platforms. It can, however, provide short-range radar imagery that we can confirm

with products gathered from other sources. Because the CGS is an LOS-based system, maintaining a link for an extended period may be a problem. Developing a retransmission system for the CGS would be a possible solution.

To truly be effective to the supported unit, the CGS crews and Apache Longbow units must develop a working relationship. They need to understand the capabilities and limitations of the two systems.

## Brigade CALFEX

Since the exercise with 1-2 Aviation in September, the 102d MI Battalion participated in a brigade combined arms live-fire exercise (CALFEX) with 1-2 Aviation and 4-7 Cavalry, also of the 2 ID. Rather than working directly with the subordinate units, the Division integrated the CGS into the Aviation Brigade command and control element, again successfully linking the two systems. During this exercise, the CGS was able to receive "shot at" files, which can assist in calculating battle damage assessments. The CALFEX showed that although a free-text feature is available, the pilots did not often use it; this is simply because talking on the radio is considerably faster than one-handed typing of messages in the aircraft, particularly given the workload in the cockpit.

## Final Thoughts

The 2d Infantry Division continues to expand on the CGS-Apache Longbow initiative. Allocation of the five CGS systems currently in the Division is to the Division main and tactical command posts, Aviation Brigade, 1st Brigade, and 2d Brigade. The Army was shortsighted in not providing a sixth system to support the targeting requirements of the division artillery. With the unmanned aerial vehicle (UAV) fielding this coming year, the Division will continue to expand on the intelligence capabilities of the CGS system. The CGS is a relatively new asset to 2 ID and the Army; therefore, MI units must

take the responsibility of integrating this system into brigade and division tactical operations centers and other units that would benefit from this technology.



*Sergeant Jessica Ward and Specialist Michael Thornton also contributed to this article.*

*First Lieutenant Christine Fallon earned a Bachelor of Arts degree in Telecommunication from Penn State University and a commission in Intelligence through the Reserve Officer Training Program. She graduated from Airborne School and the Military Intelligence Officer Basic Course. 1LT Fallon is currently a Platoon Leader with B Company, 102d MI Battalion, 2d Infantry Division, Korea. Her next duty station will be the 902d MI Group, Fort George G. Meade, Maryland. Readers may contact her via E-mail at christine.fallon@us.army.mil.*

*Staff Sergeant Steve Jaime joined the Army in October 1991 as a Fire Support Specialist (13F). His previous assignments have included Fort Sill, Oklahoma; Germany; Hawaii, and Fort Lewis, Washington. After reclassification as a Common Ground Station (CGS) Operator (MOS 96H) in August 2002, SSG Jaime relocated to Korea where he serves with the 2d Infantry Division. He has attend military schools including Advanced Field Artillery Tactical Data System (AFATDS) and Air Ground Operations System (AGOS) training, the Primary Leadership Development Course (PLDC), and the Basic Noncommissioned Officers Course (BNCOC). Readers may contact this author via E-mail at steven.jaime@us.army.mil.*

## New MIPB Mailing Address

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

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

# Global War on Terrorism:

## Polygraph—An Intelligence Tool

by Chief Warrant Officer Three Joe Don Castleberry



On 31 March 1998, in *United States v. Scheffer*<sup>1</sup> a divided U.S. Supreme Court held that either side could ban the results of a polygraph examination from use in a criminal trial because there is no consensus that polygraph evidence is reliable. The Court found that the scientific community and the state and federal courts are extremely polarized on the matter. Five of the concurring and dissenting justices noted that:

*There is much inconsistency between the Government's extensive use of polygraphs to make vital security determinations, and the argument it made in that case stressing the inaccuracy of these tests.*

The majority of the Court found nothing inconsistent, however, in the Government's use of the polygraph

for personnel screening and as a tool in criminal and intelligence investigations because, it said, such limited out-of-court uses of polygraph techniques differ in character from, and carry less severe consequences than, the use of polygraphs as evidence in a criminal trial.

The Court noted that between 1981 and 1997, the Department of Defense (DOD) conducted more than 400,000 polygraph examinations. Justice John Paul Stevens in a dissenting opinion supported its use by DOD, because, he said, its polygraph examiners were trained at its own Polygraph Institute, "which is generally considered the best training facility for polygraph examiners in the United States." The Supreme Court's opinion has put to rest any argument against the continued use of this technique as a tool in national security investigations.

### The Army Leads the Way

The Polygraph Branch, 310th Military Intelligence (MI) Battalion, conducts counterintelligence (CI) scope, polygraph screening examinations in support of DOD Special Access Programs, the Department of the Army (DA) Cryptographic Access Program, and the National Security Agency (NSA) on a routine basis. In addition, polygraphers conduct operational examinations in support of offensive CI operations, CI and counterespionage (CE) investigations, and counterintelligence force protection source operations (CFSO). With the current Global War on Terrorism and other significant events occurring throughout the world, the mission continues to increase. During the last fiscal year, the Branch conducted more than 1,100 CI-scope polygraph screening examinations and nearly 70 operational examinations. These numbers will likely increase dramatically in the near future.

The Army will continue to lead the way when using polygraphs in the tactical arena. U.S. Army examiners were the first polygraph personnel to go to Guantanamo Bay, Cuba, and Kandahar and Bagram, Afghanistan, pursuant to the war on terrorism and the search for Osama bin Laden (see Figure 1). While other agencies waited to see if polygraph examinations would yield favorable results in such an environment, Army examiners proved they could, conducting sensitive examinations to determine the veracity of information reported by known or suspected Taliban and al-Qaeda members. In one instance, use of the polygraph



A polygrapher reviews a result sheet from an interview.

Photos courtesy of the 902d MI Group.



**Suspected terrorist is escorted to the interrogation facilities at Camp X-Ray.**

nullified a significant biological weapons threat while in another it aided the State Department by clearing one

of our allies of direct involvement with al-Qaeda. It has also cleared some individuals of direct involvement with al-Qaeda and allowed commanders to employ available assets better.

### **Expanding Use of the Polygraph**

As an investigative aid, the polygraph has helped investigators in closing many investigations. In cases where the Army requested a polygraph test, the polygraph examinations have either proven or nullified numerous allegations. This has led to a significant increase in the number of requests received by the 310th MI Battalion. In the screening environment, use of the polygraph has identified numerous security concerns and possible threats on a con-

tinual basis; on several occasions, examinees have admitted to having classified or sensitive information outside government control. The polygraph has identified these potential threats and led to recovery of the information.

The DOD is continuing to expand the use of the polygraph because of its proven benefit. The 902d MI Group's polygraph examiner personnel strength may increase from the current ten examiners to twenty-five in the next five to ten years. This includes adding various programs and requiring even more polygraph examinations in those areas where intelligence is susceptible. The U.S. House Permanent Select Committee on Intelligence recently concluded that the polygraph was one

#### **Enduring Freedom (Cuba)**

- Nullified a biological weapons threat when the suspect, a known al-Qaeda member, admitted to falsifying information.
- Cleared a U.S. ally by verifying information provided by a high-ranking member of a foreign government.
- Cleared several detainees of direct involvement with terrorist activities and identified several who participated in hostilities.

#### **Enduring Freedom (Afghanistan)**

- Confirmed secret contact with a middle-eastern intelligence service by a U.S. employee working as a translator.
- Verified significant intelligence information found in the possession of a detainee in Kandahar.
- Obtained admission that a detainee actively participated in the war against U.S. Forces on the front lines near Kabul.

#### **CI/CE Investigations**

- Identified the individual who removed a Top Secret document from a secure facility. There were 25 suspects initially.
- Cleared a U.S. Army officer of espionage while confirming involvement with a foreign intelligence service.
- Used the polygraph to confirm information passed while examinee was engaging in espionage as part of an initial plea agreement to reduce prison term.

#### **Counterintelligence-Scope Polygraph**

- Recovered Top Secret/Sensitive Compartmented Information (TS/SCI) materials from a home computer due to admission obtained.
- Obtained admission relating to the smuggling of TS documents from a sensitive compartmented information facility (SCIF). Nullified a significant threat and identified a foreign national who assisted.
- Recovered 135 pages of Secret documents from a U.S. Marine Corps officer who had the information stored at his residence.

#### **Limited Access Interpreter**

- Obtained information relating to secret trips to Iraq and close associations with a government official in Iraq.
- Obtained information that tied examinee to known or suspected militant organizations.
- Obtained significant intelligence information omitted from the submitted SF-86 (Questionnaire for National Security Positions), which disqualified applicant from positions.

**Figure 1. Selected Successes Achieved Through Polygraph Examinations in Several Mission Areas.**



**The author and CW2 Edwards prepare to conduct examinations in Kandahar, Afghanistan.**

of the best tools available to safeguard intelligence information. It is another tool that commanders can use to safeguard information. This has many looking at expanding its uses to other jobs within the military where leaks can occur.

### **Conclusion**

The polygraph is still one of the best, and sometimes the only, means available to determine the

veracity of information. In the tactical environment, the Army has proven to be the expert in its employment. However, we still have a long road ahead. We need to educate those in the tactical environment better on the uses and benefits of polygraph examinations, clearly spelling out the ways in which the examiners can benefit the command. Branch personnel currently teach a two-hour block of instruc-

tion to the CFSO Course and Officers CI Course (35E) at Fort Huachuca, Arizona, on a recurring basis. Examiners also furnish tailored instruction to units throughout the continental United States when requested. Polygraph examination, like any other specialty, cannot be learned overnight and our experienced examiners are an invaluable asset that we must protect.



### **Endnote**

1. Supreme Court of the United States; Number 96-1133; *United States, Petitioner v. Edward G. Scheffer*; 31 March 1998.

*Chief Warrant Officer Three Joe Don Castleberry is currently the Chief, Polygraph Branch, 310th MI Battalion, 902d MI Group. He joined the Army in 1987 and, upon completing basic and advanced individual training, was assigned to the J2, U.S. Forces, Korea. While assigned to the West Coast Battalion, he submitted an application to become a Polygrapher. In 1991, he attended the DOD Polygraph Institute and worked as an examiner since. CW3 Castleberry has served in Korea, Denver, and at Fort Meade. He attended the Warrant Officer Basic Course in May 1994. Readers may contact the author through E-mail at tinam@meade-inscom.army.mil.*

### **ASAS User's Conference 2003**

The 2003 All-Source Analysis System (ASAS) User's Conference will be 16 and 17 September 2003 at Fort Huachuca, Arizona. The U.S. Army Training and Doctrine Command (TRADOC) Systems Manager (TSM) ASAS is the sponsor. This year's conference will focus on Lessons Learned and you, the users in the field, will primarily present the forum. We want to hear what your success stories are and what improvements you foresee requiring so that the TSM can continue to be responsive to your needs.

Due to our major focus on the Global War on Terrorism including Operations IRAQI FREEDOM and ENDURING FREEDOM, we did not hold an ASAS conference in 2002. The program has reached several significant milestones over the past two years since our last conference. Some of the highlights are the maturing of the ASAS-Light baseline system, interoperability functions, and the Block II Analysis and Control Element (ACE) workstation.

The agenda includes briefings by the TSM, Project Manager (PM), and the U.S. Army Communications-Electronics Command (CECOM), unit briefings, and demonstrations. The TSM intends it to be an unclassified event; however, there may be some classified discussions. We request all attendees transmit their clearance information (both collateral and SCI) to the telephone numbers listed below. In both cases cite the "2003 ASAS Users' Conference 16-17 September 2003" and list MAJ Eva Branham as the local point of contact. For SCI clearance information only, please pass clearance information through special security office channels to SSO Huachuca, Ms. Dondi Minor, telephone (520) 538-6500 or DSN 879-6500. For collateral clearance information only, please fax to the S2, 306th MI Battalion at (520) 533-3044 or DSN 533-821 or call (520) 533-3025.

Please send an initial response back from your organization if you will attend; list the number of people and whether you plan to brief (if so, state any schedule preferences). Also indicate if there are any areas you are particularly interested in hearing briefed or wish seeing demonstrated by the TSM, PM, CECOM, or other ASAS-equipped unit.

As you complete your briefings, please forward them to MAJ Eva Branham or Ms. Diane Rabb via E-mail at [eva.branham@hua.army.mil](mailto:eva.branham@hua.army.mil) or [diane.rabb@hua.army.mil](mailto:diane.rabb@hua.army.mil), your nd ylrmy

# Doctrine Corner

## Intelligence Support to Information Operations: Today and in the Objective Force

by Lori A. Sieting (CW3, Retired)

Today U.S. military forces face a dynamic, multidimensional, and increasingly interconnected global environment. The characteristics of warfare continually evolve with technological advancements in information systems and communications. The battlefield extends far beyond traditional parameters into the intelligence-intensive, complex realm of information operations (IO).

Terrorist groups and other adversaries use covert techniques to carry out computer network attacks, espionage, data collection, network mapping and reconnaissance, and data theft. Commanders rely extensively on multidiscipline intelligence support to furnish the information they require to target and exploit enemy information and information systems and establish protective measures to defend friendly information and systems against enemy attack or exploitation.

### Background

IO is the employment of the core capabilities of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOPs), military deception, and operations security (OPSEC), in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decisionmaking (**Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms**). Information operations target information or information systems to affect the information-based process, whether

human or automated. Commanders conduct IO by synchronizing IO elements and related activities, each of which may be either offensive or defensive.

**Offensive IO** destroy, degrade, disrupt, deny, deceive, exploit, and influence adversary decisionmakers and others who can affect the success of friendly operations. Offensive IO also target the information and information systems (INFOSYS) used in the adversary's decisionmaking processes. **Defensive IO** protect and defend friendly information, command and control (C2) systems, and INFOSYS. Effective defensive IO enable development of an accurate common operational picture based not only on a military perspective but also on environmental factors that may affect the situation.

A recent example of IO gone awry is the former Iraqi Minister of Information, Mohammed Saeed al-Sahaf's attempt to influence the Iraqi people during Operation IRAQI FREEDOM. Minister al-Sahaf promised victory for Iraq, and when U.S. troops were only a few hundred meters from where he was standing in downtown Baghdad, Minister al-Sahaf boasted that Iraqi troops had forced U.S. soldiers into a shameful retreat.

Adversarial information operations have included such actions as using misinformation to incite a riot against a government, establishment, or organization. In addition to the adversary's use of misinformation, IO may also take the form of disruption, degradation, exploitation, or destruction of communications such as Internet sites,

radio and television broadcasts, newspapers, etc. IO is a distinct element of combat power.

### Intelligence Support to IO

Multidiscipline intelligence support is integral to the planning, execution, and assessment of IO. The integration of IO into the planning process enhances protection of friendly systems and assets while exposing windows of opportunity for attack or exploitation. To plan and execute IO, we must collect, store, analyze, and present information in a form that the commander can easily assimilate. The commander and staff, when planning the friendly scheme of maneuver, use the products and analysis developed by the intelligence staff to determine when and where in the battlespace the friendly forces must focus IO.

Intelligence collection for IO includes all possible sources—national level; special operations; multidiscipline operations; open sources such as news media, academia, Internet, and commercial publications; commercial contacts; local nationals; and more. Rapid processing, analysis, and dissemination of all-source intelligence will reinforce and confirm relevant IO information and enable the targeting and exploitation of an adversary's critical capabilities, systems, and facilities.

### Specific Areas of IO Support

Intelligence support to IO includes support in seven areas: OPSEC, PSYOPs, military deception, electronic attack, physical destruction,

civil-military operations, and public affairs.

**Support to Operations Security (OPSEC).** This intelligence support consists of identifying capabilities and limitations of the adversary's intelligence system to include adversary intelligence objectives and the means, methods, and facilities used by the threat to collect, process, and analyze information.

**Support to Psychological Operations (PSYOPs).** This category of intelligence support to IO includes the environment, target groups, and influence on others, to include—

- ❑ Identifying the cultural, social, economic, and political environment of the area of interest (AOI). For example, adversary mechanisms for political control, adversary communication and broadcast systems used to elicit support from the populace, current and past adversary propaganda activities, and their effectiveness.
- ❑ Identifying target groups and subgroups and their locations, conditions, vulnerabilities, susceptibilities, cultures, attitudes, and behaviors. This includes determining popular radio and television programs and periodicals and their audience demographics; media personalities and political cartoons; and group attitudes, beliefs, perceptions, alliances, and behavior.
- ❑ Identifying the effect of planned PSYOPs on individuals outside the targeted group (for example, multinational partners and neighboring populations).

**Support to Military Deception** includes identifying the capabilities and limitations of the adversary's intelligence-gathering systems as well as adversary biases and perceptions.

- ❑ Profiles of crucial adversary leaders.
- ❑ Cultural, religious, social, and political characteristics of the country and region.

- ❑ Sources of military, economic, or political support.
- ❑ Adversary decisionmaking processes, patterns, and biases.
- ❑ Adversary perceptions of the military situation in the area of operations (AO).
- ❑ Capabilities and limitations of adversary counterintelligence (CI) and security services.

**Support to Electronic Attack (EA).** Intelligence support to IO in the area of EA includes identification and assessment of the adversary nodes and capabilities discussed below.

- ❑ Identifying critical adversary information; command, control communications, and computers (C4); and intelligence nodes. This includes determining and presenting the adversary's electronic order of battle (OB) and the information system infrastructure, the enemy's C2 system vulnerabilities, and their means of protecting their C2 systems.
- ❑ Assessing adversary EA capabilities (numbers, types, and disposition of EW systems, technical characteristics, methods of employment, and vulnerability to counteractions).

**Support to Physical Destruction** is the identification of critical adversary information, C4, and intelligence nodes, and systems (adversary information infrastructure) to include C2 systems, nodes, and locations; adversary C2 system vulnerabilities; and adversary IO systems, locations, and facilities.

**Support to Civil-Military Operations (CMO)** consists of identifying the cultural, social, economic, and political environment of the AO, including—

- ❑ Population demographics.
- ❑ Civilian populace attitudes, alliances, and behavior.
- ❑ Availability of basic necessities (food, clothing, water, shelter, and medical care) and the ability of the populace to care for itself.

- ❑ Locations and potential routes, destinations, and assembly areas or sites of displaced persons.
- ❑ Local government type, status, character, organization, and capabilities.
- ❑ Availability of local material and personnel to support military operations.
- ❑ Nongovernmental organizations or private volunteer organizations in the AO, their agendas, resources, and capabilities.

**Support to Public Affairs (PA).** This area of intelligence support to IO includes identification of factors in the environment as well as in collective opinion, to include—

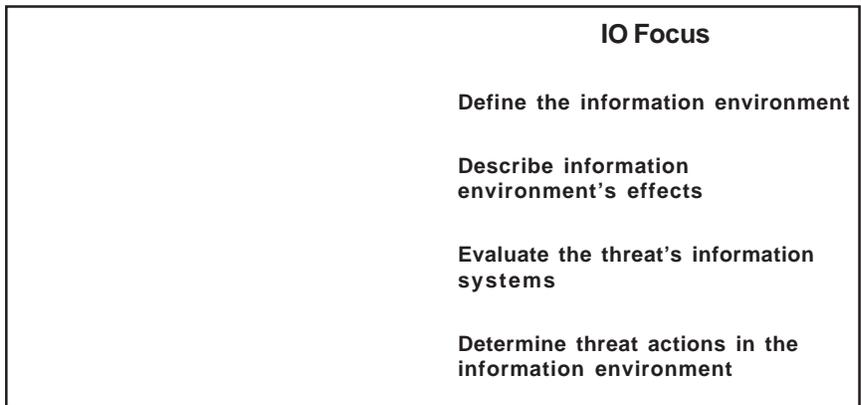
- ❑ Identifying the coalition and foreign public physical and social environment (propaganda and misinformation capabilities, activities, targets, themes, and dissemination means of the adversary).
- ❑ Identifying world, national, and local public opinion (location, biases or predispositions, and agenda of national and international media representatives in the AO, and trends reflected by the national and international media).

## Intelligence Preparation of the Battlefield and IO

The purpose of the intelligence preparation of the battlefield (IPB) in support of IO is to gain an understanding of the information environment and to determine how the threat will operate in the information environment. The goal is identification of—

- ❑ Threat vulnerabilities that friendly IO can target and exploit.
- ❑ Threat information capabilities against which friendly forces must defend.

A detailed understanding of an adversary's information infrastructure—a combination of numerous elements—is a very important com-



**Figure 1. IPB and IO Focus.**

ponent of IPB in support of IO. An information infrastructure consists of multiple types of systems, such as intelligence, logistics, medical, personnel, operations, fire support, EW, etc., that may operate as separate information systems but support the adversary and his supporting organization as a whole. The different systems, while separate, may physically share the same communications pathways or processors and are, therefore, high-value targets (HVTs) for physical destruction and a vital part of the IPB process that supports IO. To focus analysis on the information environment, the IPB steps relate to IO as shown in Figure 1.

For offensive IO, IPB is a continuous process used to develop a detailed knowledge of the adversary employment of information and information systems. IPB for offensive IO uses a process of overlapping and simultaneous actions that produces situation updates, thereby providing joint forces commanders and their subordinate commanders with flexible offensive IO options. IPB in support of offensive IO builds upon traditional IPB and requires the following:

- ❑ Knowledge of the technical capabilities of the adversary's information systems.
- ❑ Knowledge of the political, economic, social, and cultural influences.

- ❑ Ability to develop templates used to portray the battlespace and refine targets for offensive IO courses of action (COAs).
- ❑ Understanding of the adversary's or potential adversary's decisionmaking process.
- ❑ In-depth understanding of the biographical background of major adversary leaders, decisionmakers, communicators, and their advisors, to include motivating factors and their leadership styles.
- ❑ Knowledge of the area of the responsibility (AOR) and joint operational area (JOA) geographic, atmospheric, and littoral influences on adversary and friendly operations.

At lower echelons, the S2 will process information concerning IO, which is collected in accordance with the information requirements (IR) and the priority intelligence requirements



**Figure 2. Information Environment Templates.**

(PIRs) and forwarded to higher echelons for analysis, use in IPB, and decisionmaking. Higher echelons will direct OPSEC measures and other IO-related tasks. Intelligence tasks performed in support of IO, identified through IPB, include providing intelligence support to—

- ❑ Offensive IO which includes support to PSYOPs, military deception, and EA.
- ❑ Defensive IO which includes support to OPSEC.
- ❑ Activities related to IO which includes support to CMO and PA.
- ❑ Targeting (IO).
- ❑ Battle damage assessment (BDA) (IO).

The physical description and overlays of IO targets can be combined with an IO decisionmaking and execution matrix to form an accurate assessment of an adversary's information capabilities and vulnerabilities. The adversary's strengths and weaknesses are compared with the assessment of friendly capabilities to determine friendly C2 vulnerabilities and strong points.

**Information Environment Templates**

Based on the threat's normal or "doctrinal" organization, equipment, doctrine, and tactics, techniques and procedures (TTPs), the

intelligence officer creates threat models to depict how threat forces prefer to conduct operations under ideal conditions. Threat models generally consist of doctrinal templates, descriptions of preferred tactics and options, and identification of HVTs. Figure 2 depicts some of the types, descriptions, and purposes of information environment templates.

The intelligence officer produces several other products which contain IO-related information, including:

- ❑ Situation Template. A situation template is a graphic depiction of expected threat force dispositions for a specific COA. A situation template that focuses on IO depicts how the threat may employ its information assets both offensively and defensively to achieve an operational advantage.
- ❑ High-Value Target List (HVTL). The HVTL should include threat information assets, even those that the unit is not going to attack by lethal means. Typical information target sets include decisionmakers and information system assets.
- ❑ Event Template and Matrix. An event template and supporting event matrix identify specific areas and threat activities that predict which COA the threat will chose. IO input to the event template and matrix helps develop intelligence collection requirements for IO.

The intelligence officer evaluates and rank-orders the threat IO COAs according to their likely order of adoption. The purpose of prioritizing these COAs is to provide the staff with a starting point for the development of a plan that addresses potential threat COAs. Based on the time available, the intelligence staff develops each threat IO COA with as much detail as possible. In some instances, they may only develop the threat's most likely and most dangerous IO COAs. As part

of determining threat COAs, the staff postulates how, when, where, and why (to what purpose) the threat will use its information systems to support its likely objectives and achieve its desired end state.

### Intelligence Support to IO in the Objective Force

Intelligence support to IO will be increasingly critical to safeguarding U.S. information and information infrastructure in the future. Factors that contribute to this include projected technological advancements, growing reliance on information technology, and the future combat system's potential to enable easy access to products such as the common operational picture at all levels of command. Even if the adversary succeeds in interrupting portions of the friendly system, individual soldiers' initiative must automatically take the appropriate countermeasures and report information of intelligence value in support of IO. This individual initiative will be a product of training and a command climate instilled across the force long before enemy offensive IO disable components of our information systems. Intelligence support to IO in the Objective Force will be a collaborative, coordinated effort at all levels

of command. Intelligence support—including collection, analysis, developing and prioritizing adversary IO COAs, IPB in support of IO, requirements management, presentation of IO-related information, etc.—is integral to conducting IO.

Intelligence support to IO in the Objective Force will essentially have the same objectives that exist today. However, development of new TTPs will be necessary to reflect the changes in future systems and organizations. The significance of intelligence support to IO will be paramount as future information technology takes information access and dissemination to higher levels. The future information environment and its associated threats are a primary focus in Objective Force. To this end, staff structure in the Objective Force will organize not by echelon (e.g., S2/G2/J2) but rather by function in order to better focus efforts on such operations as IO.

### Objective Force Staff Structure

The Objective Force Battle Command will consist of a core staff structure, organized into functional groupings, to operate within the environment of knowledge-based warfare. The nodal construct for staff

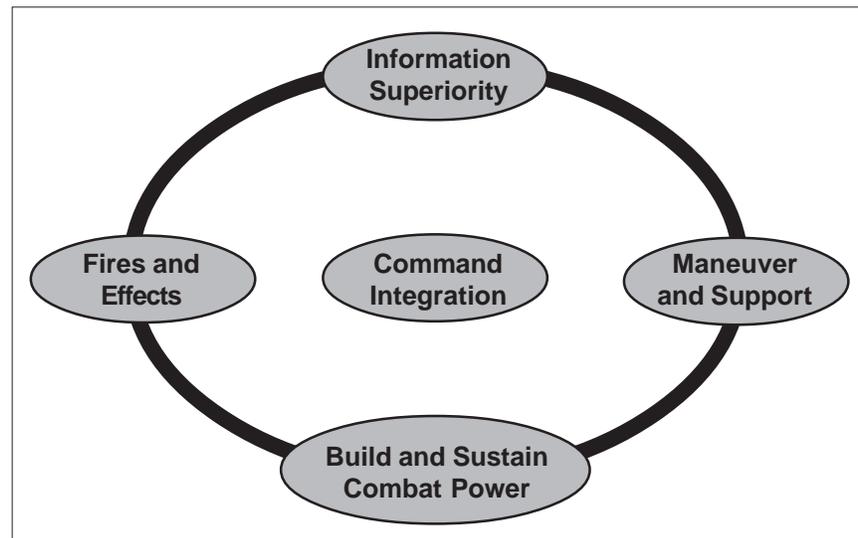


Figure 3. Objective Force Staff Structure.

organization within the Battle Command involves five nodes: one integrating node and four multifunctional nodes. The five nodes (cells) are:

- ❑ Command Integration Cell (CIC).
- ❑ Information Superiority Cell (ISC).
- ❑ Fires and Effect Cell (F&EC).
- ❑ Build and Sustain Combat Power Cell (B&SCPC).
- ❑ Maneuver and Support Cell (MSC). (See Figure 3).

Information operations will be one of the principle functions of the ISC.

### Role of the Information Superiority Cell

The ISC will develop and maintain a superior knowledge edge for the commander to execute knowledge-focused warfare. The ISC executes a variety of staff planning functions to reach this knowledge advantage. These include staff planning for information operations (offensive and defensive), network operations, surveillance and reconnaissance planning and execution, counterintelligence, information assurance, space asset access, intelligence synchronization, intelligence planning and analysis, and overall data, information, and intel-

ligence fusion. The ISC directs the planning and management functions essential to all knowledge-based warfare. The ISC will have staff expertise traditionally represented by IO, signal, intelligence, cavalry, and space with the organic reach to global assets necessary to develop and maintain the commander's knowledge advantage.

### Conclusion

U.S. force readiness depends upon our ability to provide intelligence and analysis concerning the current and future IO methods and capabilities of potential adversaries and incorporate these considerations into the planning and execution of military operations. The operational environment will continue to change as adversaries acquire access to more advanced information systems and technologies. U.S. military forces must evolve to meet the needs of the dynamic information environment.

For more information concerning Intelligence Support to Information Operations, see **JP 3-13, Joint Doctrine for Information Operations**, and **FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures** (Final approved DRAG dated October

2002). **FM 2-0, Intelligence** (DRAG dated 19 February 2003) provides in-depth information concerning IPB in support of IO. Further information regarding IO in the Objective Force is in U.S. Army Training and Doctrine Command (TRADOC) **Pamphlet 525-3-0.1, The U.S. Army Objective Force Battle Command Concept**, and other Objective Force 525-series TRADOC Pamphlets. **FM 34-130, Intelligence Preparation of the Battlefield**, provides a detailed breakdown of IPB.



*Lori Sieting (Chief Warrant Officer Three, U.S. Army, Retired) is currently a contractor supporting the Doctrine Division, U.S. Army Intelligence Center and Fort Huachuca. In addition to writing Military Intelligence doctrine, Mrs. Sieting has worked as a training developer for the Stryker Brigade Combat Team, and has served in a variety of MI assignments (tactical, strategic, and deployed) as a warrant officer. Readers may contact her via E-mail at lori.sieting@us.army.mil and telephonically at (520) 533-9966 or DSN 821-9966.*

### Rewrite of the Warfighter's Guide to Communication Architectures

We are in the process of rewriting this guide to get it up to date with the contemporary communication architectures currently in use in the tactical arena. You have many success stories about how you delivered intelligence support throughout the battlefield; please share your input with us.

Please tell us if you have done something different from the norm or if you put another piece of equipment in the loop to help a process be more useful—we are interested! The point of contact (POC) will be traveling throughout the community to validate these architectures before we publish, so if you have something that you believe could benefit other organizations, please send it and we will research it. We plan to publish this updated guide in early 2004.

Please contact the POC with your contributions for this update: CW2 Robert D. Rounds, Officer in Chief, Tactical Exploitation of National Capabilities Support Team, Operations Support Activity, and Headquarters, Operations, 743d MI Battalion. You may E-mail me at robert.rounds@buckley.af.mil or squarepair@us.army.mil and call me at (303) 677-5286/4244 or DSN 877-5286/4244.

# Proponent Notes

by Lieutenant Colonel Eric W. Fatzinger

Each spring, the Office of the Chief, Military Intelligence (OCMI), at Fort Huachuca, Arizona, compiles and coordinates the annual Military Occupational and Classification Structure (MOCS) change proposals, and sends them to the Department of the Army (DA) for final review. We are on schedule with the fiscal year 2003 (FY03) submissions and by the time you read this update, the final version should be out for major Army command (MACOM) staffing. The MI Transformation initiatives this year have again focused on changes to our enlisted structure. Officer changes, particularly within our warrant officer corps, will become more evident in next year's MOCS—as we make adjustments to accommodate the enlisted changes—but are minimal this year. Specifically, while the FY02 MOCS focused on refinements to career management field (CMF) 98, signals intelligence (SIGINT), the FY03 MOCS has most significantly affected the enlisted counterintelligence (CI) and human intelligence (HUMINT) military occupational specialties (MOSs) of CMF96.

## Enlisted Actions

**The CI/HUMINT MOCS proposal will merge MOSs 97B and 97E at Skill Level 1.** The result of this long anticipated move will be that Counterintelligence Agent (MOS 97B) will no longer be an entry-level MOS. It will instead assess at Skill Level 2 (SL2). The proposal will generate an MOS-producing course for 97B20 with expanded CI training to focus better on agent skills and tasks. The HUMINT Collector (MOS 97E) will remain an entry-level MOS but will include both select basic CI and HUMINT skill sets at SL1. The proposal also

removes the language requirement for MOS 97E at SL1.

This is not as radical a change as it might first seem. The Army will continue to address interrogator language needs but will base them on unit-positional requirements documented at SL2 and above. Both of these changes provide advantages by focusing skills to match the actual duties that our 97B and 97E soldiers are performing at the various skill levels. Just as important, it provides for a better return on language training investment (about 70 percent of the 97E first-term soldiers do not reenlist, and daily duties at the 97E10 level, in most cases, do not require the use of a foreign language). When approved, the Army will outline the guidelines for position and selected SL1 personnel-reclassification actions in a Notice of Future Change (NOFC) to be published in October 2003.

**Tactical Unmanned Aerial Vehicle (TUAV) Operator Assignment-Oriented Training (AOT).** The FY03 MOCS will establish TUAV qualification as completion of a TUAV common core of instruction plus an operational system-specific AOT track (initially for the Hunter and Shadow UAVs). This proposal will allow the Army to get soldiers to the field faster with the specific training required for their first assignments. When approved, those UAV Operator (MOS 96U) soldiers already having completed training in Hunter, Shadow, or both, will receive credit for additional skill identifiers (ASIs) as trained operators.

**98P Multisensor Operator Update.** The OCMI continues to get questions concerning when certain

soldier actions related to the creation of MOS 98P, Multisensor Operator, will occur. Creation of MOS 98P was approved as part of the FY02 MOCS proposal. This MOS will serve as the primary operator for current and future tactical SIGINT systems and ground surveillance systems (GSSs). The first tactical SIGINT system the 98P will operate is the Prophet multispectrum, multidiscipline collection, jamming, processing, and reporting system. Traditionally, when the Army creates a new MOS, it allows sufficient time for the development and implementation of an accessions and training strategy to occur over a two- to three-year period. With Prophet fielding to the Army accelerated in response to world events, this has not been feasible for this MOS.

The first 98P positions should appear in the Personnel Management Authorization Document (PMAD) this summer. Once these positions begin to show up, the OCMI will work with the U.S. Army Total Personnel Command (PERSCOM) MI Branch and the Army Staff to recommend "out-calls" from the 96R, 98G, and 98H MOSs to begin filling positions, particularly at the NCO level. (These are the Ground Surveillance System Operator, Cryptologic Linguist, and Communications Intercept/Locator, respectively.) At the same time, we will be working closely with Accessions Branch, PERSCOM, and the U.S. Army Intelligence Center's schools to begin "producing" 98Ps through the training "pipeline." During this initial accelerated fielding period, the Army may ask soldiers already assigned to units receiving the Prophet system with New Equipment Training Team (NETT) instruc-

Old		New
350B	All-Source Intelligence Technician	350F
350D	Imagery Intelligence Technician	350G
350L	Attaché Technician	350Z
350U	Tactical Unmanned Aerial Vehicle Operations Technician	350K
351B	Counterintelligence Technician	351L
351C	Area Intelligence Technician	351Y
351E	Human Intelligence Collection Technician	351M
352C	Traffic Analysis Technician	352N
352G	Voice Intercept Technician	352P
352H	Communications Interceptor/Locator Technician	352Q
352J	Emanations Analysis Technician	352R
352K	Non-Morse Intercept Technician	352S
353A	IEW Systems Maintenance Technician	353T

Figure 1. Conversion Chart Showing the Changing WO MOS Codes.

tion at the time of fielding to operate the system until the training and reclassification actions necessary to provide sufficient 98P soldiers to meet the needs of the Army.

**Upcoming Noncommissioned Officer Selection Boards.** To view by-MOS input to the senior enlisted centralized boards, go to uniform resource locator (URL) [http://138.27.35.32/ocmi/EN\\_Info\\_portal.htm](http://138.27.35.32/ocmi/EN_Info_portal.htm). This is the best place to start if you wish to know what the board members are seeking.

*As always, if you have questions on career maps, courses, impact of assignments, or any other enlisted actions, feel free to contact me, Sergeant Major Walter Crossman. You can reach me via E-mail at [walter.crossman@us.army.mil](mailto:walter.crossman@us.army.mil) and by telephone at (520) 533-1174 or DSN 821-1174.*

### Warrant Officer Actions

**Warrant Officer (WO) MOS Recoding.** While not in the recent MOCS submission, changes to the MOS coding structure throughout the Army are on the horizon. In the near future, you will see a realignment of all MI WO MOSs to 35-series as are the current commissioned areas of concentration (AOCs). As a first step in the warrant officer arena, PERSCOM issued a Notification of

Future Change (NOFC) on 8 August 2002 to **DA Pamphlet 611-21, W-0304-1, Revision of Branch 35 (Military Intelligence)**. This NOFC changes the MOS codes for our MI Warrant Officer MOSs (listed in Figure 1); it does not change the MOS titles. Although this change goes into effect in FY05, you will start seeing the new MOS codes in various documents dealing with tables of organization and equipment (TOEs), tables of distribution and allowance (TDAs), and WO training.

**FY03 MOCS Changes.** While there were no significant warrant officer changes for the MI Corps in the recently submitted FY03 MOCS, you can expect to see a number of changes next year. To accommodate the adjustments made in our enlisted feeder MOSs, we will conduct a review of our SIGINT warrant officer MOSs. We will complete this work in the fall in order to make the FY04 MOCS submission. The changes should be available for MACOM review about this time next year.

**Upcoming Warrant Officer Selection Boards.** The CW3/4/5 Promotion Board convened on 28 April and ran through May 2003. Results should be available in late August or early September. The Army and OCMI have published much on pre-

paring personnel files for promotion boards. Hopefully, those soldiers in the zone of consideration got the word and ensured that their personnel records were complete and that they had current official photographs in their files.

**Remaining FY03 MI WO Accession Boards.** We have two accession boards remaining this year. The first will be 14-18 July 2003 where all MI MOSs except 352G (Voice Intercept Technician) and 353A (Intelligence Electronic Warfare [IEW] Systems Maintenance Technician) will be considered. The September board, to be on 15-19 September, will consider all MOSs except 352H (Communications Interceptor/Locator Technician) and 352J (Emanations Analysis Technician). Interested soldiers should submit their applications as soon as possible to ensure they are board-ready and not delayed. A very recent G1 policy change will now allow consideration of applicants three times rather than just two; if you or someone you know has previously submitted a package, remember they must update their information with OCMI to keep the applications current.

*The point of contact (POC) for all WO actions is Chief Warrant Officer Five Lon Castleton. You can reach*

him via E-mail at [lon.castleton@us.army.mil](mailto:lon.castleton@us.army.mil) and telephonically at (520) 533-1183 or DSN 821-1183.

## Officer Actions

**Commissioned Officer Development and Career Management.** Changes to **DA Pamphlet 600-3, Commissioned Officer Development and Career Management**, have been submitted within the FY03 MOCS. When approved, the Army will document the major changes to the Branch-qualification sections for MI Captains and Majors. Branch qualification for MI Captains has changed to specify that all Captains must command for at least 12 months and must also serve at least 12 months in a position as a battalion S2, assistant brigade S2, or as an intelligence staff officer. MI Majors must serve as an executive officer (XO), S3, or division analysis and control element chief for at least 12 months; they must also serve as a brigade S2, in an intelligence officer position for at least 18 months, or both. These changes will bring the Branch-qualification requirements for MI Branch officers more closely in line with the Army Training and Leader Development Panel (ATLDP) recommendation to provide a better basis for officers to make personal assessments of their competitiveness for promotion and continuing Army careers.

**Change in Time-in-Grade for Captain Promotion.** The pin-on milestone for promotion to Captain increased from 38 months to 40 months this past April. We expect this to be the beginning of an incre-

mental return to the previous 42-month requirement. The current accelerated promotion rate was to alleviate the shortage of captains; since this shortage has ended, the Army is now returning to the longer developmental times for the Lieutenants before their promotion to Captain.

**Function Area 34, Strategic Intelligence Officer.** Some major changes that will soon impact FA 34 officers have been incorporated into two essential personnel documents, **DA Pamphlets 611-21 and 600-3.**

**DA PAM 611-21, Military Occupational Classification and Structure**, has now deleted all reference to the MI AOC 35B (Strategic Intelligence) and has added FA 34. This means that the Army has formally documented FA 34 within the Army and that 35B no longer exists as an AOC.

**DA PAM 600-3**, modification now requires only non-MI Branch officers to attend the Strategic Intelligence Officer Course at Fort Huachuca, Arizona, upon selection for FA 34 and before attendance at the Defense Intelligence Agency (DIA) Postgraduate Intelligence Program (PGIP). However, this does not preclude other officers from requesting attendance on a space-available basis. Additionally, the requirement for all FA 34 officers to complete the Master of Science in Strategic Intelligence degree has been dropped, but the requirement for all FA 34 officers to complete the PGIP successfully remains. The Army still encourages officers to apply for and complete the

Masters program but they will not automatically have any additional time at the Joint Military Intelligence College (JMIC) for this purpose. (In the past, some Masters candidates had received 50 to 80 days at the end of the PGIP program to do so.) This change shortens the time at the JMIC from 52 weeks to approximately 40 weeks. Finally, Branch qualification for FA 34 Majors has been changed to require these officers to serve 24 months (instead of the current 30 months) in an FA 34 position; for Lieutenants Colonel, this requirement changes from 48 months to 36 months.

**Upcoming Officer Selection Boards.** The selection board for Active Component Colonel will convene 29 July through 22 August 2003.

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



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

## New MIPB Website Address

The **Military Intelligence Professional Bulletin** will soon have a new Internet website address. The address will be <http://mipb.futures.hua.army.mil> and the alternate will be <https://www.futures.hua.army.mil/mipb>; our old address (which was <http://138.27.35.32/mipb/mipbhome/welcome.htm>) is no longer available although it has a hyperlink to the new address. While we transition to the new automated website, **MIPB** will not post the issues from April-June 2000 through January-March 2003. However, readers can contact [del.stewart@us.army.mil](mailto:del.stewart@us.army.mil) or [mipb@hua.army.mil](mailto:mipb@hua.army.mil) about those issues in the interim period.

# Sly Fox

## ASAS Master Analysts' Support to IO—Information Engineering

by Matthew J. Nunn

What does the All-Source Analysis System (ASAS) Master Analyst (additional skill identifier [ASI] 1F) bring to intelligence support to information operations (IO)? This will be the first of three articles discussing what the “Sly Fox” brings to the fight. The follow-on articles will address “Communications” and “Analysis.”

### Information Engineering Concept

The ASAS Master Analyst (ASI 1F) should be an essential player within the analysis and control element (ACE) during intelligence support to IO. The 1F brings extensive training in information engineering, communications, and analysis. Mastery of all three of these areas is paramount to successful orchestration of intelligence operations within the ACE. The balance of this article will deal with the Master Analysts and the value-added they bring in the area of information engineering.

The Information Engineering concept teaches the 1F to backward-plan to provide timely, accurate, and predictive intelligence products to the commander. The 1F is well schooled in developing the Communications Architecture (systems, capacity, protocols), Information Architecture (intelligence reports, data elements, and databases), and Information Shaping (products, detail, and fusion parameters).

### Communications Architecture

The first step in information engineering is the Communications Architecture developing a plan for the systems with which the ACE will need to interface. These include

sensors and collectors, internal and external communications, and various networks and workstations. After identifying the various systems involved, the ASAS Master Analyst will need to evaluate the capacity of the communications infrastructure to decide the types and sizes of products, incoming and outgoing, that it can support. Finally, there must be intimate familiarity with the various protocols used by the systems to ensure successful interoperability. The Master Analyst must be aware of the capabilities and limitations that any communications architecture presents.

### Information Architecture

The second step is Information Architecture, which comprises intelligence reports, data elements, and databases. Here the 1F will plan where the information and data will come from and into which databases it will parse. The Master Analyst must know what intelligence reports the system will be receive, how they will come, and the data elements that each will contain. Critical to getting the data elements into the appropriate databases for analysis, the 1F must understand how ASAS handles each type. For example, the Master Analyst must know the structural differences between U.S. Message Text Format (USMTF) and United States Signals Intelligence Directive (USSID) tactical report (TACREP) formats, in order to properly adjust and normalize systems for the receipt of each.

### Information Shaping

Information Shaping is the last step in information engineering. Information shaping will take into

consideration the product required, its context and detail and, as required, adjust the fusion algorithms (All-Source Enclave [ASE] related). The commander's preference, mission requirements, and the ability of the communications architecture to support dissemination will drive the types of products produced. Often briefings, text, and graphic reports will be necessary. How much detail is critical at a given time and the echelon defines the product; this in turn is driven by the commander, collateral recipients, and the level of detail that the workstations and communications can support. Finally, the Master Analyst will have to decide how to adjust (if required) the fusion algorithms (level of aggregation and node maintenance) on the ASE that will best support maintaining the picture for the product.

### Final Thought

The ultimate goal of ASAS information engineering is to enable the Master Analyst to combine data elements to create information to produce intelligence for the commander in a relevant, timely manner.



---

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

# 111th Training Notes

## Reorganization of the U.S. Army Intelligence Center

by Russell W. Watson, Ph.D., and George A. VanOttten, Ph.D.

To use scarce resources more effectively, Brigadier General John Custer directed the reorganization of the U.S. Army Intelligence Center and Fort Huachuca. Accordingly, on 1 April 2003, all training responsibilities other than those of the Non-commissioned Officer Academy, consolidated under the 111th Military Intelligence (MI) Brigade; the Army inactivated the 112th MI Brigade (Provisional).

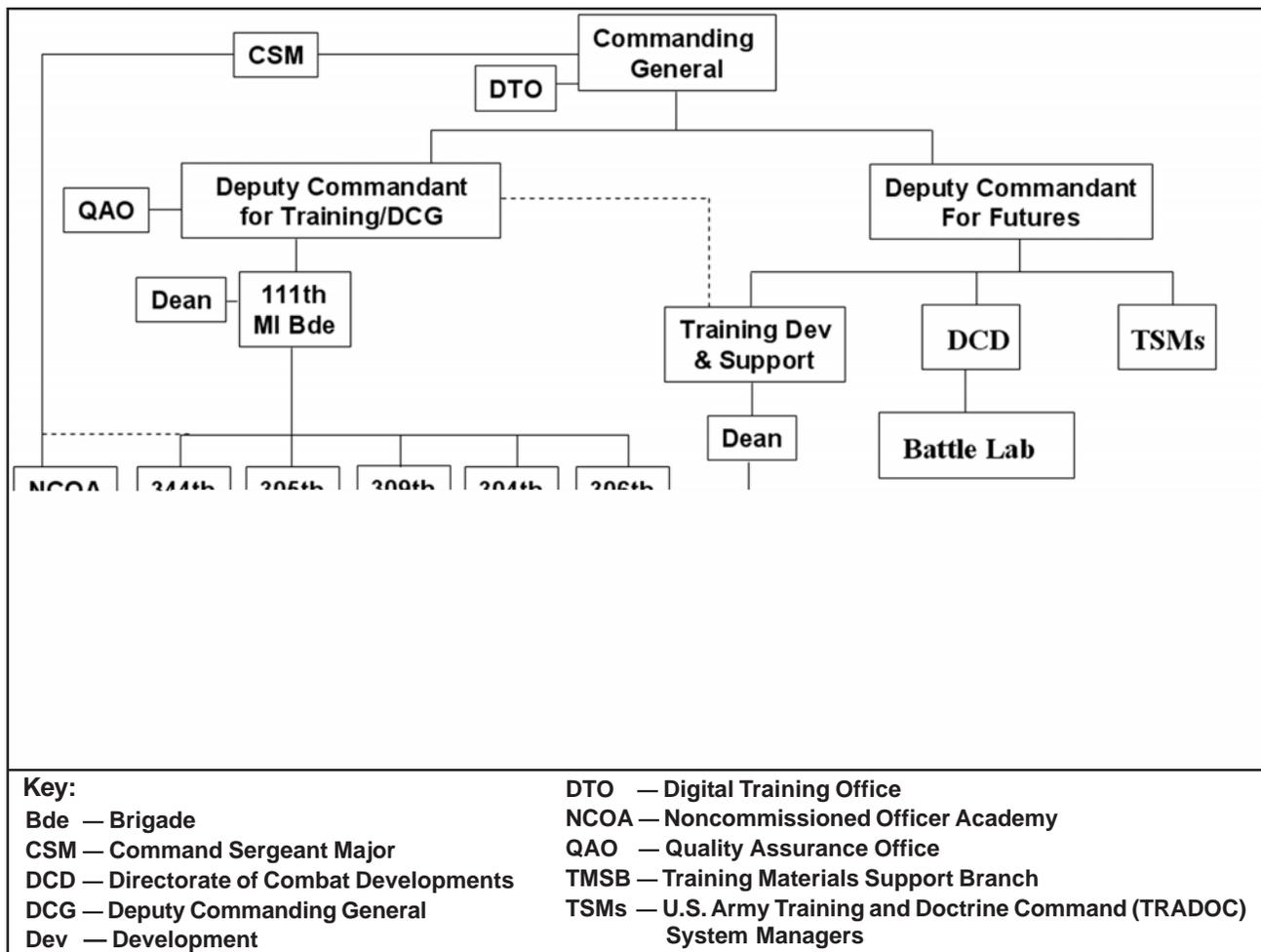
All training development and support missions, including the development of MI doctrine, transferred to the newly created Directorate of

Training Development and Support (within the Futures Development and Integration Center). Additionally, the MI Battle Command Battle Lab—Huachuca moved to the Directorate of Combat Developments. This realignment of functions better postures the Center to allow concepts to drive doctrine and doctrine to drive training development, resulting in current and accurate programs of instruction. The organizational chart depicts the new structure.

The Commander of the 111th MI Brigade is Colonel Michael T. Flynn and Dr. VanOttten is the Dean of the

111th MI Brigade; Colonel Jack W. Russell is the Director of the Directorate of Training Development and Support and Dr. Watson is the Deputy Director.

Readers may contact Dr. Watson via E-mail at [russell.watson@us.army.mil](mailto:russell.watson@us.army.mil) and telephonically at (520) 538-7303 or DSN 879-7303. You can reach Dr. VanOttten via E-mail at [george.vanottten@us.army.mil](mailto:george.vanottten@us.army.mil) and by telephone at (520) 533-5407 or DSN 821-5407. The 111th MI Brigade's website is available through <http://usaic.hua.army.mil/111bde/111th.htm>.



# Distance Learning

by John B. McGovern

An experienced Distance Learner, you participate and learn through distributive learning. You are doing so now. There are many places to go to learn, to study, and to build your knowledge base for enriching your personal and professional lives.

Do you remember reading **The United States Constitution**? Have you read it lately?

*We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.*

It is all there on the Internet at <http://www.house.gov/Constitution/Constitution.html>.

Each of you has a classic that you remember reading, perhaps in school. When was the last time you read it?

*I remember him as if it were yesterday, as he came plodding to the inn door, his sea-chest following behind him in a hand-barrow—a tall, strong, heavy, nut-brown man, his tarry pigtail falling over the shoulder of his soiled blue coat, his hands ragged and scarred, with black, broken nails, and the sabre cut across one cheek, a dirty, livid white. I*

*remember him looking round the cover and whistling to himself as he did so, and then breaking out in that old sea-song that he sang so often afterwards: 'Fifteen men on the dead man's chest—Yo-ho-ho, and a bottle of rum!' (You can find it at <http://www.online-literature.com/stevenson/treasureisland/1/>.)*

You can enhance your professional education as well through distance learning. Have you read this in Sun Tzu's work?

*Hence it is only the enlightened ruler and the wise general who will use the highest intelligence of the army for purposes of spying and thereby they achieve great results. Spies are a most important element in water, because on them depends an army's ability to move. (See <http://classics.mit.edu/Tzu/artwar.html> for more.)*

When was the last time you went to one of your own books and looked something up? You just wanted to confirm what you already knew or you wanted to refresh your memory. Nice features of digital libraries are the links you find, the ability to catch up on the latest changes in your areas of interest, the capability of refreshing yourself on past training, and the capability to see what your training future contains.

The U.S. Army is capitalizing on the wealth of knowledge already available and building more to hone the skills, knowledge, and abilities

of the force. Identifying the progress of the individual distance learner is high on the list of things we are doing to aid the learner. Learning management systems are evolving to do this.

When you visit the Military Intelligence Distance Learning site, you will encounter the current learning management system. If you have your password, you are in. If you do not have your user identification and password, you can request an account at <http://www.intel.army.mil/>. As you explore the wealth of knowledge available, you may find some of the material is not fully up on the latest Learning Management System. Use what you can. One of the other niceties is that your mind is free to explore new vistas and revisit those that feed your knowledge base.

As a Military Intelligence professional, you are invited to participate in another part of your distributive learning process. You will even find some of your career basics that you can experience again.



*John McGovern is the Senior Training Specialist as well as the Program Manager for the Broadband Intelligence Training System (BITS), Training Development Integration Division, Training Development and Support Directorate, at the U.S. Army Intelligence Center and Fort Huachuca. Readers may contact him via E-mail at [john.b.mcgovern@us.army.mil](mailto:john.b.mcgovern@us.army.mil). Robert Lane ([robert.l.lane@us.army.mil](mailto:robert.l.lane@us.army.mil)) is the individual responsible for the requests coming in through the Learning Management System on the website.*

## Security Releases Required With Your Articles

The **Military Intelligence Professional Bulletin** always welcomes your professional contributions! **MIPB** does require a release signed by your local security officer or SSO stating that your article and the accompanying graphics are "unclassified, nonsensitive, and releasable in the public domain." The release should include your name, the title of the article, and contact information for the person who signs the release. We must have a signed copy of the security release either mailed or faxed to us. If your installation or agency requires you to obtain a public affairs release as well, please do so.

# Professional Reader

## Stray Voltage: War in the Information Age



by Wayne Michael Hall (Annapolis, MD: Naval Institute Press, April 2003),  
248 pages, \$36.96, ISBN: 1-59114-350-0

In **Stray Voltage: War in the Information Age**, Brigadier General (U.S. Army, Retired) Wayne Hall provides an excellent treatise on information operations (IO) and their application to the battle for knowledge that very well may be the deciding factor in future conflict.

Future opponents, instead of engaging in conflict as it exists today, will attempt parity through "Knowledge Wars," battles for information that will permit making better and quicker decisions while denying the enemy the same advantage. Warfare will no longer occur as an exclusively "kinetic" exchange. An over-matched but well-funded, well-educated, and dedicated enemy will assume a more asymmetrical posture, simultaneously attacking well-coordinated targets, selected for cascading effect (much like the coordinated attacks of 11 September 2001.) Success in asymmetrical war will require knowledge and its application to an extent never before envisioned by man.

A "tapestry of systems" interconnects the world and people have the capacity to learn and change. Thanks to vast finances and very modern education, other organizations are or will soon be as technologically advanced as the United States. Distance and time will no longer count. People have never experienced the impact of technology as we can expect in the near future. Coordination can occur

worldwide, invisibly, at the speed of light. "Knowledge war" is inevitable, "information superiority" will belong to those who can best use the information technology, who understand the nature of future conflicts, who engage in asymmetrical conflict, and who successfully conduct "knowledge war." Deception, sophisticated and complex as it is, will become a great deal more so.

What must we do? Assemble the personnel, the thinkers, and educate them (or hire the expertise) and the equipment (much of which perhaps does not even exist today). Train, wargame, and develop cyber-warriors (men and women with the best computer and intellectual skills, planning capabilities, and understanding of political and economic, financial, and military spheres, as well as the existence of far greater relationships between man and machine). *Perhaps we should equip men with microchips or microprocessors that would enhance the sorting of mountains of information or recognize key relationships.* Should we employ cyberbots (programs to do functions digitally that man cannot (search out, acquire, retrieve, sort, stand sentry, decoy, manipulate, or destroy...digitally, at machine speed)? We must develop knowledge advantage centers to focus a vast network of agencies and knowledge workers. We should also develop a joint asymmetric opposing force, build a joint information operations proving ground, and develop and use an Internet replicator.

**Stray Voltage** is a frank and thought-provoking piece, providing a clear analysis of the highly complex problems the United States faces in IO and the way ahead, while spotlighting the formidable obstacles posed by our thinking and that of our bureaucrats. BG Hall does not sugarcoat the pill. He states for example that this country's military leaders need to acknowledge that we cannot develop the type person the cyber-warrior must be.

There is a great deal of good material out there with which to occupy one's precious reading time. Make time for this one. It is simply a must-read for all military and military intelligence.

**Dick Cameron**  
**Chief Warrant Officer Five,**  
**(U.S. Army, Retired)**  
Colorado Springs, Colorado

### 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, SIGINT, IMINT, war on terrorism, OEF, OIF, and tactical operations. E-mail them to mipb@hua.army.mil or call (520) 533-9968/1005 or DSN 821 or 879, respectively.



# Contact Information and Submissions



This is your magazine and we need your support in writing articles for publication. When writing an article, select a topic relevant to the Military Intelligence community; it could be historical or about current operations and exercises, equipment, TTPs, or training. Explain lessons learned or write an essay-type thought-provoking article. Short "quick tips" on better use of equipment, personnel, or methods of problem-solving and articles from "hot spots" are always welcome. Seek to add to the professional knowledge of the MI Corps. Propose changes, describe a new theory or dispute an existing one, explain how your unit has broken new ground, give helpful advice on a specific topic, or explain how a new piece of technology will change the way we operate.

Maintain the active voice as much as possible. Make your point. Avoid writing about internal organizational administration. If your topic is a new piece of technology, tell the readers why it is important, how it works better, and how it will affect them. Avoid lengthy descriptions of who approved it, quotations from senior leaders describing how good it is, or reports your organization filed regarding the system, etc. Note: Mailings become the property of **MIPB** and may be released to other government agencies or non-profit organizations for republication upon request.

The **MIPB** staff will edit the articles and put them in a style and format appropriate for the magazine. You can send articles, graphics, and photographs via E-mail to [mipb@hua.army.mil](mailto:mipb@hua.army.mil) or [del.stewart@us.army.mil](mailto:del.stewart@us.army.mil) and [liz.mcgovern@us.army.mil](mailto:liz.mcgovern@us.army.mil) or mail (with a soft copy on disk) to ATTN: ATZS-FDT-M, Bldg 61730, Room 105, U.S. Army Intelligence Center and Fort Huachuca, 550 Cibique Street, Fort Huachuca, AZ 85613-7017. (Please do not use special document templates and attach the graphics separately.) We can

accept articles in Microsoft Office 2000, Word 7.0, and ASCII; we need the graphics in Adobe, tif, jpg, Corel, or PowerPoint (in order of preference). Please include with your article:

- A cover letter with your work and home E-mail addresses, work telephone number, and a comment stating your desire to have the article published.
- A release signed by your local security officer or SSO stating that your article is unclassified, non-sensitive, and releasable in the public domain (see page 66).
- Pictures, graphics, and crests/logos with adequate descriptions. Submit clear "action" photos that illustrate your article with captions for the photos (the who, what, where, when, why, and how); the photographer credits; and include the author's name on photos. Please do not embed graphics in the article text.
- The full name of each author in the byline and a short biography for each. The biography should include the author's current duty position, related assignments, relevant civilian degrees (degree, school, major), and any special qualifications. (Please indicate whether we can print your telephone number and your E-mail address with the biography.)

We cannot guarantee we will publish all submitted articles but will send you a message acknowledging its receipt. We may notify you again when we get ready to publish it. Please inform us of any changes in contact information as it can take a year or more before we publish some articles.

If you have any questions, please call (520) 533-9968 (DSN 821) or (520) 538-1005 (DSN 879).



---

## Intelligence and Electronic Warfare

---

(Continued from page 50)

Common Ground System-Army (DCGS-A). The IEWTPT trains the battle commander by driving the command, staff, and intelligence information systems as wartime would drive them.



*Captain Misty Martin is the Commander of the Headquarters and Headquarters Company (HHC) at the Fort Knox Garrison, Kentucky. She is a graduate of Western Kentucky University where she received a Bachelor of Arts degree in Psychology. Commissioned as a Second Lieutenant in the Military Intelligence Corps, her previous assignments include Chief of Intelligence Systems*

*Fielding, New Systems Training Office, Fort Huachuca, Arizona; Unmanned Aerial Vehicle Platoon Leader, 304th MI Battalion; Analysis and Control Element Chief of Current Intelligence, I Corps; 555th Combat Engineer Brigade S2; I Corps G2 Intelligence Officer; and Chief of Tactical Fusion, 306th MI Battalion. Readers may contact CPT Martin via E-mail at [misty.martin@knox.army.mil](mailto:misty.martin@knox.army.mil).*

# 310th Military Intelligence Battalion

*Oriental blue is the primary color associated with the Military Intelligence Corps. Black and silver symbolize overt and covert operations and the organization's around-the-clock vigilance. The organization's Griffin embodies alertness; it is black, recalling determination and stealth. The unit's collection and exploitation mission is highlighted by the cramps or hooks. The hooks simulate flashes, representing speed and combat electronic warfare while alluding to the ability to catch and hold. Attached around the base is a black scroll doubled and inscribed "ARRECTIS AURIBUS," Latin for the unit's motto.*

Tracing its lineage directly from the U.S. Army Technical Services Detachment (USATSD), the 310th MI Battalion's lineage and honors originate with Headquarters and Headquarters Detachment, 310th Communications Reconnaissance Battalion.

On 12 April 1976, the USATSD redesignated as the U.S. Army Operational Security Group (OSG).

Reformed on 2 May 1977 as the 91st MI Battalion (Provisional), the Battalion received the U.S. Army Security Detachment Region I assets from the Signal Security Activity, Vint Hill Farms Station, Virginia. This enabled the Battalion to provide intelligence support covering the entire intelligence spectrum.

On 1 January 1978, the Battalion's designation changed to the Counterintelligence and Signal Security Support Battalion. Then on 1 October 1984, the Battalion redesignated as the MI Battalion (Counterintelligence) East Coast (known as the "East Coast Battalion").

On 1 October 1986, after four more realignment phases, the Battalion redesignated as the MI Battalion (Counterintelligence) (Technical). Under the new alignment, all previously assigned subordinate MI Detachments and Resident Offices were assigned to MI Battalion (Counterintelligence) (Security) [currently the 308th MI Battalion]. On 24 May 1991, Headquarters and Headquarters Detachment formally activated and in July 1991 consolidated into Headquarters and Headquarters Company. On 25 May 1992, the Army reassigned the Pentagon Counterintelligence Force [now a company] to the Battalion.

Redesignated as the Counterintelligence (Counterespionage) Battalion in the spring of 1993, the Battalion developed a multidiscipline approach to CI investigations, shifting away from single-discipline technical services to comprehensive counterespionage investigations. As part of this reorganization, the Battalion integrated several detachments into the Technical Support Detachment (TSD). TSD redesignated as the Technical Operations Company on 6 June 1994 and again redesignated as B Company on 1 October 1994.

On 16 October 1995, the Battalion shifted from a table of distribution and allowances (TDA) to an modified table of organization and equipment (MTOE) unit and redesignated as the 310th MI Battalion (Provisional).

The Battalion officially redesignated as the 310th MI Battalion on 1 July 1996 and unfurled its colors on Fort George G. Meade, Maryland, at the 902d MI Group change of command ceremony.

In early 1999, the Battalion transferred its Resident Offices to the 308th MI Battalion; the 310th Battalion received several elements from the inactivating 716th MI Battalion. These were the Army Counterintelligence Center, the Freedom of Information/Privacy Act Office, and the Investigative Records Repository.



**ALWAYS ON THE ALERT!**

ATTN ATZS-FDT-M (12)  
USAIC AND FORT HUACHUCA  
550 CIBEQUE STREET  
FORT HUACHUCA AZ 85613-7017

PRESORTED STANDARD  
U.S. POSTAGE & FEES PAID  
NIAGARA FALLS, NY 14304  
PERMIT NO. 28



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

PIN: 080837-00