Spring 2008

IO SPHERE

The Professional Journal of Joint Information Operations

Linking Virtual Worlds

Joint Information Operations Warfare Command

FEATURE ARTICLES

Spring 2008
IO SPHERE
The Professional Journal of Joint Information Operations
Linking Virtual Worlds
Joint Information Operations Warfare Command

Credit and thanks for our cover design go to our graphics editor, Ms Denise Maloney.

Printed by the Air Force Intelligence, Surveillance & Reconnaissance Agency Print Plant.

Staff

Maj Gen John C. Koziol, USAF
JIOWC Commander

COL Mark H. Johnson, USA
JIOWC Deputy Commander

Col John R. Roberts, USAF
Executive Editor

Mr. John W. Whisenhunt (SAIC, Inc.)
Editor

Ms Denise R. Maloney
Layout/Graphics Editor

ANNOUNCEMENTS

For the Record: The photo caption on page 34 of the Winter 2008 issue incorrectly identified Ambassador Mary C. Yates of USAFRICOM as Mary Ward. IO Sphere *apologizes for this error.*

SUMMER ISSUE SUBMISSION DEADLINE
31 MAY 2008

IO Sphere welcomes submissions of articles regarding full-spectrum IO, including its core, supporting and related capabilities and the integration of intelligence support.

SUBMISSION GUIDELINES

TEXT - Microsoft Word or Adobe Acrobat format

CHARTS/GRAPHS - TIFF or JPG format (if not 300 DPI please provide scannable hard copy)

PHOTOGRAPHS - TIFF or JPG (if not 300 DPI please provide scannable hard copy)

FORMAT/LENGTH - 1,500 - 4,000 words, double spaced

Please place graphs/photographs/charts on separate pages or as file attachments.

See the ***IO Sphere*** website from your .mil or .gov domain: https://www.jiowc.osis.gov or via Intelink at https://www.intelink.gov/wiki/IO_Sphere

Send Letters to the Editor, Articles & *Editorials* to:

iosphere@jiowc.osis.gov

Joint Information Operations
Warfare Command
2 Hall Blvd, Suite 217
San Antonio, TX 78243-7074

Phone: (210) 670-2676 x42
FAX: (210) 977-4166 or
(210) 674-5069

Disclaimer Statement

This Department of Defense publication **(ISSN 1939-2370)** is an authorized publication for the members of the Department of Defense. Contents of the ***IO Sphere*** are not necessarily the official views of, or endorsed by, the US Government, the Department of Defense, or the Joint Information Operations Warfare Command. The editorial content is edited, reviewed for classification, prepared, and provided by the J7 Office of the Joint Information Operations Warfare Command. All photographs are the property of the JIOWC, unless otherwise indicated. Send articles, *Letters to the Editor*, or byline editorials to Joint Information Operations Warfare Command, Attn: ***IO Sphere*** Editor, 2 Hall Blvd, Ste 217, San Antonio, Texas 78243-7074 or E-mail: iosphere@jiowc.osis.gov

Articles in this publication may be reproduced, with permission. If reproduced, ***IO Sphere*** requests a courtesy line or source citation.

Commander's Comments

Much of what our contributors offer this quarter deals with "cyberspace." We use this expression many times daily, attaching it to everything from our boldest strategic plans to our simplest email shopping lists. Yet, if we get network warriors, lawyers, and sociologists together, we can debate its meaning for another 25 years. The number of net-enabled cultures has increased tremendously, but have we really invented a new realm? Many observers and theorists agree we have. Discussions often view "cyber" as a prefix easily tacked onto any word to suddenly make it computer or electronic-related. This is a very limiting perspective, which constrains both our understanding and our best uses of this potent word. It's important to note this expression grew from the term "cybernetic," first used in the late 1940s, and derived from a Greek expression which literally means "the art of steering." Scientists and engineers had to understand a system well enough to model it, construct an electronic equivalent, and have the solution perform as a high fidelity replica of the original. So in a sense, the "cyber" prefix originally meant remotely navigating through some known functional process; lately we've been applying it to even larger, more complex systems.

Many are familiar with the evolution of the expression "cyberspace," from author William Gibson's 1982 need to express a fictional connectedness of humanity, to current detailed philosophical explorations of a "place." It makes sense to refer to it this way, because millions of us earn a living, have a dialog with others, and even help fight extremism there. In the early days of the telephone, did people worry about where the conversation took place? Was it "inside a wire," or in a wall-mounted box? What has really changed is our understanding of "where." In the intervening century, this realm grew at an astounding rate, and in multiple virtual directions. We no longer think of such space as simple conduit; it has become a big enough place to do much of our daily cultural exchange, our business—and for some, to carry out malicious actions. Yet, there is plenty of room to live, thrive, and create. Like any place worth living, it is also well worth protecting and defending.

Without a doubt, cyberspace is a tremendous place to carry our influence operations. Anyone, wired or wireless, can explore opinions, facts and philosophies, and convince others on literally any discussion topic. Many view dominance of this domain the way the great powers viewed control of the seas in the 15th-17th centuries, the air in the early 20th century, and space in the latter portion. The same oceans which served as a grand buffer to keep foreign forces off US soil do not deter our network-enabled adversaries. Unfriendlies can deliver everything from annoying Spam email to devastating electronic attacks from nearly any connected location on the globe—no matter how great the physical space between us.

As an outgrowth of our longstanding success in DOD network protection and Information Assurance efforts, many have historically viewed the cyber-battlespace as a primarily defensive arena. As cyberspace operations mature, we are expanding beyond this, developing new concepts of operations plus tactics, techniques, and procedures (TTP). Joint warriors across the Services (read about the Marine Corps' newest effort on page 48) are vigilantly working on the best ways to support Joint Force Commanders across this new spectrum. Yet many nations are exploring and even employing some form of offensive cyber weapons. Dealing with such threats requires we exercise both strong initiative and extreme care. Cyber weapons can quickly transit global networks, using otherwise "neutral territory" to bypass existing national and international protections. This raises numerous questions for those developing rules of engagement, laws of armed conflict, as well as how we determine operational phases. How can we be certain what second and third order effects "going after" a cybercriminal or cyberterrorist will generate? Transiting cyberspace is at once a daily routine, and a dangerous journey—if we're unprepared for the trip. Consequence management is a big part of joint planners' daily lives, yet cyberweapons demand we thoroughly examine each one, to ensure our fullest understanding of any possible consequences. Like the special weapons of the Cold War, surety plays a huge role, so expect cyberweapons authority to generally remain at higher executive levels.

So how do we use cyberspace? If we're good joint planners, we do it "very carefully." Experts among us deal with evolving issues of cyberops, cyberlaw, cyberphilosphy, and cybercrime each day. If you'd like to contribute a discussion in any of these areas, we look forward to your views. (iosphere@jiowc.osis.gov)

John C. Koziol
Major General, USAF

Applying IO in the Real World

By James G. Dewar, Major, British Army

We are all IO professionals, passionate about what we do, and our ability to make a positive difference in the battle space. Otherwise, why would you be reading this?

Do any of these scenarios seem familiar? You've read the operations order and listened to the General Officer expound on the critical nature of winning the "information battle." You measure this against available resources: two junior officers fresh from the IO course; a Chief of Staff who can neither spell 'IO' nor see the need for a weapons system that doesn't go bang; and 38 PSYOP professionals in a force of 11,000.

Do I exaggerate? Only slightly, for I've been in precisely these situations in Bosnia, Iraq and Afghanistan. In situations such as these, personality plays a critical role—one that it should not. Why is this? No officer that makes it past platoon commander would question the necessity and contribution that *all* elements of the team play in mission success. They may make fun of their counterparts in the other services, but they understand the part they play. Moreover, they also understand that though they have a view on the utility and employment of the other teams' assets, they bow to the superior knowledge of specialists. They also take exception to having their professional knowledge questioned by anyone outside their specialty. So why doesn't this attitude extend to IO and IO professionals?

Where does personality come into this? Firstly it is highly unlikely the commander will be either an IO professional or have come from any of the core or supporting capabilities. Almost certainly he will be a "J3 snob," schooled in the certainties of combat power, with instant success or failure confirmed by BDA. If you are lucky, he will have seen IO work in previous operations and therefore be predisposed to embrace it. That said, even in the early part of the 21st century this is less likely than having a commander with no IO knowledge or experience. If so, he will have to be a strong and open commander, willing to embrace "new" ideas and the patience to wait for the results. Should this not be the case, then the second personality comes into play: the collective personality of the IO team. They must be capable, professional and strong so that they can win the first battle in the IO war: convincing the commander and his staff that IO is critical to mission success.

In Bosnia we faced exactly this issue. The PSYOP team produced a weekly paper called *Mostovi* which ran up against a weekly print deadline. Not because we were inefficient, but because we had to chase it through the approval process every time. No one in the process believed it was an important part of the campaign, therefore it was never a priority. The prevailing attitude was that it was a lot of effort to make 'fire starters' for the locals. We needed to prove that people read it, that it was a local means of communicating. So we decided to run a readers survey on the back page of one issue. The survey asked a few questions about national issues, plus readers' opinions of the paper, and what we could do to make it better. To spice the pot we offered a prize for the most constructive comments: a credit card FM radio then used as a promotional tool by a British bank. When we explained what we were going to do, the idea was met with howls of derision, with the general opinion that it would be a waste of time—particularly as respondents needed to give an address in case they won the prize. At the time the circulation was 35,000, and a generally accepted rule of thumb in the UK was that about 5% of readers regularly responded to such surveys. We received 15,000 replies. Approval issues disappeared, people were only too happy to be interviewed, and rather than paying the printing contract from the HQ stationary budget, we received properly approved funds.

Sometimes two strong personalities come together, and when they do, you don't have to battle the staff. Such was the case in Afghanistan where the regional commander "got it." He encouraged the IO team and challenged them to make a difference. On many occasions he noted we were not just there to kill the Taliban—we would do that as required—but ultimately the solution lay with convincing the locals to support the Government of Afghanistan and reject the Taliban. Did the commander feel this way before arriving in Afghanistan? I do not know, but his IO chief was a strong, capable and intelligent individual, accepted into the inner command circle, and therefore had his ear. All of these were significant contributing factors. The opposite was the case during my tour in Iraq, where the IO chief was not accepted into the 'inner circle.' Consequently, even when he had good ideas no one listened, and his very capable team was sidelined.

Should the success of the IO campaign rely on this cult of personality? Of course not. So how do we overcome this problem? I believe we must tackle three areas, and they lie in our own hands to influence. We must ensure that all we do is properly planned—by this I mean we must not pay lip service to MOE. It is a difficult issue to deal with, but if we do not fully consider how to benchmark attitudes then measure any changes, we are destined to fail. If we cannot measure the effect we are trying to achieve we are wasting our time, and should look at other options. Secondly, we must improve IO training, not of the practitioners, but of those who command and control the capability. They must know what IO is and what it is not. We can manage commanders' expectations so they will understand that the "long war" will continue long after they hand over, thus becoming unwilling to accept last minute augmentees and ask "where is my IO staff." Finally, as IO professionals we must live up to that title and push against closed doors. We must never accept IO being paid lip service in planning, exercises and certainly not in operations.

Major Jim Dewar, Princess' of Wales Royal Regiment, is an IO & PSYOP planner in the JIOWC EUCOM Division, and the JIOWC United Kingdom Exchange Officer.

Cyberskepticism: The Mind's Firewall

By Timothy L. Thomas

Editorial Abstract: Mr. Thomas examines various forms of computer network-related deception, including technical and social exploitation. He examines how deceptive practices can be easily concealed within existing cultural and network constructs. Finally, he advises adoption of a proper mental framework to help defeat this class of cyber threats.

Introduction

In 2004, computer hackers in the Netherlands developed a way for unsuspecting computer users to download a virus. Their vessel for doing so was a photo of Russian tennis star Anna Kournikova, a heart throb to many young male tennis enthusiasts. As *SearchWindowsSecurity* reported:

The Anna Kournikova VBS.SST computer virus, informally known as "Anna," is a viral worm that uses Visual Basic to infect Windows systems when a user unwittingly opens an e-mail note with an attachment that appears to be a graphic image of Russian tennis star Anna Kournikova. However, when the file is opened, a clandestine code extension enables the worm to copy itself to the Windows directory and then send the file as an attachment to all addresses listed in your Microsoft Outlook e-mail address book.

Such cyber deception is, unfortunately, quite common. Episodes involving cyber deception occur daily and, in some of the worst cases, have resulted in suicides, identity theft, financial scandals, assists to pedophiles, and "cybercide" (inadvertently taking down your own network by downloading and propagating a virus). Most recently hackers have tried to penetrate the Pennsylvania Lottery. Consider the ramifications and consequences if they are successful in this endeavor!

The context that ignites cyber deception is the similarity between reality and digitally generated forms of communication (text, video, etc.). This confrontation was fully brought into focus in the 1983 film *War Games*. A computer named Joshua, while playing a game initiated by young computer wizard David Lightman (actor Matthew Broderick), takes control of all US nuclear weapons and begins a count down to launch them and start World War III. Lightman asks Joshua if he is playing the game or playing for real. Joshua answers: "What's the difference?"

Cyber deception utilizes the similarity between reality and digital communication to exploit cognitive biases in human decision-making. These biases prey on a human's proclivity to accept rewards, romance, charity, or other feelings of sensitivity and emotion; or in some cases exploit habits or environmental influences (gambling, participation in scams, etc.). Since real issues and digital issues often coincide, humans are easily enticed into believing that what is false is real, and vice versa.

This article explains the context within which cyber deception has fermented. It then offers several examples of the forms that cyber deception has taken in recent years. The study of cyber deception has obvious value for a military audience—it is a key element of IO and OPSEC. In fact, some of the best OPSEC advice available is to "be a cyberskeptic."

Social Engineering

Kevin Mitnick, Noted Social Engineer. (Matthew Griffiths, Wikipedia.org)

Information security expert Mark Edmead, writing about famed computer hacker Kevin Mitnick (who exploited human vulnerabilities to the maximum extent possible), noted:

According to Mitnick, all of the firewalls and encryption in the world will never stop a gifted social engineer from rifling a corporate database or an irate employee from crashing a system. If an attacker wants to break into a system, the most effective approach is to try to exploit the weakest link—not operating systems, firewalls or encryption algorithms—but people.

Pitting one's cognitive skills and beliefs against a person or system to access a product, a password, or some other type of information is a process known as social engineering. *Wikipedia* defines social engineering as:

"*A collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.*"

Social engineering tries to fool decision makers, and is really nothing more than an updated term for stratagems used by the Chinese thousands of years ago for similar purposes. There are many social engineering techniques, several of which are highlighted below:

- Pretexting—the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is typically done over the telephone.
- Phishing—a technique of fraudulently obtaining private information, typically by sending an e-mail that looks legitimate.
- IVR/phone phishing—technique using an Interactive Voice Response (IVR) system to recreate a legitimate sounding copy of a bank or other institution's IVR system.
- Trojan horse/gimmes—technique taking advantage of a victims' curiosity or greed to deliver malware.
- Road apple—a real-world variation of a Trojan Horse using physical media and relying on a victim's curiosity

(leaving a CD or USB flash drive in a place where it will be found).

• Quid pro quo—technique involving a random caller who states that he is from technical support in an attempt to find someone with a problem and then guide them through commands giving the caller access or the ability to launch malware.

Cyber deception exploits in electronic fashion older deception techniques known as "confidence tricks." These are the con games or scams that try to swindle a person after gaining their confidence. Confidence tricks enable cyber deception successes in get-rich-quick schemes; romance, extortion, gambling, false injury or false reward, and charity tricks; and undercover cop scams, among others.

A Fertile Playing Field

The number of cybersites that consumers depend upon daily has grown considerably over the past several years. A tiny fraction of the digital playing field includes: e-mail; *MapQuest; Google; FaceBook; Flickr; MySpace; phonebook; BitTorrent; iTunes; YouTube*; forums; chat rooms; dating; *Craig's List*; donate; blog/vlog; video games; e-invitations; e-cards; weather; text messaging; financial planning; personal websites; picture sharing; airline travel; banking; test preparation; college classes; and cell phones.

Within these cyber circles, especially when *FaceBook* and *MySpace* were startups, common ideological thought or interests served as strong bonds. Virtual trust accumulates among individuals or groups even though an actual "meeting" has never occurred. Cyber tribes form. Unfortunately, as virtual trust grows so does virtual and cognitive vulnerability. For example, someone posing as an adherent to a cause can enter a group and gather information, manipulate the group's way of thinking, or embarrass the group by pretending to be a group member but publicly criticizing its cause. This can fool readers of a website into believing that group members are not cohesive, among other consequences.

(US Navy)

"... any source, no matter how trustworthy, can turn into a cyber deceiver."

Virtual size is another factor influencing cognitive deception. On the Web, it is very easy for one or a few people to appear to represent thousands simply through the number of messages produced. Virtual quantity, as the saying goes, has a virtual quality (in this case sheer size and thus influence) all its own that persuades via peer pressure or some other uniting factor.

While the main focus of cyber deception is to manipulate a person's cognitive perceptions, software can be manipulated as well (since humans write it!). Software is the unsuspecting agent that spreads false, selective, or viral material. Web crawlers are one of the most obvious tools that can produce cyber deceptive material. For example, they can determine website content. Depending on how an algorithm is written, a Web site will gather some data and discard others. An Al Qaeda website may eliminate all information about Christianity, thus deceiving subscribers about both the nature and popularity of the religion. In this case it can be both false and selective.

In another instance, Web crawlers are often designed to match advertising to fit the content of the website. Some of those advertisements could be illusions of grandeur designed only to collect money from unsuspecting readers. Machines and software thus begin to control people through monitoring and manipulation. The cyber deception malady is present in both people and software.

While criminals and terrorists use cyber deception to collect data, cyber deception can also be used by website moderators to provide false information to the consumers visiting the site. In fact, cyber deception is one of the most common ways for law enforcement personnel to catch pedophiles.

Nicholas Carr, former executive editor of the *Harvard Business Review*, believes that artificial intelligence experts have not only succeeded in rewiring our computers but humans as well. From his point of view, people are beginning to process information as if they were nodes with regard to speed of locating and reading data. If we only tend to go to certain websites, then much like Web crawlers we only access certain types of information. This allows machines to transfer their way of thinking into humans—if the latter don't take the time to process and analyze the information.

Of course, there are a plethora of cyber deception examples from which to choose. Even a small selection demonstrates the widespread use of cyber deception . They also demonstrate any source, no matter how trustworthy, can turn into a cyber deceiver, sometimes without the source's knowledge.

Cyber Deception From an Unlikely and Trusted Source

One example of cyber deception from a trusted source involved the *San Francisco Chronicle*. The paper's website, *SFGate.com*, posted comments from readers. The paper's moderators found a way to 'neuter' what they considered problem comments. The moderators were able to do so without making it appear that a comment had been eliminated due to ideological concerns. Their methodology went as follows. When a problem comment appeared, the moderators found a cyber or digital way to eliminate the comment from the Web page for all viewers *except* from the person who submitted it. That way, the person submitting the comment was satisfied that his or her opinion had been expressed and was still "out there" on the Web. The moderator's deception was exposed when a person who had submitted a "problem" comment tried to view his comment from a computer other than his own (he wanted to show it to a friend). His comment was not there. He returned home and found the comment still on his personal computer. He then wrote to the *Chronicle* and they admitted the cyber deception. This group carried out dual cyber deception: the moderators fooled both their public into thinking there wasn't any criticism of the type leveled by the individual, and the individual was cyber deceived into thinking his posting was still online.

Another case of cyber deception was based on comments from entrepreneur Dan Ackerman Greenberg. He described some secret strategies behind the creation of viral videos—those Internet videos that really take off and become popular "must sees" such as Soulja Boy, Miss Teen South Carolina, and Smirnoff's Tea Partay music video. In essence, his strategies to make videos viral were cyber deception methods. For instance, he recommended paying people who run relevant blogs to post embedded videos. As a result, what "seems" popular has actually been pre-financed through blog masters, thus cyber deceiving the audience ("this video is on the most watched list, it must be good"). Greenburg would also create huge friend lists on *Facebook* and then send all of them a video. He would ask that his friends e-mail the video to their friends, or at least share it on *Facebook*. He would also change the name of the video so that it would appear new, though people were simply visiting the same site. At times he would have conversations with himself, recommending the video to others, or have others in his office post comments about the video and get a heated conversation going about the video. Thus his virtual conversations and other methods acted to cyber deceive many people, causing them to either watch the video or go find it, because it appeared popular. Greenberg concludes by noting that "true virality takes serious creativity." Virtual creativity is thus another cyber deception methodology for IO professionals to explore.

Cyber Linking the Virtual World With the Real World (Especially Romance)

In January of 2007, storms were battering Europe and more than 230 people had died. On the Web there appeared an article called "Full Story.exe." While providing more information on the storm, the story provided a damaging storm of another type. The file, of course, contained a virus dubbed the "Storm Worm." As *Time* magazine reported:

> *... the virus is a marvel of social engineering and "it is to viruses what Michelangelo was to ceilings." Its subject line changes constantly, it preys on shock, outrage, prurience, and romance. It mutates quickly, changing its size and tactics often to avoid virus filters. It exploits blogs and bulletin boards. It contains links to fake YouTube pages which crash your browser. More importantly it provides others with access and control over your computer.*

Real-world romance techniques on the Internet have produced some very innovative cyber deception techniques. Valentine cards sent electronically are one technique designed to enhance romance. In 2006 electronic Valentine cards were sent to unsuspecting people who opened them for various reasons (do I have a secret lover?). Some of the messages arrived "having been forwarded by or appearing to have been forwarded by people known by the recipient." While piquing one's curiosity, it also tricked people into infecting their computers.

Recently, the Russian language website CyberLover.ru was identified as capable of holding "fully automated flirtatious conversations with users of chat-rooms and dating sites, to persuade them to share their identity or visit websites with malicious content." An English version of the site has not yet appeared. The site can establish a relationship with up to ten people in thirty minutes, and purportedly its victims cannot tell whether there is a human or a computer generated response on the other end. Sergei Shevchenko, a *PC Tools* senior malware analyst, says the site "monitors the victims' Internet browser activity, automatically recognizes and fills in fields in the Web pages, generates keystrokes and mouse clicks, and posts messages, URLs, files, and photos." Clearly this is a marvel of current cyber social engineering and deception skills.

Cyber Deceptive Visitors

Important websites, such as those run by NASA, the US Army, hospitals, or the UK's Ministry of Defense, are visited thousands of times each month by people from all over the globe. Not all visits are innocuous, however. Several visitors are most likely intended or designed to simply gather data. Some may also use anonymizers to hide their true identities. The UK's Counter Terrorism Science and Technology website recently posted "who" had visited its website, to include potential suppliers. Information of this sort can be "precisely the kind of fodder gathered in foot printing exercises, in which attackers learn as much as possible about sites they intend to penetrate."

Cyber Deceptive RFID Tags

A radio-frequency identification (RFID) tag is a chip with imbedded data. When the tag "hears" a particular radio signal, it broadcasts its number, thus becoming "located." Such chips are implanted in dogs, books, and other articles to find them when they are lost. However, if the tag is removed and placed in another receptacle, then those seeking the chip will be cyber deceived into running after another source. You may be searching for a German Shepherd, but may instead locate a horse, sheep or snake depending on who hosts the chip. A more sophisticated use of the RFID chip would be stealing information from passports or security cards, which also send out a signal. Someone walking near you with a reader could get your passport or security card information. Such information could be placed in another chip or just the information itself could be used to confirm someone's identity. Some people have begun wrapping their passports in metal foil to make their information harder for RFID readers to access.

Cyber Deception to Breach Firewalls

The November 2007 issue of *Wired* magazine provided a list of methods to breach information security. First, it was recommended to go 'in disguise.' Using this cyber deception method involves using proxy servers and other software to mask location and identity. Not long ago *Foreign Policy* magazine noted that a system known as Tor was "a downloadable software that routes an Internet surfing session through three proxy servers randomly chosen from a network of more than 1,000 servers run by volunteers worldwide." This cyber deception method frustrates law enforcement agencies from finding the source of a criminal or insurgent message. Keystroke tracking software installed on keyboards allows for cyber monitoring in cybercafés to keep track of messages being sent out without the user's knowledge. Of course cyber proxies could be used against any target. Other more straightforward methods suggest common sense ideas, not nearly as sophisticated. These include scrambling messages using encryption, posting on sites rarely monitored, searching overseas versions of a website, avoiding controversial terms, and using Skype [internet protocol telephone].

Cyber Deceptive Advertising

Some eighteen months ago, *MySpace* ran online banner ads infected with adware. This allowed malware to surreptitiously track infected users' Internet usage while bombarding them with pop-up ads. In a similar episode, users were invited to download a Sudoku game to pass the time. Attached to the Sudoku game advertisement was adware providing the same type of cyber tracking.

Cyber Deception Techniques Of a Hacker

Noted social engineer Kevin Mitnick, who was arrested and served time in prison for hacking into computers, wrote the best book on cyber deception available on the market today. Titled *The Art of Deception*, he describes how he enticed people into providing passwords and codes through social engineering techniques.

Mitnick noted that firewalls and biodetection systems are great ways to prevent hacking, but that training people to spot social engineering techniques is just as important. For example, one way to get information on cyber access codes is to call an unsuspecting person at a company and pose as an associate. This initial discussion will focus on troubleshooting a nonexistent network problem for the unsuspecting person. After pretending to have fixed the problem, Mitnick says the "associate" would ask for a favor, playing on a human tendency to reciprocate for a good deed. He notes this "causes people to take a mental shortcut, based not on the request, but the favor."

Practicing cyberskepticism. (US Army)

Cyber Phishing

No discussion of cyber deception would be complete without a discussion of phishing techniques. According to *Wikipedia*, phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing often directs users to enter details at a website. Current attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical measures.

Among the thousands of phishing scenarios, several come to mind. One was the attempt to access personnel databases on people who had visited the Oak Ridge National Laboratory, starting from 1990. Staff members received hoax emails that at first glance appeared legitimate. Such messages gave information to members of a scientific conference and another pretended to have information about a Federal Trade Commission complaint.

Cyber Deception and Hoaxbusters

In an odd way, explicit warnings about viruses, and our concern about downloading a virus inadvertently, have helped spawn a number of Internet virus hoaxes. A hoax uses a hook, a threat, or a request to get someone to believe in a fake message or chain letter and send it on to someone else or take some sort of action. Hoaxes adopt many of the principles associated with social engineering. The website http://hoaxbusters.ciac.org has listed a series of hoax categories: malicious code warnings; giveaways; chain letters; urban myths; sympathy hoaxes; threats; inconsequential warnings; scams; scare chain letter; jokes; true legends; hacked history; and stories with unknown origins.

Cyber Deception By Insurgents

Insurgents now plan, recruit, teach, and finance on the Internet. Further, they deceive through a variety of techniques that military planners must consider. A member of the US Army Foreign Military Studies Office (FMSO) accidently discovered one of the most interesting techniques. It involved a cyber deception strategy known as "hide in plain site."

The FMSO analyst was looking over a website focused on Arab entertainment. By chance, his hand slipped on the mouse and pulled the cursor to the bottom of page two. There, out of site unless you knew it was there, was a counter mechanism counting backwards to zero. Then the counter disappeared. Curious, the analyst got out of the site and went back in, immediately scrolling to the bottom of page two. Again he saw the counter before it disappeared. Once again, the analyst exited the website and reentered, but this time he clicked on the counter. The link took him directly to an extremist insurgent website. This is cyber deception of a still different type, in which the access point 'cybervanished' after a certain time period.

Cyber Address Book Harvesting

Some programs are specially designed to steal the computer address book of, let's say, Mister X. When this occurs, the address "harvester" then uses the address book to send out spam or viruses with the added line "this email was sent to you on behalf of person X,"—the one whose address book was stolen. Since the information was sent to you on behalf of someone you already know and regularly correspond (X), more often than not the intended target will open the email.

Cyber Deception Via Satellite

The Russian military has explored the use of cyber deception's adaptation to a concept known as 'reflexive control' (similar, but not identical, to the US term 'perception management'). Reflexive control (RC) consists of transmitting motives and grounds from the controlling entity to the controlled system that stimulate a desired decision. The goal of RC is to prompt the enemy to make a decision unfavorable to him. Naturally, one must already have a good idea about how the enemy thinks to make such attempts successful.

Russian theorist Colonel Sergei Leonenko initially thought the use of computers would hinder the use of reflexive control since computers would make it easier to process data and calculate options. A computer-aided opponent could more easily "see through" a reflexive control measure by an opposing force, due to greater speed and accuracy in processing information. He later surmised, however, that computer use may actually improve the chances for successful reflexive control, since a computer lacks a human being's the intuitive reasoning. Leonenko suggests acting against technical reconnaissance assets, especially weapons guidance systems, which are impassive in assessing what is occurring and do not perceive to what a person reacts. He believes we live in a frightening time if, in fact, decisions are in the hands of machines "incapable of assessing what is occurring, and do not perceive what a person reacts to."

Conclusions

The major conclusion one can draw from this explanation is that in the cyber age, people have to develop a strong sense of cyber skepticism. Skepticism should not be limited to computer operators; a healthy dose should be present in Blackberry, iPhone, cell phone, and other digital device users. Without skepticism, users and operators are almost certainly doomed to exploitation by electrons somewhere, sometime. The article you are now reading could also have elements of cyber deception, since much of the information was taken from the Internet without a sure way of confirming the material's authenticity!

Cyber deception has practically evolved into an art form. It is creative, invasive, and, as Kevin Mitnick noted, strongly dependent on social engineering techniques. Before the development of the personal computer, people were fooled by confidence tricks. But these same people were never exposed to the onslaught of cyber deception attempts, nor the consequences of successful attempts (the emptying of your bank account is but one possible result) that people experience today.

The number of terms involved with cyber deception causes confusion among computer users who are not dedicated to the study of information security issues. This also increases a computer user's susceptibility to attack. For example, a recent BBC report listed several cyber deception techniques other than those listed above. The average home computer user may not totally understand the effects of the following: pharming (fraudsters redirect net users from legitimate to fake sites); rogue dialing (software that installs itself on computers and changes settings to dial a premium rate number instead of usual dialup accounts); spyware (small programs that secretly monitor sites visited); keylogging (software/hardware to track keystrokes on a computer to gather passwords and credit card numbers); and other terms related to deceptive scams on personal computers.

The bottom line: be a cyberskeptic. Only in this way can we erect an effective cognitive defense against the many forms of cyber deception. The mind has no firewall—except skepticism.

Tim Thomas, LTC, US Army, Retired, served as a Soviet/Russian Foreign Area Officer. His assignments include brigade S-2 and company commander in the 82d Airborne Division, and the Army Russian Institute. He has done extensive research and publishing in the areas of peacekeeping, IO, and PSYOP. He currently serves as a Senior Analyst in the Foreign Military Studies Office, Ft Leavenworth. He holds a BS from the US Military Academy at West Point, and Master of Arts from USC.

A Multi-Dimensional Model for PSYOP Measures of Effectiveness

By Robert L. Perry

Editorial Abstract: The author examines an imperative need to predict, recognize, and measure convincing evidence of PSYOP and IO effects. He describes the limitations of current assessment methods, and offers a comprehensive, multiple variable, continuous interaction model that will produce different effects over time.

"MNC-I conducted very effective PSYOP encouraging noncombatants to leave the city and persuading insurgents to surrender. These doctrinal psychological operations might have been the most important aspect of our operations to defeat the enemy in Fallujah, as some estimates showed that 90 percent of the noncombatants departed the city." [1]

The quote gives significant credit to Psychological Operations (PSYOP) for a major victory in Operation Iraqi Freedom. But how do we know for sure? The actual information in the quote, and the large Information Operations effort of which the PSYOP was one part, shows the difficulty of measuring the actual effects of PSYOP—or any IO campaign for that matter. In the actual effort, the well-known Operation Al Fahr (also known as the second battle of Fallujah), LTG Thomas F. Metz, the Commander, insisted that all forces develop "courses of action to mass effects in the information domain" by "synchronized, integrated, and complementary actions." [2]

His highly complex IO campaign before, during, and after kinetic actions raises the inherent difficulty that this article seeks to address: researching and assessing measures of effectiveness (MOE), in a dynamic environment with multiple sources of influence (both kinetic and non-kinetic) on human behavior.[3]

For many years, PSYOP has been criticized, their potential positive effects misunderstood, their methods underutilized—and their results discredited—in part because "their actual effects are so difficult to observe and quantify," stressed Christopher J. Lamb.[4] A long term significant factor has been developing, applying, and assessing meaningful MOEs that accurately reflect whether or not a PSYOP significantly influenced an adversary to engage in a desired behavior. Among the many factors (lack of intelligence resources for effective early planning and lack of resources for effective post-operation assessment) contributing to the MOE problem: the high expectation often placed on seeking "cause and effect" relationships in highly complex situations. This article explores the shibboleth of the "cause and effect quandary," then suggests a flexible three-dimensional model that might be analyzed in more depth, and tested to determine its usefulness in providing a more robust view of PSYOP effects.

The 2006 Joint Publication 3.0, *Joint Operations,* defines a measure of effectiveness as "a criterion used to assess changes in the system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect."[5] It defines an MOE as a criterion, a standard of judgment. This critical word *choice* means that designing meaningful PSYOP MOEs is affected by the standards of judgment used to measure the desired outcomes. Following through with the Fallujah example, the commander stated one of his objectives was to "remove noncombatants from the town." Designing an MOE to meet that objective would require a PSYOP officer to clearly understand what the commander meant by 'remove' and 'non-combatant.' He could gain that information from the commander's written intent and desired end states, or he could ask the CDR for specific parameters. How many—quantity—will have to leave to meet the commander's intent: 100% of all persons not carrying weapons, 80% of women, children, and men over age 60, etc? How far from Fallujah—distance—should they go to be considered "removed?" How long should they stay away—persistence? The answers to these questions establish the standards of judgment; they make assessing PSYOP results easier because they can be defined, their attributes analyzed, and their parameters/bounds determined. As a standard of judgment, MOE offers a way to explore more broadly and more deeply the relationship between a PSYOP action and its effects and be better able to account for the observed results and their persistent effects.

The core issue, as Carrie Gray and Edwin Howard jointly and David Grohoski separately acknowledge, is the ability to predict, recognize, and measure in some meaningful way and provide convincing evidence that PSYOP caused effects, or these were significantly influenced by non-kinetic PSYOP actions.[6] The "ability to assess effectiveness of an information operation [and PSYOP by inclusion] is limited because there may be no immediately observable effects, and even if an effect is observed, it may be difficult to relate the effect directly to the IO capability employed."[7] In short, the authors assert that even if something happens during a PSYOP campaign, it is difficult to prove the campaign caused it.

Grohoski asks the fundamental question for IO and its PSYOP capability:

"lacking physical evidence, how can we quantify the intangible attributes of the information environment (IE) to assess the effectiveness of IO?"[8] He defines the IE as a "combination of physical assets and non-physical concepts."[9] Attacking that combination with a variety of kinetic and non-kinetic actions produces effects ranging from tangible (destroyed buildings), to intangible (confused decision making).[10] Grohoski suggests every IO campaign seeks to achieve a hierarchy of first-, second-, and third-order effects: first order "destruction, degradation, and disruption of enemy signal nodes and command posts;" to create second order effects against enemy information processes to achieve the third order effect; change in the "enemy commander's decision making (i.e., the ultimate target of IO)."[11]

Gray and Howard approach Grohoski's question from a traditional military assessment hierarchy:

- Measure of merit (MOM): Much like a MOP, it is the result of an observable, measurable action—message dissemination.

- Measure of objective (MOO): Also based on observation, it answers the question whether or not, for whatever actual causes, the target audience (receivers of the PSYOP message or action) performs the desired behaviors, and the commander's objectives are achieved during or after the PSYOP effort.

- MOE: Based on intangible and indirect responses, an MOE answers the question whether or not there is a direct linkage between the message received and the performance of the desired behavior. [12]

Although Gray and Howard assert it is very difficult to prove that connection, Grohoski's methodology asserts one can use deductive reasoning to show correlation (but not causation) occurs when the impact of an action increases or decreases, while the extent of the effect increases or decreases.[13] Falling back on the adage 'correlation does not imply causation,' all three researchers assume one cannot prove direct cause and effect, because there may be hidden or confounding factors that contribute to a result.

However, the cause-and-effect quandary may require us to jump through a wider hoop. In human interactions, the inputs/influences (moderating variables) often are so numerous and so coincidental that proving direct causation of an effect or behavior (dependent variable) is very difficult. This quandary is known as the "Fundamental Problem of Causal Inference—it is impossible to directly observe causal effects."[14] However, Bradford Hill offers seven criteria that PSYOP teams can use both in planning and assessing, to help them determine whether their efforts contributed significantly to the observed behaviors.[15]

PSYOP Senior NCO in Baghdad distributes news, wonders how well the plan is working. (US Navy)

- Strength of the association between the PSYOP and the effect/behavior.
- Dose-response effect: Behavior changes in a meaningful way with the change in the level of the theoretical cause.
- "Lack of temporal ambiguity: The hypothesized cause precedes the occurrence of the effect." [16]
- Consistency of results: A series of the same PSYOP method(s) designed to produce the same desired behaviors produces similar results.
- "Theoretical plausibility: The hypothesized causal relationship is consistent with current… theoretical knowledge."[17]
- Coherence of evidence: The results do not contradict or call into question accepted facts about the desired behavior.
- "Specificity of the association: The observed behavior is associated with only the suspected cause (or few other causes that can be ruled out)."[18]

Hill stresses one does not have to have perfect alignment of all seven to infer a cause-effect relationship. If over time and with diligent research you can successfully apply these criteria to PSYOP assessments, the more likely (though never perfectly able) you will be to assess that a PSYOP method significantly contributed to observed behaviors. In short, "correlation is not causation, but it sure is a hint."[19]

Multi-Dimensional Model for Considering the Effectiveness of PSYOP

In addition to the cause-and-effect issue, this article asserts that part of the problem has been—besides the lack of understanding of and unrealistic expectations for what PSYOP can and cannot actually do—the penchant for PSYOP assessment to rely on two-dimensional assessments of a multi-dimensional problem. The ordered effects and MOM-MOO-MOE hierarchies noted above are two-dimensional and linear, rather multi-dimensional and spatial. Rather than focus on whether PSYOP A caused Behavior B in a linear fashion, PSYOP assessment should focus on PSYOP as multi-dimensional, multiple variable, continuous interaction that will produce different effects over time. Given multiple actors in dynamic circumstances, did PSYOP A, B, and C significantly affect Behaviors X, Y, and Z with what strength (force), for how long (persistence), with what intended and unintended consequences?

Every PSYOP operates in multiple dimensions along interactive continua.

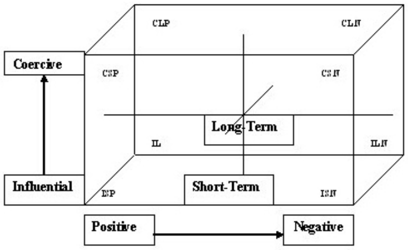


Chart 1: Three-Dimensional Model for Measures of Effectiveness

ISP = Influential, Short-term, Positive Effect
CSP = Coercive, Short-term, Positive Effect
ILP = Influential, Long-term, Positive Effect
CLP = Coercive, Long-Term, Positive Effect

ISN = Influential, Short-term, Negative Effect
CSN = Coercive, Short-term, Negative Effect
ILN = Influential, Long-term, Negative Effect
CLN = Coercive, Long-term, Negative Effect

In the following model, the effect of a message (independent variable) on consequences or observed behaviors (dependent variable) depends on the other dimensions/factors (moderating variables).[20] The PSYOP officer needs to assess whether the observed effects occur in the positive direction he intended with his message, the approximate degree to which his message actually influenced the target audience, and the persistence with which the effects last, and whether positive or negative unintended consequences impacted the outcomes, etc. This article proposes the following most critical dimensions/variables for PSYOP assessment:

- Type of non-kinetic method: Influence to Coercion (ranging from persuasive message to threat of violence. Actual violence is out of the realm of PSYOP, but obviously can be combined with PSYOP to create desired effects.)
- Complexity of method: Simple to Complex (one leaflet drop to multiple products/methods)
- Frequency: One simple occurrence to a complex campaign with multiple messages over weeks or months
- Location: One neighborhood/area to multiple locations over a broad area, even global
- Duration of effect: Short term to long term: Momentary to continuous and lasting.
- Consequences/Effects: Positive Intended—desired behaviors to Negative Unintended—negative, unplanned behaviors.

Key Difference with New Model

This model offers a critical difference versus other approaches: it accounts for both positive unintended consequences, and negative unintended consequences. Of course, no one plans to achieve negative intended effects. However, one must include positive and negative unintended effects, if for no other reasons than to gather comprehensive and accurate data, and be able to assess the relationships among all methods and effects. Then, coincidentally successful or failed methods can be tested in similar situations to determine whether the unintended positive results can be duplicated—and unintended negative ones avoided—by deliberate PSYOP.

It appears current assessment methods either ignore, consider good or bad luck, or attribute external factors beyond their control as causing both unintended positive and negative consequences. Rather, PSYOP evaluators need to examine closely these surprises to glean additional data that can inform the cause-and-effect or correlational relationships.

Multi-Dimensional Model

With complex interactions of multiple variables and the difficulties of providing prompt, accurate assessments of necessarily inexact MOEs, this multi-dimensional model may provide an expeditious way for PSYOP officers to analyze both their short- and long-term results. A three-dimensional model can accommodate the critical variables and allow PSYOP evaluators to plot actual results within these dimensions.

One version of the model shows a three-dimensional box divided into quadrants: The X horizontal axis plots the consequences/observed behaviors, either positive or negative. The Y horizontal axis is the time continuum or duration of the PSYOP. The Z vertical axis is the type of PSYOP effort on the influence-coercion continuum. The eight corners of the box reflect the eight extremes that a PSYOP effort could produce (See Chart 1):

- Most positive = Influence method, Short-Term, Positive (ISP) along the horizontal x-y axis at the X/Y nexus (0/0 scale) across time to Influence method, Long-Term, Positive (ILP). ISP > ILP = positive space.
- Most negative = Coercion method, Short-Term, Negative (CSN) to Coercion, Long-Term, Negative (CLN). CSN > CLN = negative space.

Being based on influence short of violence, PSYOP does use coercive, short- or long-term methods (threat of violence) to achieve positive effects, often in combination with kinetic operations, so the model reflects this approach with the CSP > CLP continuum, that is, from coercion with short-term positive effects to coercion with long-term positive effects. In sum, Chart 1 shows that the left half of the cube reflects various strengths of positive results while the right half reflects various strengths negative results. One could also "add another slice" to the model across the middle—an X2 axis—to add intended and unintended consequences, both positive and negative.

Utility of the Model

With this model a PSYOP team can plot the results of a unit's actions, because every effort has more than one outcome—which always occur over time. The resulting scattergram can help clarify the relationships between the types of effort and their actual consequences. It can show the "direction of the association:"[21] For example, an influence campaign over three months

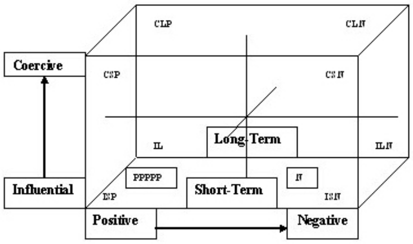


Chart 2: Example of Consequences Plotted on Three-Dimensional Model
P = Positive outcomes
N = Negative outcomes

(medium length effort) with four messages sent numerous times produces five intended positive behaviors, while it generates only one mildly negative consequence. The positive values would be graphed in the lower middle of the positive ISP-ILP quadrant, while the mildly negative consequence would be plotted at the middle of the graph. As the ongoing results of the effort are plotted over time, clusters begin to show the "shape" of the relationship, and the strength of the association among the variables becomes apparent. (See Chart 2.)[22]

If the same or similar unintended negative consequences are found to cluster around a type and timing of a method (short-term, coercive methods produce consistent negative reactions), an assessment team can analyze the situation in more depth and take action. Perhaps more important, an assessment team can review the historical record, plot the available data, and create a graphic view. This allows them to zero in on the types of efforts that both succeed and fail over time, and better guide future planning efforts.

This model is also flexible, in that as long as one keeps the dependent variable of positive-negative consequences and the independent variable of type of PSYOP (influence-coercion), an analyst can substitute different moderating variables, such as complexity, frequency, and location, among others, to conduct a deeper and broader analysis. With the different plots, one can overlay the resulting graphs to identify if, when, where, and how the various PSYOP maximize positive consequences and minimize negative ones.

This model has a number of limitations:

1) It depends on gathering accurate data about the outcomes. For example, how do you survey the people who left Fallujah to determine whether PSYOP influenced them?

2) It depends on the evaluator's accurate interpretation of those data.

3) Taken alone, the model does not adequately consider the effects of confounding variables (hidden factors that affect the outcome). Statistical analysis can do so.

4) It depends on analysts having the time and resources to plot the data and interpret the results.

5) It needs to be tested with historical data and statistically verified for reliability and validity.

6) It depends on accurate understanding of the commander's objectives and desired end states, in relatively quantitative terms, although part of the model's flexibility is that it can tolerate some ambiguity because of the spatial clustering of the plotted results.

7) An analyst must be able to judge degrees of success.

8) It is based on "an assumption that you can actually identify substantially all consequences" and it is useful "only for narrowly defined situations with sought-after effects."[23]

The long-considered, thorny problem of designing, applying, and assessing useful MOEs can be approached from a different point of view. Human interactions always have multiple causes, multiple influences, and multiple consequences, which are always more or less difficult to identify, measure, and evaluate. The PSYOP community should be less concerned with living up to virtually impossible standards that others set, and more concerned with identifying more clearly what their actions actually can accomplish: desired effects. Further, PSYOPers should demonstrate the range of those accomplishments more often. The multi-dimensional model offered here is a starting point for discussing the need to move MOE assessment away from its limited, linear methodology to a multi-dimensional approach that can account for the multiple variables. In short, the PSYOP community should seize the initiative from the MOE naysayers, and establish its own standards for assessing MOEs that reflect the sophistication and complexity of PSYOP, and the range of results and outcomes.

The False Dilemma of Correlation and Causation

The difficulty with devising MOEs is often cast as the difficulty in proving that unlike in kinetic action (with its quantifiable battle damage assessment methods), a PSYOP effort "causes" the observed behavior. Here are Hill's suggested seven criteria for assessing "cause and effect" explained in more detail, to help better understand how to apply the criteria to PSYOP assessments:

- "Strength of the association: The stronger the association appears over a series of different studies, the less likely the association is spurious [Author's note: that is, 'coincidental'] because of bias."[24] Note this criterion requires regular assessments to gauge any change, preferably with a control group.
- Dose-response effect: The behavior variable changes in a meaningful way with the change in the level of the theoretical cause. The dose-response effect is especially useful in PSYOP because it allows the PSYOP team to focus on the impact (change) of one influence method (dose).[25]
- "Lack of temporal ambiguity: The hypothesized cause precedes the occurrence of the effect."[26] That is, the desired change in behavior happens after the PSYOP campaign; of course, that means one must establish a baseline, as Barklay stressed. [27]
- Consistency of results: A series of the same PSYOP method(s) designed to produce the same desired behaviors produces similar results. Beware that such situations may include the same flaws: coincidences, a common cause for both the method and the result; and other unknown causal factors, confounding factors that affect the results.[28]
- "Theoretical plausibility: The hypothesized causal relationship is consistent with current… theoretical knowledge."[29] Of course, the current knowledge may not be adequate to accurately explain the theoretical relationship.
- Coherence of evidence: The results do not contradict or call into question accepted facts about the dependent variable, that is, the desired behavior.[30] If long PSYOP experience has shown that leaflet drops can influence enemy morale on the front lines, then it may be more likely than not that another leaflet

drop on a frontline enemy will influence their morale.

- "Specificity of the association: The observed effect [behavior] is associated with only the suspected cause (or few other causes that can be ruled out)."[31] That is, the more closely you can relate the observed behavior to only your PSYOP actions, the more likely these caused the behavior.

We must also stress that you do not have to have perfect alignment of all seven to infer a cause-effect relationship. If you can—over time and with diligent research—successfully apply these criteria to your PSYOP assessments, the more likely (though never perfectly able) you will be to assess that a PSYOP method contributed significantly to observed behaviors. In short, "correlation is not causation but it sure is a hint." [32]

Notes

[1] Thomas F. Metz, Mark W. Garrett, James E. Hutton, and Timothy W. Bush, "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review*, May-June 2006, 8.

[2] Ibid, 6.

[3] MOEs contrast with measures of performance (MOPs); MOPs measure whether the planned actions actually occurred as planned—a leaflet drop on at a village disseminated the planned number of leaflets at the right time on the right village.

[4] Christopher J. Lamb, "Review of Psychological Operations Lessons Learned from Recent Operational Experience" (Washington, DC: National Defense University Press), September 2005.

[5] Joint Chiefs of Staff, Joint Publication 3-0, *Joint Operations* (Washington, DC: 17 September 20060, GL-22.

[6] Carrie Gray and Edwin Howard, "IO MOE Development and Collection: A Paradigm Shift," *IO Sphere*, Spring 2005, 38. David C. Grohoski, "Measures of effectiveness in the information environment," *Military Intelligence Professional Bulletin*, July-September 2003, http://findarticles.com/p/articles/mi_m0IBS/is_3_29/ai_106699529/print (accessed September 7, 2007).

[7] Gray and Howard, "IO MOEs," 38-9.

[8] Grohoski, "Measures of Effectiveness."

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Gray and Howard, "IO MOEs," 38-9.

[13] Ibid.

[14] "Correlation does not imply causation." http:en.wikipedia.org/wiki/Correlation_does_not_imply_causation (accessed 14 October 2007).

[15] Hill, A. Bradford. *Principles of Medical Statistics*, 9th ed. (New York: Oxford University Press).

[16] Ibid

[17] Ibid.

[18] Ibid.

[19] Tufte, Edward R. *The Cognitive Style of PowerPoint: Pitching Out Corrupts*. Within http://www.edwardtufte.com/tufte/powerpoint (Cheshire, CT: Graphics Press), 2006.

[20] Monique Mitchell Turner, Ph.D., University of Maryland Communication Department, College Park, MD, electronic mail message to author, 12 October 2007.

[21] "Scatterplots," http://www.math.sfu.ca/~cschwarz/Stat-301/Handouts/node47.html (accessed 14 October 2007).

[22] Ibid.

[23] Richard Fravel, Chief Operating Officer, National Geospatial-Intelligence Agency, interview with the author, 5 October 2007.

[24] "Principles of causation," http://www.math.sfu.ca/~cschwarz/Stat-301/Handouts/node47.html (accessed 14 October 2007).

[25] Ibid.

[26] Ibid

[27] Chadwick Barklay, LTC, 2nd PSYOP Group, US Army Reserves, interview with the author, 28 September 2007.

[28] "Principles of Causation."

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Tufte, Edward R. *The Cognitive Style of PowerPoint*.

Mr. Robert L. Perry, GS-15, is a student at the Naval War College. He is pursuing an advanced research project on the tenets and principles of strategic communication. Before attending the War College, he served most recently as Executive Officer to the Chief Operating Officer of the National Geospatial-Intelligence Agency (NGA). He was the Division Chief of NGA's Leadership Development Center and as Intelligence Communication Instructor for NGA College. He holds a BA in journalism and mass communication from the University of Georgia and earned an MA in organizational communication from the University of Maryland, College Park (UMDCP). He also taught professional writing and business communication at UMDCP for many years. Readers can contact him at perry62550@hotmail.com

Voices on Afghanistan

By Mary E. Whisenhunt

Editorial Abstract: The author provides a detailed overview of topics and findings from a multiagency political-social exchange on Afghanistan. The forum brought together representatives from across the Middle East and North America to address content and management of Western messaging efforts in south Asia.

> ***"Understanding Afghan perspectives—what inspires, what terrifies them—is critical in assessing our success, or lack of it"***
>
> ***-- Mr Mitch Shivers***
> ***DASD (P) Central Asia***

In the fall of 2007, the Deputy Assistant Secretary of Defense for Central Asia tasked the Joint Information Operations Warfare Command to provide a series of audience analyses, in support of the US Strategic Communication (SC) Plan for Afghanistan. As part of this effort the JIOWC planned and hosted a seminar, leveraging the Virtual Integrated Support to the Information Operations Environment (VISION) program, to build an initial community of interest and obtain the required data.

The seminar brought together a diverse group of US Government (USG), foreign and industry speakers and participants, to include representatives from the Afghan government, the UN, Pakistan's Northwest Frontier Province (NWFP) Frontier Police, Office of the Secretary of Defense (OSD), NATO, US Central Command (USCENTCOM), US Special Operations Command (USSOCOM), Broadcasting Board of Governors (BBG), Assistant Secretary of Defense (ASD) for Joint Communications, Department of State Office of Research (DOS INR), Joint Warfare Analysis Center (JWAC), Canadian Forces Expeditionary Command, US Strategic Command, National Guard Bureau-Information Operations, Charney Research, The Rendon Group, SOS-International, Gallup, 1st Information Operations (IO) Command, the National Counter-Terrorism Center (NCTC), and Open Source Center.

The seminar title begins with the phrase, "Voices on Afghanistan", emphasizing the importance of understanding the audiences, by listening to foreign and domestic experts. During the seminar, representatives presented survey data and operational media analysis outlining how key themes in the DOD SC plan resonate, or fail to resonate, with regional audiences, to include the leadership and population of Afghanistan, Pakistan as well as International Security Assistance Force (ISAF) troop contributing nations. Through presentations, discussions, and information harvesting exercises, the seminar established a common frame of reference that served as a baseline for assessing public opinion on critical US and ISAF efforts to support Afghanistan and counter regional extremism.

Key Findings

- Dr. Craig Charney stated that optimism within Afghanistan is down substantially from 2005, but has recovered somewhat from lows in Spring 2007. Economy and security have become key issues. Afghans ranked the economy, infrastructure, corruption and security highest on their list of concerns. Poppy cultivation is a much lower priority for Afghans compared to other problems.
- A majority of Afghans are critical of what America is doing in their country, though they are not anti-American. The biggest drop in ratings occurred in zones where security has worsened. They see security as America's responsibility, and if they don't like what they see, the US image suffers. In the November 2007 BBC poll in Afghanistan, as well as in previous BBC polls in 2006 and 2005, respondents were asked when they believe US forces should withdraw from Afghanistan. In 2007, 14% said the US should leave now, as opposed to 13% in 2006 and 8% in 2005. At the other end of the spectrum, 42% in 2007 said the US should withdraw only when security is restored, compared to 55% in 2006 and 65% in 2005–a 23% change from 2005.
- In the November 2007 USCENTCOM poll, confidence in the Afghan National Army tended toward the positive, with 54% responding in the positive (6 to 10) confidence range. Only 12% tended toward the negative, while 29% did not express confidence or lack of it. In the same poll, confidence in the Afghan National Police also tended toward the positive, with 45% responding in the positive (6 to 10) confidence range. Only 3% tended toward the negative, while 33% indicated they were neither confident nor expressed "no confidence" in the National Police.
- In the same poll, respondents generally felt that NATO forces and foreign civilian organizations were not helping their local community achieve greater security and prosperity. A combined 34% somewhat or strongly agreed that NATO was helping their local community while a combined 62% somewhat or strongly disagreed that NATO helps.
- The Afghan government is grateful for US/NATO support, yet concerned because the population perceives that outsiders are running the show, not the Afghan government.
- It is important to note that to Afghans, US military, NATO/ISAF, and Al Qaida are all "foreign fighters." There is a sense amongst the Afghans that the USG carries out its own agenda without involving the Afghan Parliament.
- From 2004 to 2006, public opinion moved strongly against the Taliban, but began swinging back in 2007, largely as a result of security issues. Taliban gains are a mirror image of US losses of support. However, polling indicates that the vast majority of Afghans are repelled by Taliban tactics. Attacks against government officials, police, teachers/schools, and civilians were rated as "Not Justified" by from 94-97%; suicide bombings were rated as "Not Justified" by 89% of those surveyed, while attacks against US military forces were rated

as "Not Justified" by 78%, a three point increase since 2007. The seminar working groups noted that the population blames both the Taliban and US for the violence, and that civilian casualties caused by US airstrikes can cause entire tribes/villages to move to the Taliban's side (the Taliban are known to "hype" airstrike damage to damage any residual goodwill toward the US). The Afghan populace is vehemently opposed to suicide bombing for any reason and is generally aware that the Taliban use them as human shields when they fear attack by US/NATO forces.

• Dr. Brian Williams, with considerable in-country experience *[see interview, page 32]*, briefed that the popularity of the US among Uzbeks is declining. Uzbeks have deeply-rooted fears of a centralized, Pashtun-dominated state… when the US presents itself as the sponsor of a centralized state, we are taking sides on something that isn't necessarily good for Uzbeks. We must have an awareness of these historical sensitivities…otherwise we will lose pro-US supporters who sense we are bolstering the Pashtun government at their expense.

• Everyone—even Taliban—wants their kids to have an education, including their daughters.

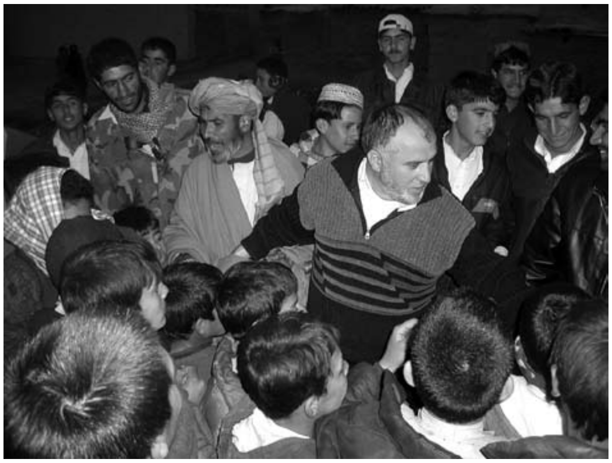
• The main source of Afghan information or news comes from family, tribal elders and community. Once messages reach friends and family, information tends to rapidly spread through the informal network. Radio is the best means for reinforcing communications through personal contact. Surveys indicate radio listening is uniformly high throughout Afghanistan at up to 96 per cent of all adults. Afghans listen primarily to FM frequencies in urban areas, but in rural areas the use of medium wave and short wave frequencies is high. There are two main listening peaks, during the morning and evenings. Radio audiences will gradually decline as ownership satellite dishes and cable continue to expand into the rural areas of Afghanistan.

Afghans live on face-to-face communication. 75% of Afghans rely on family and friends for information, with cell phone usage growing and further amplifying personal contact. Additionally, Mullahs and their sermons continue to be an important source of information in Afghanistan.

• 71% of Afghans don't have access to TV due to lack of affordability and electricity. In urban areas, where television is available, an Asia Foundation survey (Oct 2007) reports Private Tolo TV reaches 51% (audience share) of television viewers in Afghanistan, while Ariana TV comes in second with 18%, with National Afghanistan TV and Aina TV coming in at 12% and 4% respectively. The growth of private television stations however has been the most significant development within Afghan media during the last few years.

• BBC has reported that newspapers were read by 15% of all adults within Afghanistan. It is widely reported that Afghanistan has an illiteracy rate estimated at 70%.

• The US BBG has a virtual think tank on Afghanistan–a large staff with many foreign nationals which DOD and DOS can tap to enrich understanding of how to communicate with Afghans.



Tribal elders and Afghan National Army troops hand out winter supplies in Shindad Province. (Defense Link)

• According to Ambassador Ron Neumann, former US Ambassador to Afghanistan, Afghanistan lives on oral communication. We will never be fully understood; the US will never match the expectations of the Afghans. But we must enable, and allow our people on the ground the right information to export it.

• The seminar's Afghan participants noted that Afghans understand that if Taliban fighters and Al Qaida were not engaged in Afghanistan, then US forces would not be necessary. Americans, however, are more available, and as foreigners, more acceptable, as a target. Afghan expectations on infrastructure development have not been met, negatively impacting perceptions. The perceived gap between what we say and what we do is another key factor fueling negative views of the US. Our rhetoric has often outdistanced their reality. "I believe our (Afghan) expectations were far too high in the beginning, and too optimistic." (Ambassador Jawed Ludin)

• "All problems are 'local' in Afghanistan; one district's challenges are not the next district's. On the ground, "we are divided on almost every issue." (Shahmahmood Miakhel, former Afghan Deputy Minister of the Interior

• "What is important is for the farmer to hear that poppy cultivation is illegal on the radio, and then in the morning, see a couple of police vehicles in the village." (Shamahmood Miakhel)

• Coalition forces are well aware of the importance of civilian casualties as a strategic concern and have taken strides to identify shortfalls and take proactive steps. While unfavorable sentiment on civilian casualties increased during the past three years, contributing to more negative coverage, increases in neutral reporting on the topic in the past six months indicate some success in attaining balanced levels of favorable and factual sentiment on efforts to prevent civilian casualties.

• From a tactical perspective, American forces are not seen positively. No matter how well we are doing, we are garrisoned; living in security bubbles. Their perception of us is as a powerful, invincible force. Afghans don't want to go near our military forces—they are considered unapproachable, heavily armed, and intimidating.

Pakistan

• According to Ambassador Ludin, from Afghanistan, even the mainstream Pakistani media has actively worked against Afghanistan and the West. It is both anti-war on terror (WOT) and anti-President Karzai.

• The Taliban spark anti-US sentiment by capitalizing on several linchpin actions—periodic US airstrikes on tribal areas (which elicit a desire for vengeance), casualties they inflict on Pakistani/US-led armies (which highlights the militants' bravery), and US threats or provocative statements against Pakistan/Holy Cities.

• The seminar's Pakistan working group agreed that overall, the Pakistan government's perception of the Afghan government was negative, and that relationships between the governments were antagonistic, even "poisonous" at times.

• Pakistan's perception of the ISAF/US missions in Afghanistan is largely ambivalent at best. There is significant concern that the mission represents a possible future that could be antithetical to Pakistani objectives; i.e. Islamabad is wary of any factor that could empower Pashtuns on the Afghan side of the border, as it could equally empower those on the Pakistan side.

• In the November 2007 USCENTCOM poll, a plurality (32%) was very opposed to the US and NATO using Pakistan territory as part of the effort to fight Al Qaeda and the Taliban. A higher percentage (36%) said they were unsure. Only 5% were very or somewhat in favor.

Use of Pakistan for Missions in Afghanistan (2007)

• The 2007 USCENTCOM poll asked respondents whether they paid attention to information provided by the US military, and whether they found the information very accurate, somewhat accurate, not very accurate, or not accurate at all. A majority (59%) of respondents felt that information from US military sources was not very accurate or not accurate at all. However, about one in three (34%) were not sure.

• Nationwide in Pakistan in the USCENTCOM poll, a majority of respondents (58%) had very unfavorable attitudes toward the US government. A combined 80% held somewhat or very unfavorable attitudes. Working group discussions indicated that many viewed the Pakistani relationship with the US government as a guarantee against Indian attack.

Afghan man receives a new radio in Oruzgun Province. (Defense Link)

• Asked about challenges in the region in the November 2007 poll, a majority (55%) viewed the US as presenting the greatest challenge to stability and security, a larger percentage than says India (31%). Afghanistan (9%) is barely a concern.

Greatest challenge to stability & security - Country (2007)

• In seminar working group discussions, most agreed that the US was viewed as a "fair weather friend" and that the Pakistani populace was generally suspicious of the US. Currently, the relationship varies issue by issue (and often day by day), and is based on external factors, rather than Pakistan's needs. The US lacks a "personal touch" in its dealings with Pakistan and often appears unfriendly—"too straight forward" and "too casual." Fasihuddin recommended that it would be helpful if Americans dealing with Pakistanis could learn a few words and more about Pakistani culture when dealing with them.

• Television is the dominant medium within Pakistan; 87% of the adult urban population and 67% of the rural population watch at least once a week. Cable or Satellite TV access was 61% in urban areas (up from 45% percent the previous year); in rural areas it has risen from 4 to 8 %. Urdu is the language most widely used by broadcasters, although a number of channels use English and other languages in their news and programs.

• Domestic radio broadcast coverage is 80% of the country and reaches 96% of the population. According to the Open Source Center, Radio Pakistan is the only radio outlet allowed to carry news. Radio Pakistan newscasts and state-run Pakistan TV newscasts carry only brief, factual reports on developments in Afghanistan. Pakistan TV is the only television outlet allowed to carry news and the only one allowed to broadcast terrestrially. President Musharraf has cracked down on private cable TV stations due to their perceived political impact. Coverage of Afghanistan in Pakistan media is very spotty, with the exception of bilateral encounters. Cell phones and text messaging are growing phenomena.

• According to a 2003 estimate, adult literacy was 46% overall (63% in urban areas and 34% in rural areas). The All Pakistani Newspaper Society lists 283 member publications, of which 190 are dailies. Total average daily circulation is about 6 million.

• Mr. Fasihuddin, Deputy Commander of Frontier Reserve Forces in Pakistan's Northwest Frontier Province (NWFP) *[see interview, page 21]*, noted that the Pakistani media and official statements do not use the word "Taliban" when reporting on the fighters in the tribal areas; they rather use the word "miscreant" (sharpasand) or "militant" (askariyatpassand). The general public has little or no respect for a militant or miscreant, but the civilian casualties attributed to US cross-border attacks, lies, and day-to-day hardships experienced by those in the border region have created doubts in their minds." (Mr Fasihuddin).

• There are strong, symbiotic linkages between Taliban in Pakistan (Taliban-P) and Taliban in Afghanistan (Taliban-A). The groups are mutually supportive despite differences including location and tribe—the common determinant is Maslow's hierarchy of needs—survival is all. While not all the Taliban-P are necessarily supporters of Mullah Omar, if asked to provide forces to support Taliban-A they will generally do so, so long as circumstances permit.

The Taliban-P is far more concerned with tribal lands and local issues than it is about the global Al Qaida movement; local politics dominate their political landscape. Al Qaida has succeeded in integrating itself into the FATA, where they have married into various tribes, negating the "foreign" aspect of the group (a considerably different perspective than in Afghanistan). Consequently, few are willing to take up the banner against Al Qaida on the local level. Al Qaida members also attach themselves to local and powerful chiefs that appear impervious to Pakistani government or international influence.

ISAF

• Ms Gina Faranda, DOS INR, noted that support for the ISAF mission is declining in Europe. Those who see it as stabilizing Afghanistan do support it; those who don't see that, don't support the operations. Only in Germany has support for ISAF remained steady. Support has been highest in France. Overall, in Western Europe, publics tend to see the mission as a failure. They define success as the stabilization of Afghanistan. They support the goal of stabilizing Afghanistan, and they view ISAF as focused too much on military operations.

• Ms Lynn McConaughey, The Rendon Group, briefed that political stability and the general security environment are increasingly being characterized in less favorable terms to European audiences; thus the rise in negative and neutral reports. Rather than seeing messaging on progress, populace support for the Afghan government, achievements in stabilizing provinces outside Kabul, we are seeing officials and observers provide cautious assessments of the general security environment, often using the term "deteriorating".

• Media analysis shows that political stability and the general security environment in Afghanistan are increasingly being characterized in less favorable terms to European audiences; thus the rise in negative and neutral reports. Rather than seeing messaging on progress, populace support for the Afghan government and achievements in stabilizing provinces outside Kabul, we see officials and observers providing cautious assessments of the general security environment, often using the term "deteriorating."

• NATO's image has been pretty resilient even after decline of US image.

Implication: highlight NATO leadership, not US leadership.

• Some NATO allies have projected themselves as being completely separate from the US/UK presence. Future themes and messages should focus on identifying military actions as "coalition-led," transitioning to "Afghan-led" operations.

• Blanket SC courses of action targeting ISAF-contributing nation audiences are less than useful. Each nation has its own set of priorities and domestic politics; therefore SC planning must include a nation-by-nation subset of goals, means and measures of effectiveness.

• Ambassador Neumann added that there's a broad European perception that Americans are all about fighting. That's not true; we are all about the integrated solution. We can do better but not by what we say in Washington DC, Kabul or Brussels. Europeans ask why their forces are there at all… their media asks, is it worth the loss of life? People believe what they see. Bring ISAF-contributing nation Parliamentarians to Afghanistan and show them the reality on the ground.

• Other recommendations include:

- Develop media kits for planned and anticipated events like journalist trips, including context of mission in various places, TCN activities; translate and hang this information on appropriate websites for download

- Encourage each ISAF country to create its own mission Web page and hang website on ISAF and/or other sites; information on sites must make information available for sharing among members.

- Push information from ISAF press conferences instead of just "making it available."

- Map the ISAF communications cycle–where does the information go? Who touches which parts of communications? Determine where delays occur and on what grounds.

- Conduct a daily or weekly VTC between regional US and NATO military forces about media outreach—current and planned activities—for cross fertilization and situational awareness.

- Encourage Afghan government officials to reach out to TCN countries; including to political opposition; bring them to influential think tanks, NGOs, press clubs.

- Bring positively affected Afghans to X country; bring Afghan officers to TCNs; amplify in media.

- Shorten the timing cycle to ensure receipt of information that is as close to "ground truth" as possible.

• Flash points for European audiences are troop casualties, the perceived lack of progress in the Afghan security situation, Afghan civilian casualties and the characterization of operations as "US-led." The prevailing sentiment in Western Europe is that the US and ISAF are not being careful enough in efforts to avoid civilian casualties. Canada's actions and communications in advance of Operation Medusa seemed to make an impact in the Canadian understanding of the dynamics of civilian casualty avoidance. Working group discussion then shifted to the need to manage expectations on civilian casualties, and noted that our vaunted technological (military) prowess exacerbates this problem. There is a widespread perception that the US military can do anything, and that if anything goes wrong, we did it intentionally.

• Currently, large majorities among the British, French, German, Italian and Spanish public acknowledge the threat of a resurgent Taliban or international terrorism to their national security. However, threat perception is not closely linked to support for ISAF overall—a critical delta and opportunity in overall SC strategy.

• Speaking about the mission in terms of an effort to train Afghan security forces as part of an exit strategy is a potential theme for coalition country audiences.

• In counter-narcotics messaging in Western Europe, we should consider amplifying the linkage between poppy growing and heroin/opium sales as a funding source for terrorism.

Subject Matter Expert Presentations & Assessments

Afghanistan and Pakistan: Public Opinion Trends and Strategic Implications (Dr. Craig Charney, Charney Research):

• Optimism within Afghanistan is down substantially from 2005, but has recovered somewhat from lows in the springtime. Economy and security have become key issues. Afghans ranked the economy, infrastructure, corruption and security highest on their list of concerns. Poppy cultivation is a much lower priority for Afghans compared to other problems.

• President Karzai's job performance numbers are down, though still positive. The security situation is now reflected in Karzai's approval ratings.

• A majority of Afghans are critical of what America is doing in their country, though they are not anti-American. The biggest drop in ratings occurred in zones where security has worsened. They see security as America's responsibility, and if they don't like what they see, the US image suffers. And they don't like what they see.

• Civilian casualties caused by US/ISAF forces are very detrimental to Afghan confidence.

• In the counter-narcotics realm, almost half of Afghan farmers accept opium cultivation, but with a guilty conscience. Few support aerial spraying—the health risks are perceived as enormous. Survey results indicate that the most effective way to cut opium cultivation involves financial incentives, not forced eradication.

• Over one-fifth of votes are "swing supporters" in the contest with the Taliban. The swing supporters are positive on country, democracy, and women in Parliament, and want democracy to co-exist with Islam. Their priorities are infrastructure, jobs, and security. The people we need to win over are fairly supportive of drug cultivation and don't favor aerial spraying. They're fairly cool toward the US.

• We win them over with wedge issues, including morality, democracy, girl's schools, the Karzai government and development. Strategic keys to winning the swing groups include:

• US/NATO force presence and effectiveness in maintaining security while avoiding civilian casualties

• Avoiding civilian casualties and insensitivity is imperative; we need fewer bombs and more boots on the ground

• Apologize and compensate when civilian casualties occur; investigate and prosecute when justified

• US must support national reconciliation programs, highlighting the fact that it is the Taliban who are responsible for the conflict, not us

• Develop roads, jobs, power and security in swing areas, and let people know about progress

• Personal contact is central

Discussion: Ambassador Ludin disagreed with the concept of "swing supporters" in Afghanistan, asserting rather that the entire population could be considered 'fence sitters.'

Pakistan

• In terms of capacity to govern, Pakistan has remained viable because its leaders continue to have considerable popular support. As a result of Benazir Bhutto's death, however, instability and lack of popular support for leadership have become bigger problems.

• Classic factors drive discontent with the government, to include the economy, corruption and law enforcement performance.

• A common factor in regional priorities is the economy.

• Looking at the NWFP specifically, it is a much more conservative area.

There, most believe women should follow their husband's lead and do not feel threatened by Islamic extremism. Only 32% are concerned about Islamic extremism in the NWFP, as opposed to 50% in the rest of Pakistan.

• Key information sources in the NWFP include:

• Community news: neighbors, local mullahs

• National affairs: television, neighbors

European Perceptions of ISAF/US Military Operations in Afghanistan & Strategic Themes (Ms Gina Faranda, DoS INR):

• We see declining support for the ISAF mission in Europe. Those who see it as stabilizing Afghanistan do support it; those who don't see that, don't support the operations.

• Only in Germany has support for ISAF remained steady. Support has been highest in France. Overall, in Western Europe, publics tend to see the mission as a failure. They define success as the stabilization of Afghanistan. They support the goal of stabilizing Afghanistan, and they view ISAF as focused too much on military operations.

• As to the question of "Are Europeans doing their fair share?" Most survey participants think Europe should be involved and that they are engaged in the right amount of support.

• The Spanish are the least in favor of participating in ISAF.

• Large majorities in Western Europe continue to see the Taliban as a threat.

• NATO's image has been pretty resilient even after decline of US image. Implication: highlight NATO leadership, not US leadership.

• Publics generally support non-traditional (i.e. non-kinetic) NATO roles.

• While the US image is currently the lowest it's been for 50 years, confidence in NATO remains strong. Europeans still see NATO as crucial to their national security and an important institution. They clearly support the building blocks for what NATO is trying to accomplish, but don't see the progress.

Discussion: Some Western European ISAF-contributing nations desire to disassociate themselves with kinetic operations complicates press reporting; some have asked not to be mentioned in press releases involving combat operations. This leads to a dearth of information about what ISAF forces are doing. Involvement in combat operations can, and is, used as a political weapon in Western European domestic politics. In many European nations, ISAF involvement was predicated on a non-combat role.

Media Analysis Trends on Afghanistan (Ms Lynn McConaughey, TRG):

- Political stability and the general security environment are increasingly being characterized in less favorable terms to European audiences; thus the rise in negative and neutral reports. Rather than seeing messaging on progress, populace support for the Afghan government, achievements in stabilizing provinces outside Kabul, we are seeing officials and observers provide cautious assessments of the general security environment, often using the term "deteriorating."
- Afghan government officials and parliamentarians are the main driver of statements that either equivocating in their support of Afghan stability and security or are not on message about efforts and progress. The Afghan government is missing opportunities to position government achievements in areas of stability and security.
- Poor security is used as key rallying point for lawmakers opposing the Karzai administration.
- Pakistanis use security as a scapegoat message when under pressure for failing to curb cross border militant movement.
- Increased visibility in operations storylines will promote the image of strength/credibility of the Afghan government. Reporting on Musa Qala, while mostly neutral reporting portrayed the Afghan government and coalition operation in a favorable light. The public relations effort surrounding the event successfully shifted the media agenda from attacks to operations, influencing more neutral to positive coverage. The storyline also emphasized the role of Afghan troops jointly coordinating with the coalition.
- Overall, unfavorable sentiment on civilian casualties increased during the past three years, contributing to more negative coverage. However, increases in neutral reporting on the topic in the past six months indicate NATO/US military success in maintaining balanced levels of favorable and factual sentiment on efforts to prevent civilian casualties.
- In Western Europe, the debate often reverts to defining the ISAF mission in terms of peacekeeping vs. counter insurgency, a dynamic or frame which does not lend to increasing support for the mission among coalition nation citizens and lawmakers. Speaking about the mission in terms of an effort to train the Afghan National Security Forces (ANSF) as an exit strategy is a more appealing message for coalition country audiences. Criticism of NATO focused on perception of occupation and civilian casualties.
- Afghan media does not play a huge role in influencing Afghan audience; the main source of Afghan information, news is from tribal elders/community.

US Embassy Islamabad relief efforts near Shinkiar, Pakistan. (Defense Link)

Discussion: There is no "one-stop-shopping" mechanism or process for responding rapidly to civilian casualties. We are unable to rapidly integrate and synchronize responses to negative news, and are consigned to responding rather than planning ahead and preparing storylines to fill the message space with positive stories. One problem at NATO is that often no one is sure whose lane is involved in civilian casualties and other operations.

Taliban & Al Qaida Key Communicators on Strategic Themes (Mr Ed Pressman, SOSi/STRATCOM):

- There has been a clear focus on ISAF/NATO in Taliban and Al Qaida messaging, with the tempo spiking dramatically. That spike occurred in conjunction with offensive operations. Extremely striking in 2007 was the growth and consolidation of messaging in monitored media. The frequency of press releases grew by 36%.
- The sophistication of messaging has also increased. Taliban field commanders are being increasingly visible. They are using more Web forums to promote upcoming releases of announcements.
- We observed a clear Al Qaida movement away from the "Arab voice" toward one based on Western argumentative logic. Its appeal is more Western-focused, and is a clear attempt to break through language barriers.
- Taliban messaging is not strategic in nature—they are tactical communicators.
- In terms of media analysis, when AQ initially started messaging, there was an incredible emphasis on analysis by the media. Now, the statements are in and out of the media extremely quickly. AQ is going into different markets to try to regain "market share."

Discussion: Follow-on discussions indicated that we must further refine audiences and measures of effectiveness and goals. The USG, NATO, and Afghan government should decide where priorities lie and collectively develop a holistic strategy to move toward those goals, incorporating a feedback mechanism. As noted earlier, Al Qaida and Taliban messaging and targets are not the same and require different strategies and approaches.

Regional Media Environment

Reaching Audiences in Afghanistan and Pakistan (Ms Setareh Jorgensen, OSC):

Afghanistan

• Asia Foundation survey (Oct 2007): Private Tolo TV reaches 51% (audience share) of television viewers in Afghanistan. Ariana TV comes in second with 18%, with National Afghanistan TV and Aina TV coming in at 12% and 4% respectively.

• 71% of Afghans don't have access to TV due to lack of affordability and electricity (access to electricity could change considerably once work on the extension of electricity lines from Central Asia and the renovation of the Kajaki hydroelectric dam in Helmand is completed). Most people with access to television live in urban areas.

• 88% said the most common media source in their household was a radio.

• Despite low literacy rates in Afghanistan, there are 250 print outlets in the country.

• We've found 30 blogs in Afghanistan and they are not of high value. We do monitor some Taliban websites. Overall, Internet use is only at 2% in Afghanistan, as of research conducted in August 2007.

• The popularity of soap operas and entertainment on television has increased significantly; the Islamic clergy have urged President Karzai to combat "immorality" of televised programs.

• The Afghan media is expanding rapidly, but there is still pressure and fear. Media in areas not under control of the central government has not blossomed yet.

Pakistan

• The US is generally viewed very negatively by local populations. For example, Mr Fasihuddin's nephew, who is standing for election, asked that he not tell anyone he was going to the US or the nephew would "lose the campaign." Even Mr Fasihuddin's wife encouraged him to "Do a good presentation so the coalition will leave."

• Radio Pakistan is the only radio outlet allowed to carry news. Radio Pakistan newscasts and state-run Pakistan TV newscasts carry only brief, factual reports on developments in Afghanistan.

• Pakistan TV is only television outlet allowed to carry news and the only one allowed to broadcast terrestrially. President Musharraf has cracked down on private cable TV stations due to their perceived political impact.

• Coverage of Afghanistan in Pakistan media is very spotty, with the exception of bilateral encounters.

• Cell phones and text messaging are growing phenomena.

Discussion: Ambassador Ludin posited that fighting the media war is as important and consequential as the military war: "I don't think we really grasp the importance of the media. For example, the Iranian media has played a very damaging role in Afghanistan. The Government of Iran is funding media outlets broadcasting to Afghan audiences, supporting not only extremely negative coverage, but total, complete disinformation. In addition, even the mainstream Pakistani media has actively worked against Afghanistan and the West. It is both anti-war on terror (WOT) and anti-President Karzai." (Ambassador Ludin).

Assessment

Perception of NATO and US Support to Afghan Institutions. A majority of Afghans are critical of what the US is doing in their country, though they are not anti-American; 65% still have positive views of America itself though that figure has dropped 28 points since 2005. The biggest drop in ratings occurred in zones where security has worsened. Afghans see security as America's responsibility, and the reason for the US military presence in Afghanistan. If they don't like what they see, the US image suffers.

In a November 2007 USCENTCOM poll, the largest percentage of respondents (61%) believe the US and NATO are committed to helping Afghanistan for five to 10 years into the future. Only a small percentage (12%) think the US/NATO will remain for less than two years, while only 11% think the forces will remain for more than 10 years. That being said, Afghanistan working group participants noted that in their experience, there is a degree of expectation amongst Afghans that the West will not support Afghanistan for the long-term.

Additional Observations: Most seminar participants agreed that the major obstacle in getting the USG message to the Afghan population, and a source of our negative image, is that we are foreigners, and "foreign fighters" at that. The population is more likely to forgive acts of violence committed by Taliban because they are "local" (with the exception of suicide bombings). The population is more vocal in responding to negative events attributed to US/NATO than those of the Taliban because they fear retribution by the Taliban. Numerous examples of staged protests against US activities were cited in this discussion. It was noted that the Taliban, as opposed to the general population, are well aware of US tactics and use our scruples and honor against us.

Mary Whisenhunt, Lt Col, US Air Force, Retired, is a senior analyst for The Rendon Group. She served as an intelligence analyst, operations officer, and squadron commander, and led coalition network development efforts at USCENTCOM. She holds a BA from the University of Wisconsin, an MA in International Relations from Webster University, was a Fulbright Scholar at the University of Trondheim, Norway, and a Defense Fellow at the Massachusetts Institute of Technology. Readers may contact her at mwhisenhunt@rendon.com

Policing Pakistan's Northwest Frontier: Fasihuddin Interview

Interviewed by John Whisenhunt, Editor

Editorial Abstract: Fasihuddin, a senior law enforcement officer, attended the "Voices on Afghanistan" seminar to provide a Pakistani perspective. He discusses the challenges of policing the Afghanistan/Pakistan border regions, and offers recommendations for more effective cultural and technical law enforcement in the region.

Views expressed by Fasihuddin are his own, and do not represent the Police Service of Pakistan, nor any official Government of Pakistan position.

***IO Sphere**: Can you please set the stage for our readers, and tell us a little about the Northwest Frontier Province (NWFP), and the challenges you have carrying out security operations there.*

Fasihuddin: Pakistan is a federation, and two of the provinces, Baluchistan and the NWFP, are adjacent to Afghanistan. You know there has been war in Afghanistan for many years, first with the Soviets, then the Talib fighting, and the third stage is the War on Terror. We have seven tribal agencies, collectively called "FATA" [Federally Administered Tribal Area], and most of them are adjacent to Afghanistan. The people living on both sides of the border speak the same language, and are mostly of the same ethnic group. The tribal identity means they have strong affinity for one another, so for centuries they have had relationships, often through matrimonial alliances, and many other transactions of a socio-economic nature. So when there is a war in Afghanistan, it is automatically felt in Pakistan, in the tribal areas. There are so many incessant problems caused by the war in Afghanistan, and it has a lot of implications for the people of NWFP and Baluchistan.

As a law enforcement office in NWFP, we have tremendous difficulties. First, we were never trained, like many police forces in the world, for the War on Terror. Police are the front line of defense in any civil society, but most have never been trained for a warlike situation, but today we face that in these two provinces. Plus, we are under equipped, understaffed, and poorly paid—we have logistical and capacity constraints. In our budget, 88 percent of the money goes to salaries and allowances, leaving only 22 percent for capacity building such as arms and ammunition, which is of course very low. Secondly, since our independence in 1947, the population and crime rate have gone up five and nine times [respectively], but the police force has grown only two times during the same period. Police salaries have never really increased. You would be surprised by how many police officers, who are entitled to certain kinds of weapons, simply don't have them. So these are some of the difficulties, as well as being less in number and less prepared than the terrorists. And there are certain attitudes by certain former Inspectors General of Police: they did not realize there is a war next door to us! These spillover effects can be felt in many districts. We began to have terrorist attacks in our cities. But they did not try to convince the government, donor agencies, nor the international community, to be prepared for the coming situations. Now in the NWFP, we are experiencing terrorist attacks in greater numbers than the FATA—the tribal areas. Suicide bombings only numbered six in 2006, now there are 28 in the NWFP, and 71 in the whole country in 2007. We have a big number out of that 71. Yet in that same time frame, the police did not arrest a single suicide bomber. These are challenges we are facing. We have to modify our roles, not just in increasing our numbers and our capacity, but our attitude towards the problem. Police can address such problems by two methods: zero tolerance, which we're not equipped to do; and community policing. Yet, our training, our police academies are not ready. In the past five years when all this was going on, we should have changed our curriculum, but we still use the old colonial system. We've had proposed reforms which have not been implemented. Again, there are many challenges.

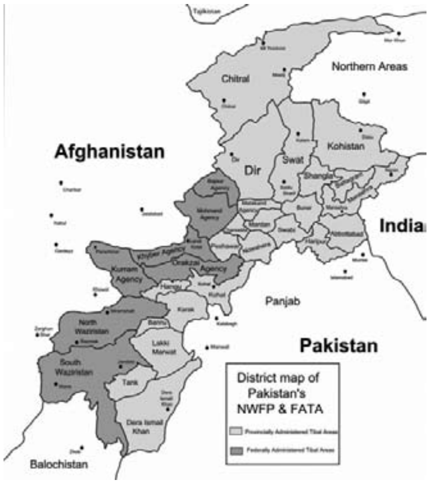
Fasihuddin addresses a village council in the Northwest Frontier Province. (Author)

***IO Sphere**: You've had firsthand experience dealing with extremists and their tactics. You've adapted as best you can given the limitations you've described. How have both your own methods and the terrorists' methods evolved? How are they changing their tactics?*

Fasihuddin: The terrorists are using the latest techniques, the most modern equipment, the most modern communications gear, so we must revamp the whole police model. Naturally, in times of such rapid change, we must adjust our own attitudes and skills, in a way I call "TASK: T is training; A is attitude; S for skill; K for knowledge." Training means to learn to a certain repeatable level, yet our average constable or rifleman only has a tenth grade education. They are generally unaware of the world situation, and do not know what we mean by the War on Terror—they are not conceptually clear on whom they are fighting. There is not a single piece of police curriculum about Al Qaeda, or sectarianism. There are codes of law, police rules, things like that. Our police have never been taught about terrorism and suicide bombing, the techniques of terrorists. They think they will be chasing robbers and thieves! Whereas, the situation has changed. Similarly, they are trained with the Kalashnikov rifle, but not with things like computers or bomb disposal. Now there are certain special police teams with these skills, but we need such general training for all police, because these things are everywhere. Every policeman is concerned with a bomb blast here, and in every city. Most of our force is unaware of things like wiretaps, intelligence analysis, money laundering, international crime—none are included in the police syllabus. Ask a line constable [police officer] what is meant by 'organized crime,' and he is unable to answer. The man on the street with the rifle is not clear on these topics, and how to fight them. Senior officers have a new course, but senior officers are not fighting on the street, they are managers and policy makers. We have to change for the sake of the man is who chasing terrorists to their hideouts. I don't know how to use night vision devices, because I am not trained. And the constable, as especially as he is promoted, must know these things. So, we must be technologically equipped and professionally trained to match to the terrorists. And we must change attitudes. Many lesser educated people, even in law enforcement, think we are fighting our own countrymen… they think the Taliban are our friends, our brothers! The whole way we go about things, getting information, intelligence-led policing—we don't use this yet. The New York Police Department certainly learned this after 9-11, working with major agencies and the Department of Homeland Security. We have intelligence agencies, who are working independently, disparately, but they are not supporting police, and it is very rare for them to let police into their criminal analysis. And we need knowledge: of police work, police culture, as well as world knowledge! How did police respond in New York, in Norway, in Turkey, in Madrid? What are their computer analysis models? We should study the available modus operandi and police approaches of different countries who are confronted with the same situations. So this is what I mean by our TASK: how we must cope with our challenges.

***IO Sphere**: In the West, we don't always seem to understand the cultural and tribal distinctions you've described. What group or country seems to be most successful in understanding the situation? Who is a good model?*

Fasihuddin: The British ruled India and south Asia for 200 years. When confronted with the Afghan and Pashtun people, they were defeated twice. Then they started studying the culture, history, and geography of that area. I am happy that most of those British officers wrote wonderful books about the Pashtun people, even Pashtun poetry. We have the best of our history in those books. The way the UK soldiers fought the bad guys is marvelous. They built forts, checkpoints on the borders of cities, just to keep the tribal people away. They developed a system where they exercised their influence through local tribal chieftains, by giving them respect, what they call "lungi," as well as the title of "Malik" [literally "chieftain"]. Again, very respectful, but also entrusting him with responsibility for keeping order and going after bad guys. Also, they did development work for the local people. Instead of sending their own [British] troops, they hired local forces in the form of frontier constabulary, and they developed a model where the officers developed the policy, but the implementing people, the visible "front" were the local people. That was how they caught the bad guys and provided security in the cities. So that is one successful historical model. In fact, [current] British Prime Minister Gordon Brown has stated they are thinking of using that model again.

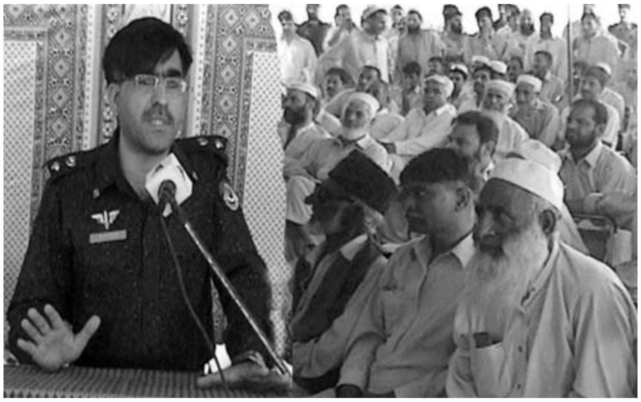


The Northwest Frontier Province region.
(Wikimedia)

I have done this same sort of thing, community policing in my districts, and we were successful in controlling crowds who were demonstrating against the Danish cartoons [depicting the Prophet Mohammed, in 2006]. The city of Peshawar experienced tremendous looting, killings, violent demonstrations. It was a similar case in Lahore, where banks were looted by criminals who crept in among the agitators… but not in district Charsadda. There were 54 different protests and demonstrations in the months of February and March, 2006. But not a single case of disruption or looting took place because we took local leaders into confidence. We told them "you may stage your protests, you may show your anger, but you may not be violent because the chief is with you. If anything happens, it will be on you." So they cooperated with the police – that is how we do good community policing. Many a time in this War on Terror law enforcement officials have been kidnapped and some were killed – their throats cut. But in some cases, when there is some confidence building between the people and the police, the kidnappers will release them. There is a thing called "Nanewatei," [a forgiveness process] or regret, in which people go before the "Jergah" [tribal consultative body], tender an apology and ask for a pardon in the name of God. You pay them something, and admit your fault, and you can be forgiven in the local system. Islam endorses this: when someone is repentant, you should forgive him. Yesterday I mentioned the incident where NATO airstrikes killed 82 small children reciting from the Holy Book, and then suicide bombing started happening in Pakistan as retaliation. Were I the commander of NATO forces at that time, I would have called for a Jergah, asked the bomber pilots to accompany me, and go to that area. I would have told the council: "we were given bad information, we are unhappy over this incident, we are your brothers, we are not against Islam. It was a mistake, we apologize for it." This would have been a good move, and they (NATO) would have been forgiven by the tribal people. You can do this if such a thing happens again, and see the results.

***IO Sphere**: Which is certainly another reason to better understand the culture. You've talked about the importance of dialog. What are your thoughts about inter-faith exchanges, such as between Muslims and Christians?*

Fasihuddin: I'm a strong supporter of inter-faith dialog, for many reasons. In Arabic, there is a saying [speaks phrase], which means "the strength of a man lies in his intelligence and his tongue." It does not say it is in your hands. The Holy Book says time and again it is for people who think. [Recites passage from the Quran] "There are signs in this book for those who have intelligence." I have yet to see a verse in the Holy Book that says: "This book is for those who fight." I have read it many, many times, when I was in Islamic school [madrasah]. I had an Islamic education because I belong to an Islamic family. The Holy Book says [recites verse from Quran] "All People of the Book, come to a dialog. Come to a point where we share what is common." We all worship God, so come to this common point. India for example, was conquered by the Muslims in 710 AD. Until the coming of British rule in 1857, India was ruled by Muslims. Yet there were marriages, mixing of families. History does not show Muslim rulers persecuting Hindus. The great Mogul Emperor Akbar was supported by the best ministers, who were Hindu. The best rulers had the support of Hindus and others. We lived there in relative harmony for centuries, and it was not until the British policy of "divide and rule" that created differences between the faiths. Many books were published with accusations, and no one knew who was publishing what. In 1918 there was the Khilifat Movement [launched by Muslims in India to protect the Ottoman Caliphate after World War I], but this was stopped by Western interests. In Pakistan, the Father of the Nation Mohammed Ali Jinnah, when he first took charge, was asked by a Hindu scholar about treatment of minorities. He said "I'll not be the Governor General of Pakistan, I'll be the Protector General of Minorities!" He said "you are free to go to your mosque, your church, or temple… there is religious freedom." In the modern era, Pakistan is a Muslim country, but we are surrounded by India and China… Iran and Turkey are Muslim, yes. China has tremendous respect in Pakistan, ask anyone. There is no anti-Chinese feeling there. There might be some in the US, but not in Pakistan. The Japanese are the most respected people in Pakistan. Why? Because they are free thinkers! Now as far as India goes, we don't have disagreements with them on a religious basis—there are political problems. How many Muslims live in India? About the population of Pakistan. Are they barricaded in? Is India going to "throw them out" to Pakistan? No.


Community policing in action. (Author)

Right now, interfaith dialog is a necessity. Why? Because the War on Terror has been given a color of religiosity. To the uneducated Muslims, it has been painted as a war against their religion. That is the biggest problem of this war. Muslims must be told this is not a war against any religion, or group belonging to any religion. Killing in Islam is forbidden: if a terrorist kills an innocent person, he is not a true Muslim, he is not a true believer! His ID card or passport might be labeled Muslim, but he is not a true believer. We need interfaith dialog, because if religion has the strength to divide people, it must also have the strength to unite people. Religion is a great motivating factor, a great engine to guide people! You need computer networks, media and books to influence people, and the words of great leaders in speeches… but you have a big, influential, powerful tool in your hands. But why haven't you used it for bringing peace to the world? How many people believe in religion? Millions, maybe billions… most people! So, if they believe in something, they should believe progressively, systematically, for all humanity. People should not believe in something that destroys humanity. Religion is an asset, which unfortunately we cannot use. You use poetry, music to motivate people… why can't you use religion? That's why the terrorists have gained on us; they are motivating people with distorted words. We should be ahead of them, using religion in true perspective, to move the people against the terrorists. They are fighting us with something that is very much in their minds: they think they will be praised by Almighty Allah, that the Prophet will receive them in Paradise. This is a force in the hands of bad guys. Yet, where are the counterarguments? We have kept our eyes closed! We must start telling them that bad people are giving false information, that these people are conspirators who have twisted the words of the Prophet… they must be told they are being fooled. The Prophet says if someone attributes something to him that he has not said, that person should seek his place in Hell. We need to show skills, knowledge, technique, and explain that these people are going against the words of the Prophet. Religion is a great power in the hands of intellectuals and policymakers, but their advisors and ministers are not well-versed in religion.

The Western media is making a mistake: there is only one religion that is Islam. There are sects, just like in Christianity and Judaism, just like there are tribes in various nationalities. Certainly there are schools of thought, just like in a Western university with different departments: they don't fight, they interact via dialog. But the Western media, due to meager understanding of our culture, says there is "political Islam," "militant Islam," "Islamic terrorism," "radical Islam." How many more words can there be? But, simple Muslim people say "look, the West is propagandizing against us." Now, if you say for instance, look at Mr. So-and-So in a specific group like Al Qaeda, he is a terrorist. Or, there are bad guys in the fighting or combatant part of the Taliban. Then [the people] will understand you are not painting all Islam. If you name a specific group and call them "bad," you have reservations about their policies and political agenda, well, you have free speech and can call them what you want. What is really meant by terms like "political Islam" or "militant Islam" is that Islam speaks on different aspects of life: Islamic view of politics, Islamic view of society, Islamic concept of history. You can find theses and doctorate work on these topics. But saying there is "militant Islam," we don't know that. The Prophet says Muslims do not use their hands or their tongues against other believers. The Holy Book says peace is the best. So where are these people getting "militant Islam" from the Holy Book?

***IO Sphere**: Unfamiliarity with the proper expressions hurts everyone in this situation. And we often look for the differences rather than common elements among faiths.*

Fasihuddin: Yes, like the cartoon issue [Danish newspaper depiction of Prophet Mohammed], and how we controlled this situation. We asked the international community for interfaith dialog, and many people have written about it. There are similarities, because the truth has been revealed unto many: Abraham, Jacob, Isaac, the Tribes. We don't distinguish who is better; all have had knowledge and powers revealed to them, but we are not supposed to judge among them, who is greater, who is smaller. The same is true for modern scholars, for example, Radah Krishnum was a great person. I respect him tremendously. He was a great scholar, a teacher at Oxford University [UK], and he was the President of India. We must read his books and teachings about religion, the importance of religion. I have quoted many times from his books in my work, and you can see in his works how religion can be used for the betterment of mankind. Again, the question is how well we can use it.

***IO Sphere**: Thank you very much. I don't want to keep you from the seminar any longer, so we should get you back there.*

Fasihuddin: Yes, thank you very much.

Fasihuddin served as the Police Chief in two districts, as Deputy-Director Intelligence Bureau of Pakistan (Research and Anti-Terrorism Section), and as Commanding Officer in the Frontier Constabulary in the semi-tribal areas of Pakistan, next to Afghanistan. Presently, he is the Deputy Commandant, Frontier Reserve Police, NWFP. He received many awards and distinctions during his school and college days, including an award from the President of Pakistan on 'Islam and Contemporary Issues' in the Civil Services Academy of Pakistan. He presented his paper on 'Knowledge-Based Poppy Cultivation Control: Personal Experience from Local Police Practice' in Turkey, selected for publication in the *Special Issue of Police Practice and Research*, a peer-reviewed magazine. He presented his community policing best practices on the subject, 'Blasphemous Cartoons: Agitation and Local Police Efforts in District Charsadda, NWFP, Pakistan' in the 6th Annual Meeting of European Society of Criminology. He is currently introducing criminology as a separate academic discipline in Pakistan, having written a proposal and master level curriculum now under review by scholars and intellectuals. Fasihuddin received his Bachelor of Law (LLB) and Master of Political Science with Gold Medal from the University of Peshawar, North West Frontier Province (NWFP), Pakistan.

Ask the Cyber Insurgent

By Jan C. Norris, Major, USA

Editorial Abstract: This article won the 2007 Armed Forces Communications Electronics Association Excellence in C4I/IO Writing Award at the US Army Command & General Staff College. Major Norris provides a critical analysis of the current US military information superiority posture, and recommends a construct to enhance cyber targeting and surveillance.

"Attention in the operations center, attention in the operations center, as of 0730 this morning, our steady theater IO campaign has allowed multi-national forces to achieve information superiority, Victory is imminent."

These words have assuredly never been uttered in any US-led military operations center, nor are they likely to be heard anytime soon in Iraq or elsewhere… at least not with a straight face.

US Joint and Army Information Operations doctrine maintains that achieving information superiority (IS) is a critical factor for success in military operations. Yet for the past four years, US forces have been unable to achieve true IS in connection with Operation Iraqi Freedom (OIF). While possessing an overwhelming edge in information technology to dominate IS, US forces have faltered in one critical area: denying the enemy the ability to collect, process and disseminate an uninterrupted flow of information. Through five years of OIF, the cyber-enabled insurgent has evolved and operated relatively uninhibited using the Internet and media. Both serve as a means of controlling and sustaining momentum, and achieving both tactical success from within by recruiting and mobilizing personnel—and strategic success by influencing international perceptions. If IO are to ever gain status as a decisive form of operational warfare, the US must increase the focus and scope of cyber-surveillance and targeting, so that forces engaged in OIF can deny the cyber-insurgent cyberspace Internet and media access and mobility. To edge closer to achieving a level of IS that directly impacts operational success, we need to establish a Joint Cyberspace Surveillance Targeting Cell (JCST).

Given current tenets of IO doctrine and the ability of US forces to successfully dominate in a majority of the contributors to IS, there should logically be some degree of IS influence on military operational success. But does achieving IS really matter if there is no effective way of denying or mitigating the enemy's medium for information exchange? Is achieving IS even a real concern for today's commanders at the operational level of war?

Security Operations Center. (US Army)

In Iraq, several distinguished leaders developed innovative techniques and procedures for success in defeating local insurgents on the ground, and engaging the Iraqi populace using IO. Many recognize General David Petraeus and Colonels H.R. McMaster and Dave Putnam for their exceptional ability to conduct successful tactical ground campaigns against the threat, while also and perhaps more critically, engaging the Iraqi leadership and population through sound IO efforts. Despite successful IO and recent positive "surge strategy" trends, there appears to be little attention, focus or mention of achieving IS in after action reviews and lessons learned. A much longer period of time is still needed to achieve the desired end state of Iraqi autonomy, where the insurgency is neutralized and host nation population confident in a stable, legitimate government.

The OIF scenario leads back to similar questions; what difference does having IS and conducting IO matter for US forces in Iraq? On the ground, it certainly helps in building trust and confidence between Iraqi local communities and US military and Iraqi forces while having the ability to collect intelligence via advanced systems and technology helps in detecting patterns of activity to track and target the enemy. But are IS and IO helping to mitigate the cyberspace activity sustaining and feeding the insurgency? From a macro view of the information environment, do US forces truly have IS? In most cases the answer is no. Very little is being done to decisively engage the enemy in cyberspace. An insurgent can possess information superiority and an information advantage because he can stay hidden, yet see US forces and decide when to attack. IO efforts and achieving IS can be fleeting; its forces must recognize this and take action to reduce the enemy's IS and operational efficiency. IS in the new operational environment must include denying information helpful to the enemy. A recent posting to an extremist Web site announced a competition to design a new Web page for an Iraqi militant group. The incentive was the chance to fire missiles by remote control at a US military base.

Since 9/11, the growth of extremist-related Web sites has grown significantly to well over 4,500. Many of these sites strongly advocate Al Qaeda's ideology and have evolved into virtual bases for recruiting, training, coordinating attacks, sharing information, fund raising (even using PayPal) and influence. The Internet allows for 'cyber-mobilization' of a variety of ethnic populations around the globe with similar cultural and ideological causes. It allows many extremist groups to come together quickly in chat rooms and plan and coordinate activities. In essence, the Internet is feeding the cyber-insurgent at a steadily growing pace.

Terrorist groups have applied the same innovation and ingenuity on the Internet as they did in planning the intricate 9/11 attacks, especially in avoiding detection, disruption or destruction of Web site information. Common cyberspace stealth methods include use of encryption, domain name changing, use of proxy servers to obscure locations and “dead dropping,” where information is saved as draft messages in fake email accounts. These are accessible to anyone having a password, thereby avoiding transmission and detection. Considering the hundreds of thousands of servers and Internet service providers (ISPs) worldwide, plus the billions of bytes being transferred every second, the insurgent/terrorist has a large playing field to roam—with many choices for data and site hosting. Not surprisingly, many significant Al Qaeda and extremist-linked sites in recent years have been sourced to American ISPs, and their presence was largely unknown to the US providers.

In essence, the Internet is the ideal communications tool for insurgents, and it reflects the framework of their operations: decentralized, anonymous, and offering fast communication to a potentially large audience. It has created a virtual or cyber ‘umma’ [Arabic for the larger Muslim community], which like the actual umma, encompasses both moderate Muslims and Islamic fundamentalists.

Therefore, regulating cyberspace terrorism and insurgent activity is quite challenging for the US. Law enforcement agencies have, for example, become very efficient in tracking and convicting cyberspace violations of child pornographic laws, but face legal hurdles in the cyber-insurgent fight. Challenges include rights to free speech, getting international partners to take decisive action, and crossing of international borders when targeting cyberspace terrorist/insurgent data. Coupled with the fog of countless on-line insurgent activities, these legal restraints and data flow have left the US government far behind their adversaries in terms of Internet skills and achieving IS. A contributing cause is a lack of cultural and language understanding, and not being able to properly get inside the insurgent’s cyberspace ‘circle of influence.’ Some of the most important US Government agencies tasked with tracking and intercepting Al Qaeda members and activities in cyberspace place little importance on the technological and cultural aspects—and associated skills and knowledge—that are critical to the fight. We must establish a method for better combating cyber-insurgents, one where the Department of Defense is teamed up with Interagency organizations.

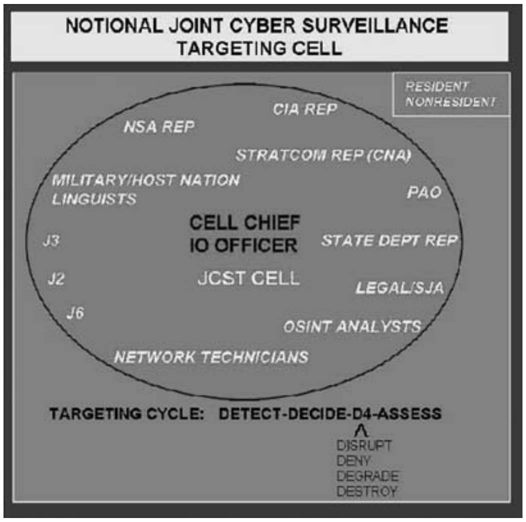


Figure 1. Joint Cyber Surveillance Targeting Cell.

Current IO doctrine addresses Computer Network Attack (CNA) as a subset of computer network operations (CNO), specifically “actions taken through the use of computer networks to disrupt, deny, degrade or destroy (D4) information resident in computers and computer networks.” Little else is discussed, as CNA details and processes are sensitive and classified. JP 3-13 does describe a notional joint IO cell, but without specific emphasis on cyberspace surveillance and targeting.

While combating the cyberinsurgent is a complex task akin to “a cat and mouse chase and finding a needle in a haystack,” certain deliberate measures can have impact. Creation of a Joint Cyber-Surveillance Targeting (JCST) Cell (Figure 1) inside at the operational level is a start. For example, in the US Central Command (CENTCOM) theater of operations, a JCST cell could be embedded within the MNF-I staff in Baghdad—where it is currently needed most. In other regional combatant commands (RCC) without active on-going combat operations, the cell would function at the RCC headquarters. As this mission clearly falls in the information environment, the fifteen to twenty member cell would be led by an IO officer (O-5 or O-6). Specialties would include interagency cyberspace analyst representation from the CIA, NSA, USSTRATCOM, FBI, and State Department as well as joint military intelligence open-source analysts and linguists, host nation linguists, and information technology specialists (both military and contractor) specializing in wide area network architecture and attack/infiltration. Manning the cell jointly would better educate and train military and government agencies for future joint cyberspace related operations. The JCST cell would continuously scan the Internet for suspected insurgent/terrorist activity, and employ developed technologies, harnessing automation to search and capture Web content. Acting much like a conventional joint targeting cell, the JCST could use a targeting model similar to the Decide-Detect-Deliver-Assess (DDDA) process. However, with Joint Cyberspace Surveillance and Targeting, the process would change to Detect-Decide-D4-Assess, where D4 is “disrupt, deny, degrade or destroy.”

JCST cell operations would detect and analyze suspected sites, and if the leadership decides the site is a source contributing to insurgent/terrorist activities—and can be targeted—the cell could take the next step. Network technical specialists would move to take one of four actions: disrupt, deny, degrade or destroy the site, or let it remain as is for further exploitation. Cell efforts could also re-direct individuals browsing the Web for insurgent sites toward US-constructed sites, providing counterpropaganda to potentially dissuade an insurgent recruit. Decisions to execute any action against a site ultimately rest with the JCST cell chief, unless suspected sites involve external countries where action may involve political sensitivity. In cases where the terrorist site source or host is outside the US, and targeting the associated network or server would impact other important non-insurgent users or organizations (i.e. a banking network), the cell would use a target nomination process. The JCST State Department rep would use Department of State channels to contact the source country for targeting clearance. This approval process would need to carefully avoid compromising US intelligence gathering techniques. Once a site is targeted the cell would make follow on assessments, revisiting ISPs with a history of known or unknown insurgent hosting, to track any recurring patterns. When possible, the JCST would collect and target individual webmasters who are building and creating such sites. Though the scope of targeting such individuals goes beyond the capabilities of the JCST cell proposed here, the information collected would be passed on to appropriate State Department, law enforcement or military officials for action. International support is essential for denying service, particularly in developing countries with known cyberspace terrorist activity and weak governments.

US Government and military personnel may quickly refute the JCST idea as 'double work,' given what the Joint Functional Component Command-Network Warfare (JFCC-NW) and other DOD CNO teams already provide. However, few if any such cells exist with the necessary mix of military and interagency expertise collocated in one spot. Having the cell forward, on the ground in a combat theater of operations may also seem pointless given current communications reach capabilities; yet it is vital. A forward point of presence optimizes speed of decision for establishing linkages, from cyber-insurgent planning, training and recruiting activities, to insurgent activities on the ground. Forward presence also allows direct 'face-to-face' access with the theater commander (MNF-I) and joint/coalition staff. Further, targeting cell personnel can gain a much better situational understanding of insurgent operations by being 'in the culture.' They get a better perspective on insurgent motivation by having host nation personnel available to translate both cultural and linguistic aspects of extremist website content. Additional JCST cells could be positioned in different countries within the theater, where languages and cultures vary and regionally-specific specialist staffing is appropriate. Over time, given proven quantitative measures of effectiveness, theater commanders could track 'cyberspace targeting' as a line of operation contributing to defeat of the enemy center of gravity—and protecting coalition forces and missions.

Many consider the power of the Internet as a means for global information sharing, communication and creation of virtual communities among the most important innovations of the past century. Yet this same interconnected network of worldwide computers, switches and servers, and the cyberspace contained within, has equal potential as a tool for enabling terrorism and death. As enemies of the United States continue to overtly attack its military technological strengths through asymmetric and insurgent warfare, they will also continue to exploit the power of the Internet to extol their ideology and kill Americans. Are information operations a decisive form of operational warfare? If one were to ask the cyber-insurgent, the answer right now is *yes*. Their operational efforts in cyberspace have been decisive for tactical success. In his September 2007 report to Congress on the situation in Iraq, General Dave Petraeus noted "the need to contest the enemy's growing use of that medium (cyberspace) to spread extremism" and that "regional, global and cyberspace initiatives are critical to success." Bridging the gap between the Interagency and military, the proposed JCST cell is an IO organization with potential to neutralize and defeat the cyber-insurgent by bringing together the right mix of personnel to decisively combat insurgent cyberspace activity. Positioned forward in the combat theater, the JCST cell will be immersed in the target culture, to better link operational insurgent activities in cyberspace to tactical actions on the ground. Since OIF began, the relevance of IO, achievement of information superiority, and which side truly has the information advantage all remain in question. By enabling US forces through a deliberate process for targeting and denying enemy information flow in cyberspace, the JCST cell could well prove IO as a decisive form of operational warfare. We may still earn shouts of 'imminent victory' in the theater operations center… with a straight face.

MAJ Jan Norris, US Army, serves as Chief of Current Operations, 311th Signal Command (Theater), Ft. Shafter, HI. Previous assignments include Commander, High Tech Regional Training Center, Sacramento, CA and G33 Information Management Officer, I Corps. He holds a BS in Journalism from Virginia Commonwealth University, a Master's in Applied Linguistics from Old Dominion University, and completed Command & General Staff College in 2007.

Joint IO in Counterinsurgency Warfare: A Critical Gap in Capability

By Lane V. Packwood, Major, USA

Editorial Abstract: MAJ Packwood examines the challenges of carrying out an influence campaign at the operational level, especially given current counterinsurgency demands. He argues that while our ability to conceptualize and synchronize information operations improves, we need to revise IO culture through new guidance and behaviors.

Counterinsurgency warfare (COIN) is now a subject of utmost importance within the Army and Marine Corps. Afghanistan and Iraq have refocused attention on this particular form of conflict as it fits into the Range of Military Operations, and strategists theorize that such Irregular Warfare may be the rule rather than the exception in the future. As a consequence, both services have published updated COIN doctrines incorporating the hard lessons learned over the past 5 years. Succeeding in shaping the information environment features prominently in the updated doctrines. At the same time information operations has been evolving to provide commanders with this capability. However, while our ability to conceptualize and synchronize IO is improving, current joint IO doctrine does not provide an optimal framework for addressing the most urgent IO need in COIN: influencing a neutral majority of non-combatants to support US objectives. In spite of its widely acknowledged importance, current doctrines and organizational cultures impede us from successfully "winning hearts and minds" in counterinsurgency warfare.

COIN warriors at work. (US Marine Corps)

IO in Counterinsurgency Warfare

The 2006 edition of Field Manual (FM) 3-24, *Counterinsurgency*, contains the US Army's revised COIN doctrine. According to this reference, an insurgency is "an organized, protracted politico-military struggle designed to weaken the control and legitimacy of an established government, occupying power, or other political authority while increasing insurgent control." Counterinsurgency, therefore, is an "internal war." It is "military, paramilitary, political, economic, psychological, and civic actions taken by a government to defeat insurgency."

These political and psychological actions take a prominent place in FM 3-24 based on a critical assumption about the ideological loyalties of the general population during an insurgency. Between insurgents and counterinsurgents is a larger neutral majority undecided about which side offers a better future. FM 3-24 states that "the primary struggle in an internal war is *to mobilize people…* for political control and legitimacy [italics added]." The real objective is not to seize and hold terrain or to decisively defeat enemy formations (although these may be necessary), but to win the support of a "neutral or passive majority" of the population. Both insurgents and counterinsurgents must mobilize this neutral majority to their respective cause in order to ultimately triumph. Because of this, "the information environment is a critical dimension of such internal wars, and insurgents attempt to shape it to their advantage." Thus, the political and psychological struggle to attain legitimacy in the minds of a neutral majority, not the physical destruction of enemy fighters, is the counterinsurgent's supreme imperative.

Therefore, by necessity this neutral majority constitutes a population of non-combatants, although a prominent feature of insurgency is the almost complete lack of distinction between non-combatants and active fighters. Even if this neutral majority gives tacit support to imbedded insurgents for social and cultural reasons, or is likely to do so, FM 3-24 asserts that they can be swayed—indeed, they must be swayed—and therefore occupy a distinct non-combatant role in the battlespace. In fact, if we follow the logic of FM 3-24 to its necessary conclusion, the key measure of effectiveness for a successful COIN is the steady conversion of yesterday's high value targets into tomorrow's loyal allies.

In this environment, FM 3-24 looks to Information Operations as critical to the overall success of the mission. All operations, lethal and non-lethal, must be conducted with an eye on the psychological effect on this population of non-combatants. "Arguably, the decisive battle is for the people's minds; hence synchronizing IO with efforts along the other [logical lines of operations] is critical. Every action, including uses of force, must be wrapped in the bodyguard of information."

A joint Marine Corps-Special Operations Command *Multiservice Concept for Irregular War* is equally emphatic on the importance of IO in influencing non-combatants. This guidance highlights how understanding the role of ideology in a counterinsurgency is "essential to campaign development." "Information operations must infuse all other lines of operation so that every activity creates the correct perception." Commanders must manage perception in ways that "morally isolate" the enemy (insurgents) from the population (non-combatants) in ways very similar to FM 3-24.

In short, US counterinsurgency doctrine states that it is crucial for IO to influence a neutral majority of non-combatants to support US objectives. This all-important need is echoed by commanders in the field. Colonel Ralph Baker, Commander of the 2nd Brigade Combat Team, 1st Armored Division, wrote of his experience in Baghdad:

> *Soon after taking command of my brigade, I quickly discovered that IO was going to be one of the two most vital tools (along with human intelligence) I would need to be successful in a counterinsurgency campaign. COIN operations meant competing daily to favorably influence the perceptions of the Iraqi population in our area of operations. I quickly concluded that, without IO, I could not hope to shape and set conditions for my battalions or my Soldiers to be successful.*

Other commanders at the tactical level consistently remark that IO is essential to garnering support among local populations, in order to make any progress along other lines of operation. "Whoever achieves victory will be the opponent who most effectively conveys his perception of reality and aspirations for the future with a host-nation populace and an international audience" writes one company commander. LtCol Joseph Paschall, Chief of Psychological Operations at Headquarters Marine Corps' Plans, Policies and Operations Division, writes that at the end of the day IO is "influencing the way someone thinks" in order to "build rapport," "form relationships," and "capitalize on good works." To this I add my own experience as a company commander in Kirkuk, Iraq. Influencing the neutral majority of non-combatants to support US objectives was by far our highest priority and one that we struggled with daily.

Joint IO Doctrine

The importance of IO in COIN provides much of the current urgency in updating and improving joint IO doctrine. Joint Publication (JP) 3-13, *Information Operations*, provides a 2006 revision that defines IO as "the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC) and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." EW, CNO, PSYOP, MILDEC and OPSEC form the five IO core capabilities, with other functions, particularly Public Affairs (PA), providing supporting and related capabilities.

"Influencing the neutral majority of non-combatants to support US objectives was by far our highest priority..."

Not every capability within this broad spectrum is equally important in influencing the neutral majority of non-combatants, however. While EW and CNO provide the Joint Task Force (JTF) with very powerful tools for achieving specific effects, their primary use is against adversaries' communication networks, as opposed to non-combatants. Jamming cell-phones and reading emails add a great deal to the fight against insurgents, but it is more difficult to see how they will endear non-combatants to US objectives at the same time. Nor will MILDEC or OPSEC, two very operations-centric capabilities, have a large impact on influencing broad public attitudes in the way COIN doctrine demands.

Two other capabilities provide much more promise: PSYOP and PA. PSYOP in particular seems ideally suited for the task of influencing the neutral majority of non-combatants. DOD defines PSYOP as "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals." Of all the IO capabilities, this definition of PSYOP seems to fit the bill perfectly.

In practice, however, neither PSYOP doctrine nor organizational culture fully supports influencing the neutral majority in COIN. Doctrinally, PSYOP is actually far more focused on adversarial targets, which in the COIN environment consists of enemy fighters and their direct supporters. The DOD *Information Operations Roadmap* repudiates the above definition, summaring PSYOP as "aggressive behavior modification" of "adversaries (implicitly combatants, regular and irregular, and those who provide them with intelligence, logistics, and other assets in the operational milieu)."

This view is supported by a comprehensive National Defense University study on the uses of PSYOP in Afghanistan and Iraq. Its analysis of the sometimes conflicting Joint and Army PSYOP doctrines "observed that all of the PSYOP objectives enumerated in joint doctrine for both stability operations and major combat operations easily fit into four broad mission objectives." These were "isolating an adversary from domestic and international support," "reducing effectiveness of adversary's forces," "deterring escalation by adversarial leadership," and "minimizing collateral damage and interference with US operations." Notice that three of the four mission objectives are explicitly adversary focused.

One can also see this adversarial focus in PSYOP's historical performance. The NDU study shows PSYOP is very effective in delivering specific messages to specific adversaries at the tactical level, such as delivering leaflets or broadcasts to persuade enemy units to surrender. When thoughtfully integrated into tactical operations, PSYOP can help win engagements and save lives. But when called upon to influence non-adversaries on a wider, more general level, the results are much less clear. The IO imperative in COIN doctrine seems to imply theater-level or "strategic" PSYOP directed and managed at the JTF level to shape the attitudes of a large population of non-combatants.

In IO doctrine, this is the intended role of the Joint Psychological Operations Task Force (JPOTF). Briefly, a JPOTF is a joint PSYOP cell assigned to a JTF to advise the commander and provide a link between the tactical PSYOP assets supporting maneuver forces, the JTF, and higher supporting assets in the Combatant Command or DOD. In recent COIN operations, commanders have used the JPOTF to provide the theater-level efforts to "convey the legitimacy of US policy and objectives to the general population," which would presumably be an effort to influence the neutral majority. But according to the NDU study, the performance of the JPOTFs in Afghanistan and Iraq has been largely disappointing. Their efforts have been marked by "friction, assessment difficulties, and, at times, a lack of sophistication." Commanders and PSYOP practitioners consistently complain of poor communication between the JPOTF and both higher and lower assets, as well as low product quality, confusion in goals, and ambiguous results.

While some of this is undoubtedly the result of basic resource shortfalls, discrepancies in PSYOP doctrine and organizational culture lie closer to the root cause. At the theater or strategic level, PSYOP starts to blend with PA and public diplomacy, raising several serious doctrinal and policy issues. This difficulty is further exacerbated by organizational culture. Many PSYOP practitioners resist this broader mission, and are ill-trained to do it. Naval War College strategist Carnes Lord writes, "The military PSYOP community has been sensitized over the years to the deep unpopularity of PSYOP in the wider culture." Military and civilian leaders alike tend to look upon PSYOP with a combination of skepticism and suspicion. Lord writes that in response the PSYOP community tends to askew the kinds of campaigns needed for non-combatants, and continues to operate with very risk-adverse product approval processes.

PSYOP then, does not perform in the broad manner described by Joint Doctrine. It does not operate equally against all "foreign audiences." The JPOTF notwithstanding, PSYOP's mission, capabilities and culture make it very adversary focused. Lord argues that "the comparative advantage of PSYOP as a military instrument is clearly on or near the battlefield, in close conjunctions with and support of actual operations or their aftermath." The NDU study supports this conclusion and goes so far as to recommend that PSYOP focus on its tactical adversarial mission objectives and not be looked upon as a tool of public diplomacy or PA (through the JPOTF, for example). Study author Christopher Lamb writes, "PSYOP doctrine and mission statements that could easily be confused with mandates to conduct public diplomacy and public affairs are not helpful."

"If PSYOP cannot effectively influence the neutral majority in COIN, can Public Affairs fill the gap?"
(Defense Link)

If PSYOP cannot effectively influence the neutral majority in COIN, can Public Affairs fill the gap? The mission of PA is to "expedite the flow of accurate and timely information about the activities of US joint forces to the public and internal audience." Whereas PSYOP may be ill-suited for shaping attitudes among ambivalent non-combatants, PA seems to naturally operate in this area. PA Officers (PAO) see their primary responsibility as maintaining credibility and truthfulness, two critical advantages in the fight with insurgents for legitimacy. Some in the IO community argue that this makes it "the ultimate IW [information warfare] weapon," precisely since it is "so stalwart in its claims of only speaking the truth."

To a certain degree, the integration of PA into IO Cells in Afghanistan and Iraq reflects this view of PA's role in COIN. Through distinct IO Cells in the JTF staff structure, with designated senior IO staff officers in charge, commanders attempted to comply with the Joint IO Doctrinal vision of "integrated employment." An IO Cell is a natural way of bringing together IO's core, supporting and related capabilities, of which PA plays a very public and important part. Some argue that they succeeded too well. Critics allege that several operations actually included attempts to use PA or PA-like activities to conduct MILDEC and PSYOP. Accusations continue that commanders fed false information to the media with the intent of deceiving adversary fighters on the battlefield, who they knew were watching.

As a result, the PA community has strongly resisted this trend. PA's organizational culture does not support this kind of influencing and DOD policies against propagandizing domestic audiences, even inadvertently, place this kind of "integration" in murky legal waters. Many PAOs vehemently object that current joint doctrine "allows influence operations to bleed into public affairs and allow IO officers to use the press as a battlefield tool." LTC Pamela Keeton, former PAO for Combined Forces Command-Afghanistan, writes, "In theory, the idea of merging PA, IO, and PSYOP appears to make sense; in practice, however, the goals of these three functions are quite different. Public Affairs is charged with informing the public with factual, truthful information, while IO and PSYOP seek to influence their audiences to change perceptions or behavior."

In addition, PAOs resist proactive strategic influencing even when it entails nothing but factual, truthful information. Lord writes "it is the nature of the public affairs function to be reactive rather than proactive and concerned primarily with day-to-day handling of the domestic press." PAOs eschew anything resembling manipulation or "spin," regardless of factual accuracy, and prefer straight-forward, carefully phrased press releases on daily events.

To summarize, in spite of the supreme importance laid out in COIN doctrine of winning the support of neutral non-combatants, joint IO doctrine does not provide commanders with the clear capability to do it. This kind of Information Operation hits a seam in our doctrine. On the one hand, PSYOP is best suited for targeting adversaries in tactical contexts. Its doctrine and organizational culture militate against broad, general influencing and commanders are highly sensitive to PSYOP's stigma in the public eye. On the other hand, PA resists any subordination and integration into what it sees as potentially manipulative influencing operations—and prefers sticking to basic daily fact providing to media contacts.

Solutions

A full-examination of potential solutions to this capabilities gap is beyond the scope of this article. Possibilities include reassessing PA doctrine to make it more amenable to influencing, rather than simply informing, foreign audiences. One line of reasoning focuses on the nature of truth, and casts doubts on PA, or any information source, being able to transmit unbiased truth regardless of its stated intention. "We in the West, and particularly in the United States, tend to believe that there is only one truth and that others see and understand as we do," writes Christine MacNulty in a US Army War College study. "In the Armed Forces, this is known as "mirror-imaging"; in anthropology it is known as ethno-centrism." According to this line of reasoning, PA is naïve in supposing that it can only be involved with simple informing. The very act of informing implies some version of mirror-imaging. It would be best if PA adjusted to integration into a synergistic IO campaign that achieves the commander's intent.

And yet, this is so counter to PA's internal beliefs, and potentially so damaging to public perception of military operations in the domestic press, that few advocate this change. If the association between PA and IO becomes common knowledge, PA risks damaging the integrity, truthfulness, and credibility of its meesage sources and contents.

Others argue that the activities necessary to influence neutral non-combatants require entirely different capabilities at the operational and strategic levels of war than either PA or PSYOP can currently provide. Carnes Lord recommends DOD create an entirely new capability called "defense public diplomacy." This would require a new cadre of public diplomats or communicators within DOD (including the uniformed military), specialized in strategic communication. This would clearly add powerful tools to a JTF commander's IO arsenal, but at enormous cost. Lord's proposal requires a new functional combatant command staffed with hundreds if not thousands of highly educated strategic communicators in and out of uniform. No doubt a leap forward, but one still years (and hundreds of millions of dollars) down the road.

The most pragmatic solutions then, may lie in reforming PSYOP itself. One could go against the recommendation of the NDU study, for example, and continue working on improvements to theater/operational level PSYOP through the JPOTFs. This will require new doctrines, career paths and professional education for PSYOP practitioners, so they can influence complex non-adversarial audiences far better than they do currently. More significantly, it will require a new public persona for PSYOP, one that puts practitioners and observers more at ease with the business of influencing. There does not seem any simple way to delineate where PSYOP ends and public diplomacy or PA begins, especially when dealing with neutral non-combatants. There may not be any clear demarcation, and thus no practical way to assign these different functions to clear "lanes." Before pouring more resources into efforts that many people describe as 'propaganda and manipulation,' PSYOP will have to find some way to portray its efforts as 'marketing' or 'engaging.' It is a subtle difference, but an extraordinarily important one. Ultimately, this last challenge may prove more difficult in the end.

Bibliography/references for this article are on the IO Sphere Home Page at: https://www/jiowc.osis.gov/Publications/IOSphere/index.cfm Click on the "updates" link under the Spring 2008 issue.

MAJ Lane Packwood, US Army, is a Field Artillery Officer in the Idaho Army National Guard and is currently a student at the US Naval Command and Staff College, Newport, RI. MAJ Packwood has a BA from Brigham Young University and a MA in Political Science from the University of California, Los Angeles. MAJ Packwood has served in various command and staff positions in both the US Army and Army National Guard, including a tour as Battery Commander during Operation Iraqi Freedom.

In the Mountains of Afghanistan: Brian Glyn Williams Interview

Interviewed by John Whisenhunt, Editor

Editorial Abstract: Dr.. Brian Glyn Williams shares a ground-level perspective on tribal groups in Afghanistan, noting differences in attitudes toward the Western militaries. He observes a lack of cultural training and awareness among NATO and US forces in the region, and recommends revised standard operating procedures to help the current influence campaign.

IO Sphere: *We'd like to start off by talking about your last trip to Afghanistan. You've described more of a polarity between groups, especially when it comes to attitudes toward NATO and the US. You coined the expression "POAs" or "Pissed-Off Afghans," suggesting poor trends. What changes did you see?*

BGW: I remember being there in 2003, seeing an almost hubristic optimism. As an American, you felt like "There's nothing we can't do!" Momentum was on our side, the Taliban were "dead-enders," to use the expression coined by Secretary of Defense Rumsfeld. That sort of captured the moment. There was an occasional bombing in Kabul, and you heard about little rumblings or trouble down in the southern provinces, but momentum was clearly ours in 2003. People had really high expectations. Then the Americans began bringing in more troops. The Taliban regrouped, having gotten a lot of inspiration from the Iraqi insurgency, a lot of "hands on" training, and more examples of how to kill Americans; these things inspired and 'regalvanized' the Taliban. I went back again in 2005, and provinces I had no trouble entering two years earlier were a little more dangerous. The bombings were al little closer to home: an ISAF bus with troops aboard had just been blown up. The level of expectation had been tempered a little bit more by realities. Then I went back again in 2007, and boy, it had changed completely. There had been about 115 suicide bombings in the country, and it had the effect of say, the Beltway Sniper [Washington DC area in 2001] on common people's perceptions of progress. So, things were changing for the worst. For example, you could not drive from the capital in Kabul, to Kandahar [Afghanistan's second largest city], on this brand new "showcase" road we built, because it's too bloody dangerous! Foreigners can't go on that road. Most Afghans are afraid to go on that road unless they have some sort of protection from the Taliban—there are just too many checkpoints. So that speaks volumes on the level of security and stability, and optimism on the ground—things that shapes peoples' perceptions. Combine this with the Americans who are there, the sponsors of the Karzai government, are never really interacting with the populous. Most Afghans see them in the form of say some A-10s [Thunderbolt II "Warthog" aircraft] overhead, or convoys barreling through their town with speakers blaring "clear the way," or heavily armed guys in Kevlar running a checkpoint. If you wanted to spin this from an American perspective, it's like we had SWAT teams with shields and masks in say, Appalachia. Now say, make them from another country and you really compound matters. People would probably have that same perspective [as those who are intimidated by the US presence]. You're going to have disagreements, miscommunications, failing expectations, these all combine… then we have relatively few troops on the ground: remember this country is larger than Iraq. Our troops rely on close air support, which unfortunately cannot always be close enough, and we have the threat of "collateral damage"—which Afghans call 'dead friends and relatives.' All of these things combine, just like say a little thing like the high price of gas here makes people dislike our own government, to create those "POAs."

Dr. Williams and young Hazara friends near Bamiyan, Afghanistan. (Author)

IO Sphere: *Did you find a particular ethnic or tribal group more supportive of the West? Do you think we're properly factoring in the various groups in our influence efforts?*

BGW: I think I could almost rate the groups based on their identification with the Western mission. But are we as Americans taking those factors into consideration? No. As Westerners we underestimate the ethnic cleavages, the differences in language, in ways of warfare, religious differences, Turkic-Mongol versus Aryan-Pashtun histories etc. Even here in our conference, the word "ethnicity" doesn't come up! We seem to have a romanticized version of the country as being "Afghan," when only about 38% of the country really identifies themselves as Afghan – the ethnic Pashtuns. So that means we aren't dealing with groups like the Aimaqs [semi-nomadic, multi-ethnic], or the Turkmen, or the Uzbeks, or the Hazara, or the Tajiks. They almost don't exist in our vocabulary, yet they're the majority of the country. Ethnicity is very, very important, and very salient. It shapes everyone's' identity, and their perception of our mission, our assistance, in the country. If I had to give a broad generalization, I would say among the Pashtuns, you have greater resentment towards the US. It is Pashtuns who predominantly make up the Taliban, and live in the provinces that support the insurgency. Pashtuns live in Kandahar and Helmand, and Khost. Where there is violence in non-Pashtun areas, typically you will find Pashtun enclaves there. Traditionally they are the ones who fight off the invaders, they have a tradition of being xenophobic—fighting off all external interference, British, Soviet, American… the "infidel of the week." They are rightly proud of their fighting tradition, and I admire them on that level. They live in what I call the "Quran Belt," like the US "Bible Belt." They are more conservative, "family values," or fundamentalist types. They are more predisposed to see things through the lenses of religion, and a tradition of resistance. If you move to other zones, you have less xenophobic distrust. I have found Hazara… Shiites, to be very warm and welcoming. They are more liberalized, more secular, and have warm perceptions of the US. And if you move down from these mountain people, down to the plains: the Uzbeks, I found them to be very pro-American, very secular, very willing to have us come into their villages. Those are safe areas. You can travel across that [northern Uzbek] realm and not find someone who doesn't want us there. When traveling there I was told when I returned home to "tell the Americans not to leave! The day you leave, the Taliban will come back, the war will come back!" I found billboards thanking the US military! You just don't find that in Eurasia. I took pictures of several [such billboards]… amazing. Tajiks too I think are less xenophobic. But part of our problem is the other groups think we have sided with the Pashtuns, President Karzai is a Pashtun, as are many who run the government. So even though that's what we think of as a majority, it's not. People in the north say, well, the Americans are sponsoring him [Karzai and the Pashtuns], not us. So we as Americans underestimate the real depth of these historical animosities.

***IO Sphere**: You touched on this in your blog: the Pashtuns always seem to think "we'll drive the invaders out." Some groups want us there, but don't the invaders always leave at some point ?*

BGW: Yes, you hear this in the Taliban's pronouncements: "Time is on our side." They believe that. They will outlast us like all the past invaders. The Soviet experience taught them to believe in their own resilience, how they defeated a modern mechanized army, how they defeated the British Empire. These stories formed their identity in much the same way stories of the Alamo formed ours. So the Pashtuns certainly have that going for them. On the other hand, their self-perpetuated reputation overlooks some historically inconvenient facts. Other foreigners have in fact conquered them, and done a good job at it! The Mongols wreaked havoc with grace and ease, slaughtering thousands of Pashtuns. The Mongols ruled over them for hundreds of years, and Safavids from modern day Iran ruled over them. We typically don't know about these either, but the truth is they have been beaten, and beaten well in battle. And they won't tell you about it, but dig into history a bit and you'll find out. It's not in glib Western accounts either, which talk about the Pashtuns as being 'invincible.' They can be beaten. But they are in some ways living in history, thinking we are just like the last two invaders, Britain and the Soviets. But go back 150 years and the Sikhs ruled over Peshawar (a major Pashtun city now in Pakistan), go back a century before and the Mogols ruled Kabul, and before that the Mongols. So we need to be aware of selective memories on both sides.

***IO Sphere**: We talk about subtle points of culture, yet we still seem to have trouble learning them. You mentioned you met some of our experts who are in a secure area, behind a fence. Are security concerns making us too cautious at the expense of cultural understanding?*

BGW: Yeah. The only time the Afghans interact with Westerners is when our folks end up looking like "Robocop." Living in garrisoned community, and only getting out into the Red Zone, heavily armed, is going to be a disadvantage. The Taliban don't have these constraints. They move freely, use the cultural paradigms to interact with people, at all hours. They don't have to get approval 24 hours in advance to walk through a village, so this cultural and logistical capability gives the Taliban a tremendous advantage – the difference between the insurgent, and the "imperial" grunt, who is in some ways garrisoning a frontier. There is no way to get around that without getting our troops into the villages. It might make them a target, but it might let them interact on a less hostile basis with those people we want to win over. Once again, we're back to winning hearts and minds of people, pulling them from the insurgents… very much classic counterinsurgency doctrine. If the insurgents are more successful interacting with people, then you will lose. I'm not a policymaker, and I'm not suggesting we need to get 19 year-olds from Nebraska sitting down with Pashtun white beards [village elders], I'm just relating my experiences.

Let me use another example from when I was in Kosovo. The Americans would follow standard operating procedures (SOP) that would not allow them to interact with the population, and go through a village in full body armor. The Italians on the other hand would drive by with a bottle of wine, stopping in the town, having lunch with the locals, and being much more integrated into the community. They [the Italians] heard rumors, found out about hotspots, because they had their finger on the pulse of the people in a way Americans following SOPs did not. I think these same things hold true for Afghanistan, that if you can shake hands and show less of a fighting face, then of course you'll be more effective.

***IO Sphere**: Speaking of confused cultures, what about our own? As a body of people trying to develop a common message, we have troubles. Is the US Government as a whole culturally hindered? As an advisor, how do you recommend we work better as a team?*

BGW: I think we do have a cultural hindrance. Only ten percent of Americans have passports! Of that ten percent, if you take out Canada and Mexico, you don't have a whole lot of folks traveling the world. If you take out Spanish, then we are a monolingual society. We believe, in a uniquely American way, that you can go into someone else's country without knowing the language, and reshape it. Only Americans have that sense of "pure optimism." To put the shoe on the other foot, it would be like a bunch of Scandinavians coming here and telling all our women to get out from under the oppression of the fathers, and their husbands… and doing it through the medium of Norwegian, in a place like Texas! It wouldn't work. We are so confident: we put man on the Moon, we discovered electricity, we can reshape a country. These types of optimism are our greatest strengths and greatest weaknesses. Because we don't have an imperial history like the British or the French do. We don't have universities like the School of Oriental and African Studies at the University of London, where for the last hundred years they have trained young mandarins to go out and run the empire. We don't have that imperial tradition, or one of embracing other languages and cultures, and in a place like Afghanistan, it shows… in both good and bad ways. We do believe we can dig the wells, and win the village elders over, and build the schools and win over the villages. That is something wonderful and unique about us. But the fact we have to rely on interpreters is also unique: and it's an Achilles' Heel for our operations in Afghanistan. So how do we address that fundamental an issue? Well, I think it begins with better training for people going into the zone, about the culture – providing "context." People going to fight or help in a zone like this need more context. It's hard to do, but knowing how to speak Pashtun or Dari can save lives. These things could really help us get our message across. And certainly could help us win the underlying battle – the real battle of hearts and minds.

***IO Sphere**: Some folks have pointed out that our soldiers' language guides have an emphasis on how to say "halt," rather than "please" and "thank you." Let's switch gears a bit. We hear a lot about suicide attacks, and you've done some of your research in this area. In an article you published in late 2007, you described how these bombers are resorting to new ways, I think you said they're being "duped, bribed, or brainwashed." Are they desperate, or just changing tactics?*

BGW: Yes, they're changing their tactics. But I wouldn't describe them as desperate, because theirs is a calculated action: they'll use what works. This goes back to Iraq, which showed extremists one thing: suicide bombing wreaks havoc when you have people trying to win hearts and minds. I think of the Canadian troops in Kandahar, who were distributing candy to village children after digging a well—very effective hearts and minds actions—a bomber walked right in between them and detonated himself. Canadian soldiers lost limbs, bled to death, children were slaughtered. With one bombing, those weeks or months of work ended. The Canadians become jittery; forces started putting loudspeakers on their trucks broadcasting "keep away from our convoy" messages. And young people don't hang around with troops anymore to get candy. So unfortunately it is a very effective technique they learned from Iraq. They adjust, they learn, they adapt. In the mid-1980s, they adapted to the air threat by using Stinger missiles against Soviet helicopters. This time they've learned, not from us, but from the Iraqi insurgents; they've seen that suicide bombing is the "Stinger missile" of this war. It is one of the most effective things in their arsenal, the ultimate asymmetric weapon. It makes US troops not do what they need to do, which is go in there and interact closely with these people. I hear the media, and military public affairs people saying the terrorist suicide bombers are becoming desperate, but I don't see it that way. I see it as clever asymmetric tactics, in some ways like a laser guided bomb or a JDAM [Joint Direct Attack Munition]… "Mullah Omar's Missiles" they call them.

***IO Sphere**: How do we approach this problem? Where do we spend our money to mitigate this threat?*

BGW: We have to go after it on many levels. You have to go on the offensive. Let's look at Chechnya: suicide bombing came and went there. It began in about 1999, and ended by about 2004, in part because the Russians were clever— they helped change the (local) religious culture. They sponsored moderate Sufi mullahs (priests) who loudly proclaimed that those who committed suicide went to Hell, even those who committed a so-called "martyrdom operation." That was heard loud and clear in the mountains of Chechnya, and needs to be done in the mountains of Afghanistan. Families of people whose sons commit a suicide attack should not be given grace, they should not be taught their sons are in Heaven, they should be taught this was the equivalent of murder. Suicide is a taboo for Muslims in the same way abortion is for Catholics, yet the paradigm has been warped by the extremists. So we need to go after the culture, use the mullahs to issue fatwahs [religious edicts], decreeing and bringing to light the verses of the Quran and in the Al-Hadith [Muslim sacred text]—the words of the Prophet Mohammed—that make this very clear. Suicide in any form, even in an offensive form of combat against infidels is in fact suicide and it is wrong. You also begin by highlighting the havoc these actions wreak on society. My studies have found the vast majority of victims of these suicide bombing are civilians. We need to go in there and photograph and distribute the carnage to the area where the bomber came from and say "this is your handwork! You call this jihad?" If the Afghans can use "Shabnamahs," the so-called "night letters" to threaten and intimidate, as well as get their word out, we need to issue some ourselves. We cannot let them have victory in this field. We need to highlight the carnage this tactic creates: it's killing women and children, it's not "macho," it's not a noble war, it's fodder that sends you to Hell. The other level of interaction is of course working more closely with local communities, getting out of your body armor, talking to people at home and at work to get information, get local tips… but we're constrained by our own SOPs on that one.

***IO Sphere**: Many would say that (approach) is exactly what helped with recent security gains in Iraq. What are your impressions so far in this Afghan seminar?*

BGW: I find something missing from the discussions: *the Afghan people.* I think that data such as polling numbers is incredibly useful and interesting. But it gives you two dimensions, not three. I think this whole exercise tells us something interesting about ourselves: we honestly believe that using polls, metrics, and charts, we can reshape our identity in this conflict. Or reshape our identity in the Afghan's eyes that is. I see the facts, and I compare them with my own experiences of months and months trudging the ground in Afghanistan, and I find them to be useful… but they don't provide the whole picture. If Al Qaeda wanted to understand us, they could do opinion polls! They could say this percentage of Americans favors the war, this percentage doesn't, so let's do this based upon Taliban polls! But does that really capture the granularity—to use a key term these days – the nuances of America any more than it does Afghanistan. Can it tell you the difference between a Cubano from Miami, a Yankee from Maine, or a Good 'Ol Boy from Texas? There are many different levels and nuances polls can't tell you: why the New York Yankees fans hate the Boston Red Sox fans. If you really want to understand Americans, you have to know that stuff. Conduct all the polls you want, you won't get all those colors and layers. We're doing surface analysis based on science. Don't get me wrong, these are based on good methods, but we're leaving out certain factors when building the stats and data harvesting. They are a good starting point, but there is a danger we will bureaucratize and metricize the Afghans, using otherwise useful tools, but we will take it too far. We won't include key aspects like geography, ethnicity, religion, and culture—these things that need to be woven into the data to give us the third dimension. The data is a good basis, but we shouldn't give it more clout than it deserves. I think it is brilliant that we are doing this, God know the Soviets could have done with this when they wreaked havoc in Afghanistan, but as this seminar and others show, unlike the Soviets we care, and want to know what Afghans are thinking. Collecting opinions is very beneficial, but this is only the beginning. I was in one of the "hearts and minds" conferences, and a guy came in and talked about how to sell Coca-Cola [to Muslims], and it was a very interesting talk. I recall sitting down with these Pashtuns, who were illiterate, living in the frontier region between Pakistan and Afghanistan, near Jalalibad—near Usama Bin Laden's old base—actually about five miles from Darunta, where he planned a lot of his attacks. And I'm remembering this guy's excellent [Coca-Cola] talk, his surety about marketing this product, yet looking at these nomad elders, eating rice with their hands, telling stories about Bin Laden. I'm thinking to myself, no amount of marketing expertise in Washington, DC about how to sell Coca-Cola is going to reach this guy with grease in his beard, who prays before, during and after each meal, and devoutly throughout the day. He doesn't read, he can't find his homeland on a map, because he's never seen one. You can almost write a novel about America's optimistic perceptions, based upon Hollywood marketing, and how someone like that would never fit the paradigm. The best conference would be to drop all the participants into that village for a month, then come back and regroup, and see how much of our thought process turned out to be superfluous. How much of our cool data is actually wheel spinning,? It doesn't have true reflections of illiteracy, xenophobia, blind fanaticism. There are ancient blood feuds, isolation, misogyny, and poverty… things I am only now beginning to understand from my experiences. I hope these factors will come more into play as we continue our discussions.

***IO Sphere**: Thank you for your time and insights.*

BGW: My pleasure, thanks for the invitation.

Dr. Brian Glyn Williams, formerly lecturer at the University of London, is currently tenured Associate Professor of Islamic History at the University of Massachusetts-Dartmouth. He is author of *The Crimean Tatars: The Diaspora Experience and the Forging of a Nation* (2001). He serves as a counter-terrorism analyst at the Washington DC-based think tank, the Jamestown Foundation, and has carried out work tracking suicide bombers in Afghanistan for the US Government. His field work ranges from Kosovo to Kashmir to Kazakhstan including three field trips to Afghanistan. His work there included interviewing Taliban prisoners of war, living with Northern Alliance warlords. Reader can contact him via http://brianglynwilliams.com

Blogging to Win Hearts and Minds

By Diane Vanderpot, Colonel, USA

Editorial Abstract: Colonel Vanderpot looks at the impact of military blogging, to include issues ranging from potential operations security and force protection vulnerabilities, to soldiers' personal enrichment needs. With proper blogging guidelines, plus common sense, she suggests blogs offer a potential information operations force multiplier.

http://blog.al.com/afghanistan/2007/10/security.html

31 October 2007

Security

Posted by Michael Tomberlin October 25, 2007 8:00 AM

It is a basic need for everyone, including us here at Camp Vulcan. Continuing our tour around the camp, next stop is the force protection measures. A lot of time and materials have been used providing us with fighting positions, bunkers and barriers that provide both physical protection and an emotional piece of mind. I will not go into detail for operational security reasons, but the ongoing expansion of Camp Vulcan has given us a number of dismounted fighting positions and mounted fighting positions where we can drive a Humvee up to the wall and use the crew-served weapon mounted in the turret to fight off the enemy. To protect us against mortars and rockets the enemy may use to shell us, we have concrete bunkers reinforced with sandbags. Dirt filled Hesco barriers surround our barracks, recreation building, TOCs, bathrooms and even our generators. The large Hesco barriers that surround Camp Vulcan are topped with rolls of concertina wire. We have multiple gates at our new entry control point to prevent anyone from driving or walking into the Camp Vulcan. All of this, and Camp Vulcan sits inside an Afghan National Army FOB, with its own barriers, guard towers and the like. Needless to say, we feel pretty safe inside the walls here. That's how we define "security" here at Camp Vulcan. It's funny, because this time last year, in my nice job and comfortable home, I would have described security differently.

"The view from one of our dismounted fighting positions at Camp Vulcan."

"Bunkers and barriers surround our barracks and bathrooms."

"Mounted fighting positions are designed to drive a Humvee into place."

The Blogger

MAJ Michael Tomberlin posted the security entry into his blog "Yellowhammering Afghanistan" on 25 October 2007. Does it give away critical force protection information like the distance between a Hasco barrier and living areas? Can the Taliban use any of this information to attack Camp Vulcan? This article examines Operations Security (OPSEC) and military blogs —which can be a double edged sword. It focuses on the positive aspects of blogs like getting a first hand account of what happened in a fight and winning over America's hearts and support. It also discusses some negative aspects, like providing classified information, divulging current tactics or embarrassing the US military.

Blogs are an outlet for people to post journal entries. Deployed soldiers writing blogs must fully comprehend the potential audience of their words and pictures before hitting the send button. MAJ Tomberlin's entry may appear interesting, and provide insight to the quality of life at Camp Vulcan to his intended readers, most probably family and friends. But a foe may be able to find these pictures and descriptions, use them to build a diagram of Camp Vulcan, and discover vulnerabilities in force protection.

Why Soldiers Blog

Military blogs are the soldier's most modern way to communicate. Soldiers deployed to war have always sent letters home describing their living conditions, the actions they have participated in, the lousy food, their emotions as they watch fellow warriors die, and how much they miss home. Today's soldiers are no different, the tools they have to communicate with friends and family allow almost instantaneous information to flow. The Internet makes communicating easier, it's faster to type and change mistakes than writing letters, and email is weeks quicker than the postal system.

Concurrently with the beginning of war in Iraq, blogging became a popular way of expressing one's feelings about any subject. Young soldiers, who always seem to be on the cutting edge of technology, found it easy to communicate outside the bounds of their camps by typing blogs. Blogging gives them an opportunity to communicate their experiences to outsiders, and provide more detail and a counter perspective to the media. They see what the main media networks present to viewers back home, and realize the stories are packaged based on the network's bias and on what will attract viewers.

Soldiers want the American public to know the real story. Corporal Michael Bautista, a machine-gunner based in Kirkuk said it this way: "It kind of transformed itself from a desire to convey my personal experience into letting people know the real story. I think the main coverage that you'll see at home is this car bomb blew up; this amount of people died. I think my main effort now is more toward showing that this is a good thing that we've done, regardless of… what political decisions were made to get us here. This is a just cause, and that it is— it's a righteous endeavor. That's part of why I write. If I'm given an opportunity to say it, by God, I will. We have done a good thing."

Milbloggers want to share their experiences as lessons learned and advice to other soldiers. The Army maintains official websites for lessons learned, requiring units to provide after action comments to be incorporated for future use in developing tactics, techniques and procedures. Young soldiers, however, are more interested in the 'down and dirty' from like peers. Their peers will give the low down to soldiers preparing for deployment on what they can expect.

Less than one percent of the American population serves in the military today and blogs help amplify the military message of trust, camaraderie and valor to a nation with no combat experience. The on-the-scene perspective written by the amateur journalist/soldier whose words are candid and sometimes colorful seem more credible than the official pronouncement from either Baghdad or the Pentagon. Journalist Ralph Peters notes "The best blogs offer a taste of reality of Iraq or Afghanistan that the new media rarely capture. And they're often a grand, irreverent hoot."

Stories from soldiers's blogs have mesmerized America with first person accounts of heartfelt agony, sorrow, pride and strength. Blogs make the war more real. Brown University held a conference entitled, "Front Line, First Person: Iraq War during October 2007." The conference brought together soldiers, journalists, and academics to try to understand ground-level experiences in Iraq and why so few of these stories get out to the American public. Many of the speakers concluded that first person accounts are the most honest, but may not be fully appreciated by a public who has no basis of comprehension. However, the more informed public may have more support and trust in their military.

Who Reads Blogs?

According to *Technorati*, a tracking engine for Internet sites, in October 2007 there were 109.7 million total active blogs, and of those 3835 were active military blogs. Blogs are updated regularly, with approximately 1.6 million entries added daily. Milblogging.com currently indexes 1,839 military blogs in 32 countries with 4,040 registered members. Milblogging.com puts finding frontline stories at your fingertips, highlighting the best military sites and listing the 'top 100' blogs.

These types of sites alert other bloggers to false stories, and help quickly discount them. The blogger community, or blogosphere, is to a large degree self-policing. Milblogs are frequently linked to other milblogs and members frequently comment on each others' stories. It is natural to check out what others who have commonality are writing. This readership helps police those who tend to embellish their war stories.

Sometimes, the soldier gets caught up in his desires to become famous. This is the case for Private Scott Beauchamp who was writing blogs for the New Republic's "Baghdad Diarist." Under a pseudonym, Private Beauchamp wrote stories "telling of outrageous behavior by US troops belittling a woman scarred by an IED, wearing a skull fragment from the remains of a child found in one of Saddam's mass graves, and intentionally trying to kill dogs with armored vehicles." Michael Goldfarb, editor of the *Worldwide Standard*, thought the stories were fishy. He recruited the greater blogosphere to determine the reliability of Beauchamp's claims. Within days he received ten responses from military personnel who were disgusted by these claims, and gave solid explanations why they were lies. The US Army completed an investigation of Private Beauchamp, and found all his allegations to be false. The investigating officer stated Beauchamp took small bits of truth, twisted and exaggerated them into fictional accounts, then put them forth as 'the whole truth' for public consumption.

Interestingly, this story did not hurt the military. Readers quickly saw through the fabrication and questioned the author and asked for verification. Unfortunately the *New Republic* believed. Even with others questioning the story's validity, the editors did not investigate these allegations, and stood by their story. The *New Republic* currently has no record of Beauchamp's stories posted on their website.

Safeguarding Information on Military Blogs

Army policy now requires Soldiers to inform their chain of command of their milblogs. In August 2005, Army Chief of Staff General Peter Schoomaker sent guidance to the field requiring that Army leaders make their subordinates aware of how enemies exploits sensitive information and images on the Web. Downloaded photos of M-1 Abrams tanks penetrated by an RPG [rocketpropelled grenade] can easily become training and recruitment tools for the enemy. For the most part soldiers abided the directive, and closed down their blogs. CPL Bautista said he received tacit approval from his platoon leader who reviewed what Bautista wrote. The corporal understood as long as he did not comment on Army policy, politics or issues that may have operational security risks, he could write what he wanted.

Sergeant Major of the Army Kenneth Preston addresses this issue on his website. He states that Al Qaeda proclaims they derive 80 percent of the information in their terrorist handbooks from open sources, and soldiers writing sensitive information on blogs are helping Al Qaeda kill fellow soldiers.

According to MAJ Elizabeth Robbins, a public affairs officer for Multi-National Force-Iraq, the Army cannot effectively mandate that its personnel refrain from all public communications. To do so the Army would have to stop all communication means to soldiers' family and friends. MAJ Robbins points out that private soldiers' communications to family members, who subsequently make inadvertent or intentional public statements, are the primary source of leaked sensitive information.

The Army recently revised Regulation AR-530-1, *Operations Security*. It states all personnel must prevent disclosure of critical and sensitive information in any public domain to include, but not limited to, the World Wide Web. It details examples of what is considered sensitive: improved explosive device strikes; battle scenes; casualties; destroyed or damaged equipment; personnel killed in action, both friendly and adversary; and the protective measures of military facilities. The regulation also directs commanders to properly implement OPSEC procedures, and ensure appropriate controls on information posted to the Internet.

Further, Multinational Corps–Iraq established a policy specifically directed at military members posting blogs. It lists five types of prohibited information: classified information, casualty information before next-of-kin notification, information protected by the Privacy Act, information regarding incidents under ongoing investigation and For Official Use Only information. Soldiers serving in MNC-I must also register their websites with their respective chains of command.

All these directives are difficult to sort through. Many soldiers have chosen to close their blogs in order not to violate policy. One deployed military blogger, who elected to stop blogging rather than face the scrutiny of command, wrote "Operational security continues to be an issue for our Armed Forces. Therefore, it is with heavy heart that I must back away from the blogging community… I pray that I have been able to shed some light on the everyday events that our men and women overseas deal with… into their struggles and triumphs… What I do, I do willingly out of respect for our leaders and love for our Soldiers."

Way Ahead For Milbloggers

Military blogs pose challenges to operational security, but they have also provided incredibly positive information. The official military information campaign struggles with how it tells the American public what is happening in the war. The media tells the angle they want to portray, but deployed military bloggers tell first person stories from the heart. Support and popularity of their following is cult-like.

Gary Trudeau, the creator of *Doonesbury,* has collaborated with several military bloggers to create a book, *In The Sandbox*. This book is a compilation of blog entries from service members deployed to Afghanistan and Iraq. Trudeau notes the military called it "[a] hotwash," and "it's the kind of first-person journalism that you really can't find anyplace else."

This kind of marketing makes more people aware of military blog sites, and helps sell a positive image of the military. It is using information operations to win the hearts and minds at home.

When soldiers are told the importance of observing operational security in terms of protecting themselves and their buddies, they understand and usually comply. The boundaries and rules for military blogging are new, yet military bloggers tend to police themselves and demand truth in writing. They can exert pressure on non-compliers. Commanders and supervisors have responsibilities to conduct OPSEC training for Internet forums, and to ensure such guidance is understood and occasionally checked.

Most importantly, the rewards of well written, accurate portrayals of daily life in the combat zone will be a force multiplier to information operations.

Bibliography/references for this article are on the IO Sphere Home Page at: https://www/jiowc.osis.gov/Publications/IOSphere/index.cfm Click on the "updates" link under the Spring 2008 issue.

COL Diane Vanderpot, US Army, is currently attending the Naval War College, Newport, RI. Her previous assignment was as the Chief of Operations, G2, Headquarters US Army Europe in Heidelberg, Germany. After completing the War College in 2008, she will be assigned to Multi-National Forces-Iraq. Readers can contact her at diane.vanderpot@us.army.mil.

Irregular Warfare IO: Understanding the Role of People, Capabilities and Effects

By Norman E. Emery, Lieutenant Colonel, USA

Editorial Abstract: The author characterizes current information operations campaigns in Southwest Asia in the context of irregular warfare, a type encompassing insurgency, counter-insurgency, terrorism and counter-terrorism elements. He recommends models for enhanced effects-based planning, and evaluation of results.

[Editor's note: This essay is a Combined Arms Center US Army Information Operations Proponent Writing Contest Award winner.]

The current conflicts comprising Operations Iraqi Freedom (OIF) and Enduring Freedom (OEF) do not truly qualify as specifically conventional or unconventional warfare, but lie somewhere in between on the warfare spectrum. Conventional US military units in Iraq and Afghanistan find themselves enveloped in an operations model more special than conventional. Labeled as *Irregular Warfare* (IW), for many senior and mid-grade officers and non-commissioned officers this concept has little resemblance to those they learned from doctrine and training center rotations.   Once in theater, US military members of various ranks and services are required to engage with unfamiliar skills in political, economic and social networking to complement military operations. Not to be overlooked is the complexity of the various enemies we face: a nexus of terrorism, insurgency, criminality and negative transnational factors that comprise a collective threat—unbounded by our militaries' same ethics or rules.   Most critical is our awareness that all actors, state and non-state, are competing for the same objective: the people.

We need to understand how this requires a change in application of Information Operations (IO) that is markedly different from that used in traditional, or conventional, warfare. In IW, various non-lethal capabilities have a more prominent and necessary role than in conventional warfare. Significantly, IO directly impacts the operational focus of IW—the people that comprise the relevant populations. Current Joint and Army IO doctrine does not adequately address the challenges US forces confront during long-term stability operations, in the face of irregular adversaries and asymmetric conflict. Doctrinal emphasis remains entrenched, focusing on the adversary decision-maker while minimizing the importance of projecting public information and engagements to key non-adversarial audiences, especially foreign populations. These critical tasks require greater expertise, and an understanding of the IW Information Environment (IE). To succeed in IW, IO officers need to understand how IW compares to conventional and counter-insurgency (COIN) warfare, the importance the population plays, how various adversaries project their information, plus the need for proficiency in cultural and human behavior studies. IO planning must consider not only actions to support the tactical operation, but the hierarchy of effects within the Information Environment that impacts a unit's areas of operations and influence.

To accomplish this we must examine the role and education of IO officers, and propose needed operations and current IO doctrine, so we do not continue to prepare soldiers to fight today's war with yesterday's tactics, techniques and procedures. An examination of IW IO must not simply impart vignettes, lessons learned and opinions; it must consider what makes IO a challenge in the current combat zones and how those factors necessitate conceptual IO adaptations. Indisputably, the current complex war environment requires this change.

Irregular Warfare and Relevant Populations

The US Department of Defense (DOD) developed an *Irregular Warfare Joint Operating Concept* (JOC) to define key elements and strategies for current and future conflicts on the spectrum between conventional and unconventional warfare. The JOC defines IW as "a violent struggle among state and non-state actors for legitimacy and influence over the relevant population." Irregular Warfare is a form of armed conflict, as well as a form of warfare encompassing insurgency, counter-insurgency, terrorism and counter-terrorism. COIN, a spectrum of actions taken by a government to defeat insurgencies, is an IW component. Therefore the majority of COIN principles and models also apply to Irregular Warfare. IW is a different—but not a lesser—form of conflict than conventional warfare. While conventional warfare is direct military confrontation between states, Irregular Warfare focuses on control and influence of populations, rather than of an adversary's forces or territory. The dichotomy is balancing operations against the enemy with those to influence the population. Neither can be ignored, nor can both be addressed equally. The IW challenge is that the adversary is not a single, easily characterized entity. In Iraq and Afghanistan, the insurgencies are not united monoliths; the "enemy" is comprised of nationalists, protectionists, extremists, rejectionists, criminals and terrorists. Separation of the populace from the insurgents is a basic objective of a COIN strategy. However, in IW separation of the terrorists from the insurgents is clearly another matter. For simplicity in this discussion, the term Anti-government Forces (AGF) refers collectively to all groups engaged in armed conflict against either Coalition Forces or a state's legitimate security forces, or both, regardless of motivation. While no single term can properly categorize disaggregated groups that share common goals but competing objectives, this does make the collective groups vulnerable to effective information operations: we can drive a wedge between these tenuous and convenient partnerships.

The Human Terrain

Just as IW has no monolithic enemy, neither are there a single people who comprise the desired and relevant population. Lieutenant General Peter Chiarelli demonstrated an understanding of this when he command the US 1st Cavalry Division, responsible for the security of Baghdad, in 2004. He emphasized the need for full-spectrum operations (well-coordinated combat, stability and information operations) to effectively create a stable and secure environment in the Baghdad suburb of Sadr City. Key to ensuring focused efforts was not only understanding daily competition for the population among various Anti-government Forces, but also understanding and approaching the population as three distinct constituencies (Figure 1): opposed, unopposed, and undecided. Understanding these groups and their cultures can better determine both the type of operations conducted (lethal combat or non-lethal support), and messages delivered. Opposed audiences, comprising active AGF members or supporters of the various "enemy" groups, are therefore opposed to the state or ruling authority. The unopposed simply support the government. While it is difficult for opposing sides to dislodge their respective audiences, the true battleground lies within the remaining fertile constituency: the undecided, or "fence sitters." The undecided range from the poor to the professional, and are generally waiting out progress and security concerns to determine who will gain their support; the victor will be the one who gets them 'off the fence.' It becomes a zero sum game for the state. The military and AGF compete for the bulk of the population that has yet to commit, and can be swayed with the promise of hope or the threat of violence. It is necessary for the US military to accept that instead of winning over this population segment, victory may just be 'not losing it to the enemy.' A mantra the US military often uses to describe its efforts to maintain the unopposed and sway the fence sitters is "winning hearts and minds." Too often we interpret a 'hearts and minds' campaign as having the population *like* us, but really it is understanding the requirement to reach a population through emotive and cognitive means. It is more than noble efforts to build infrastructure, hold elections and create jobs; we must leverage existing social and political networks, and build support within them, to separate the insurgency from the population.

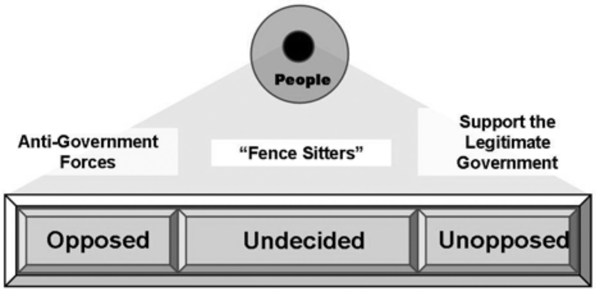


Figure 1. The Three Population Constituencies in Irregular Warfare

IW Conflict Model

Several conflict theory models address the population's role in warfare, the most well known being Prussian strategist Carl von Clausewitz's warfare trinity: military, government, and people. According to Clausewitz, military operations focus on an opposing state's armed forces as a means to control the government, theorizing that populations will follow their government's lead and accept the political outcome. An example would be Japan's surrender in World War II. The only military objective involving the population was minimizing civilian interference with operations. The Trinitarian conflict model, a variation of the Clausewitz trinity and a principle of COIN theory, portrays non-state actors pursuing the Clausewitz paradigm in reverse order. One confronts the people first, in order to influence the government and avoid direct confrontation with the military. The non-state actor has a greater chance of defeating the government if it gains control or majority support of the population; if the government falls or compromises, that negates the non-state actor's need to attempt a decisive military engagement. Figure 2 depicts the Clausewitz trinity adapted for IW, and centrally portrays the *critical and common element* to both the state's and insurgents' success: the people. This model, developed by a retired Special Forces officer with significant COIN experience, portrays how the state covets the population and it's military to remain supportive of the legitimate government. The mirrored model illustrates the military and insurgent preferred approaches to engaging and winning the population, rather than pursue exclusive armed engagements. In a basic COIN model, the US provides limited assistance, such as the current support in the Philippines. The revised IW model depicts direct US involvement with a cooperative state, the population and the insurgents—representing current operations in Iraq and Afghanistan. Essentially, because IW is a social-political crisis, this type of warfare requires more than a pure military solution. The political and psychological aspects of IW are just as important as the physical actions. With people as the center of focus, information operations play a very significant role.

IO Challenges in IW

"Irregular warfare is about people, not platforms."

The key military objective in IW—people comprising the general relevant population—is also important for IO. They comprise the target audiences we want to engage, inform and influence. How an audience reacts (directly and indirectly) to messages impacts how and when the US ultimately achieves its campaign objectives. It is important not only to understand our primary audience, but also how easy it is lose focus by pursuing tomorrow's headline, —or reacting to yesterday's—instead of sticking to a uniform, long term strategy.

We should seek to shape the information environment (IE) for long-term success, and not be bogged down in point/counterpoint with various adversaries vying for notoriety. Public Affairs can counter specific adversary actions, but IO collectively should counter adversary strategies. In order to achieve their goals, commanders and IO officers must understand their environment. The IE is part of the operating environment, grounded in the physical domain, and comprised of three dimensions: physical, informational, and cognitive. All communication systems, including human information networks, reside in the physical dimension. The informational dimension "consists of the content and flow of information." The cognitive dimension is the most important; in this realm the decision makers and target audiences think, perceive, visualize, and decide. Simply put, if you are at a computer terminal, the computer is the physical dimension; the informational dimension is the data flowing through the computer; and your viewing and processing of that data is the cognitive dimension.

Know your Audience

A shortcoming of current IO doctrine is its primary focus upon influencing critical adversarial decision makers. This approach neglects a key target of Irregular Warfare: the relevant population not categorized as adversarial. The DOD *IO Roadmap*, produced seven months after the invasion of Iraq and 25 months after entering Afghanistan, asserts that IO "must be refocused on adversary decision-making." It fails to acknowledge a necessity, let alone a role for IO, in building relationships with civilian populations and effectively communicating the US military message as means of achieving tactical and operational objectives. However, we can fall in the trap of simply directing information towards populations as a whole, rather than attempting to evoke a specific cause and effect response amongst specific constituencies. This strategy is a critical concept which operations and Irregular Warfare doctrine should both address and explain. By failing to understand the various audiences, we pursue or react to information or incidents with actions which seek to blanket all the audiences, making it costly and ineffective. A common mistake in IW is to develop and disseminate a one solution/message-for-all approach. It is inefficient to expend resources trying to convince the audience already committed to us, therefore we should avoid blanket messaging and instead make "maintenance" or reinforcement efforts using minimal resources to the unopposed audiences. This puts our full effort toward the undecided audience. US politicians employ this same strategy during national elections. Thus within one theme/message/information goal, there could be three variations targeting adversary decision makers, as well as the three constituencies and their key non-adversarial leaders of influence, such as tribal leaders, imams, civic and political leaders.

We cannot persuade every possible audience or adversary to reconcile, and therefore combat operations are required to destroy these groups. IO planners must consider not only actions to support the tactical operation, but the hierarchy of effects within the IE that impact a unit's operational area. A commander engaging physical, informational, and cognitive dimensions at the tactical level can gain exposure at national, regional, and international levels. Impact in the cognitive dimension can have direct or indirect, positive or negative, effects on *all* commanders in theater. This is already quite accepted—a condition resulting from continuous IW operations in recent years. Joint doctrine dictates that during conflict the US military achieves and maintains information superiority (IS), at key points in time and space. IS defined as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." It is important to understand that despite its superior technology, the military will rarely, if ever, gain information supremacy in IW—and information superiority is fleeting. We cannot prevent an adversary from putting out a message or information. What we can and should do, is set conditions for the key audiences (unopposed, opposed, undecided), so even when opposing messages come out, they do not effectively *resonate*.

Our adversaries' information goal is to be first, which is rewarded in a rumor-centric society. First out is not necessarily a victory, nor second out is necessarily a loss. Our goal needs to be first with the truth. Sometimes the enemy gets the word out first word, but we can render it irrelevant by staying on message, consistently iterating and repeating mutually supporting themes. Our adversary has not necessarily gained success just by delivering his message, nor has he dealt us a defeat, just as US message delivery is not in itself a success. The issue is how the message resonates with target audiences. A global information environment where most people believe the first story out creates the temptation to respond with a strategy of short engagement actions, instead of adhering to the enduring conditioning actions. We should not view IW IO efforts as short-term, especially when most insurgencies historically last 9-12 years.

There are no well-codified rules in IW, but in competing for the population, terrorist and insurgency groups must also abide by the rule of understanding their audience. The descent

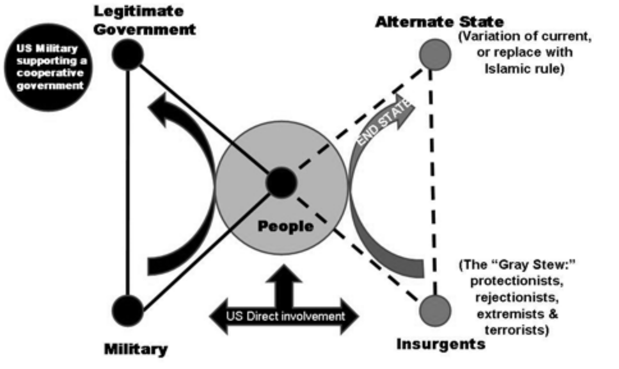

Legitimate Government
US Military supporting a cooperative government
Alternate State
(Variation of current, or replace with Islamic rule)
END STATE
People
(The "Gray Stew:" protectionists, rejectionists, extremists & terrorists)
US Direct involvement
Military
Insurgents

Figure 2. Clausewitz's "trinity" (Military, Government, People) adapted for IW with US Military Direct Involvement

into barbarity (in this case beheadings, deadly bombings) by such groups as Al Qaeda in Iraq achieve not a persuasive effect against the fence sitters, but instead a possible loss of support from its own constituency. Competing adversaries within a state (such as in Iraq, home to numerous Sunni insurgents, ranging from moderate to extremists) can also lose audiences as populations as a whole are being presented with various and conflicting messages. This is to our advantage and it is critical to develop and reinforce consistent themes and messages over time in coordination with Iraqi and Afghani governments.

Good News Stories and US Popular Support

Since information is central to our ability to shape battlefields, unity of effort and purpose is vital. While there must also be unity of information for indigenous and global audiences, if we concentrate on winning the local audience first, the US/global audiences will follow. IO and PA officers (PAO) at the operational level face a dilemma when encountering military leaders who believe there is a need to push "good news" stories, to counter the perception that only tragedy, hardship, and failures occur in combat zones. This tactic is clearly aimed at US audiences, as Iraqis are concerned with proof and perception of physical security, not stories of school openings. Unfortunately, the 'good news story' becomes a misguided sprint strategy, as perhaps some military leaders believe they have a responsibility to balance, if not counter, the output of news outlets in order to maintain US domestic support. Any service member knows of positive successes, operations and experiences, though relating such stories can be a challenge, even from supportive media. In 2006 Journalist Lara Logan wrote of her frustration in getting relevant data from a general officer who wanted to share a good news story. She tried to get the "good news" facts, but the officer could only relate statements asserting that security is "better," "great progress" is being made, 100,000 cubic meters of trash have been removed from neighborhoods, and operations were implemented toward the goal of improving electricity availability for 3,000 homes. To be fair, any leader attempting to portray *national level* progress with *tactical level* empirical results would understandably receive a tepid response. Progress is sometimes the sum of achievements and atmospherics that are difficult to articulate. Nevertheless, this is an IE nuance 'sensed' by those operating in the combat environment. In preparation for discussing success, our leaders must recognize that a single achievement can seem insignificant when offered out of the context of overall progress, or when it is buried amidst the reporting of turmoil. As the military relies more and more on commanders to convey progress, PAOs are doing far fewer visual and print interviews than might be expected. This shift in communication requires these spokesperson leaders understand the trap of relaying empirical tactical progress to US audiences who do not view the conflicts as city sectors, and to better articulate progress without it sounding hollow. One method is to relate success that has or will occur over time with subjective and empirical metrics. An example is "a new power plant opening in town X will provide reliable electricity to several hundred homes, create 70 new jobs in a region where men have resorted to participating in insurgent activity to provide for their families. This will likely result in a vastly improved security situation in the coming months, and is a model of progress that is proving successful in this region."

The Enemy has No Rules

Non-state actors reign supreme in the Information Environment. Information is the commodity with which they purchases cooperation, survivability, perceptions of victories, and silence amongst supporters. The terrorist and insurgent do not have an IO doctrine—a Western term. Extremists use three broad methods in their information effects strategy: **Projection** of its message to various target audiences; **Protection** of vital information to enhance survivability and decision making; and **Collection** of information on its enemies. Our adversaries have a strong understanding of how to leverage the IE, and the US military should not abdicate that battlespace in pursuit of perpetual raids and kill/capture operations. Because the AGF does not have military parity with the US, it seeks successes not on the streets but in the information environment. Here the AGF have the advantage of being unbounded by the rules and ethics of responsibly releasing truthful information. The enemy has no rules. They can exaggerate claims, sensationalize events, omit facts, purposely mislead, and release information quickly without extensive staffing. In decades past, all sides used traditional media to reach their audiences, but now largely depend on the asymmetric and ubiquitous Internet realm, where "the keyboard equals the Kalashnikov." In the IW environment, the gap between the US and its adversaries' various media/ Internet means capabilities is much smaller than the gap between their respective military force capabilities. Islamic terrorist and insurgent groups whom we once considered ignorant and primitive are making effective use of cyberspace as a messaging and communication medium. The concern is not just command and control via the Internet—expected

Human Terrain Team in action. (US Army) in the 21st century—but the proliferation of messaging and propaganda directly connected to AGF engagements in Iraq and Afghanistan, especially as it relates to causing or exploiting US and Coalition casualties. Groups boosting video output include those affiliated in Iraq's predominately Sunni Arab insurgency, as well as the Taliban, who ironically opposed cameras when they ruled Afghanistan. Inevitably, other extremists groups will soon adopt this practice. Libyan firebrand Abu Laith al-Libi recently urged Islamic insurgents in Somalia, who have mostly ignored the medium, to begin using video to promote awareness of their cause. Information Operations not only project our messages, but seek to deny and degrade adversarial messages, as well as enemy Internet access and effectiveness. Countering these videos is of urgent importance, because research shows "Internet chat rooms and forums are replacing mosques as venues for recruitment and radicalization." This course of action requires both ability and willingness to directly and indirectly engage adversarial Internet operations.

Leveraging the Information Engagement Capabilities in IW

IO is a key COIN logical line of operation, if we want to win the war of ideas, destroying the will and legitimacy of the insurgency. It has the same if not greater relevance in IW. The solution to IO challenges in IW is to have close, if not centrally coordinated, efforts and actions amongst public engagement-related IO capabilities. It is critical that we set aside current doctrinal construct of IO core, related and supporting capabilities, because this creates false barriers to planning, coordinating, and executing IO in Irregular Warfare. These core capabilities have a logical but not natural grouping, and constrain leaders' views of IO by portraying it simply as these five core capabilities. While an important guide, we should view doctrine as a point of departure in the constantly evolving Irregular Warfare environment. IO is not simply a grouping of capabilities that comprise information, but should be viewed as *a grouping of capabilities that affect information.* More importantly, IO collectively has a specific purpose and emphasis within an overall plan of action. It operates under the same dynamics, and is inseparably linked with kinetic combat operations. IO is more than just PA and PSYOP releases following a mission. Tactical commanders in Iraq and Afghanistan have had success with public information engagement as a main effort. Public information engagement should consist of coordinated and combined efforts of Public Affairs (PA), PSYOP, Civil Affairs (CA), Combat Camera (COMCAM), and face-to-face (F2F) engagement. These capabilities are critical, because IW requires a de-emphasis on information technology.

Holding Your Enemy Close: Making PA, PSYOP and IO Work

In IW, unity of the information effort is vital. The two key specialties of PSYOP and PA—the latter a doctrinally related capability—are mutually supportive in today's combat environment. They are also the most divisive in terms of coordination and execution with respect to one another. Many who work in Public Affairs have the misconception that PSYOP, and by extension IO, is nonfactual or even subterfuge. Leaders can dilute IO's value by thinking it is the semantic equivalent of PA or PSYOP augmenting combat operations. It is certainly not heresy to group PA and PSYOP into a coordinated public information construct—both use similar means (relaying a truthful message to specific audiences) to achieve different objectives (inform versus influence). A coordinated effort maximizes message effectiveness.

It is essential for Brigade or Regimental Combat Teams to develop the capability to influence and inform key target audiences at the local level. One brigade commander chronicled that his main targets were Iraqi and Arab media, because these informed the population in his area of operations. This should be done through local media or F2F means, because a national release by a theater PAO is insufficient to reach the fence-sitters and the uncommitted. In many ways PA is underused in IW foreign media operations, especially in reaching a tactical target audience population. PA in support of IW should be more than just informing the US public. The Joint definition of Information Operations, the integrated employment of capabilities "to influence, disrupt, corrupt, or usurp adversarial human and automated while protecting our own," limits public affairs application in IW. The definition does not address non-adversarial populations, and does not include "inform," thereby hindering necessary PA involvement (in coordination with IO) in reaching specific foreign audiences. Commanders cannot succeed without using PA and PSYOP capabilities as one voice, to disseminate messages, engage tactical audiences, foreign media, and foreign populations, plus coordinate counterpropaganda efforts. This is not so much an issue of public communication as a matter of foreign communication. PA (inform, unclassified) and PSYOP (influence, classified) have a convergent relationship with respect to foreign media operations; PSYOP can extend the message's momentum as the public affairs-driven news cycle winds down. An uncoordinated foreign audience engagement with one capability greatly increases the likelihood PSYOP encroachment into PA's lane. It is a bit ironic, but for PA to actually protect its contribution to the mission, it must work closely with PSYOP and IO planners.

Further, PA and PSYOP should cooperate in influence operations because the military has too few trained communicators to adequately deal with the overwhelming information demands of Irregular Warfare. The PAO is an invaluable information battlespace advisor to the commander, and naturally understands the information environment as a whole. If the PAO excuses himself from a process in which he is invited and encouraged to participate, then his best advice will be on information decisions made without his involvement. If PA is committed to a command's success, it will be part of the staff information operations planning process.

Few people think of COMCAM and F2F engagement as IO, but these fall within practiced information engagement capabilities. This reinforces that IO is an element of operations, and not simply a grouping of capabilities that various staffs "own." F2F engagement is relevant and valuable at the tactical and operational/theater levels, as an information delivery platform to achieve inform, influence, or co-opt effects. F2F engagement is a technique to engage key influential leaders (municipal, national, civic, and tribal) both prior to and post operations. F2F implementation by a commander instead of the IO officer does not negate it as an IO function. IO strives to achieve specific results in the information and cognitive domains; the executing platforms simply vary to those most appropriate. COMCAM supports IO by documenting events and operations, not only for success exploitation, but for mitigation. Their records can also counter post-mission misperceptions and accusations. While commonly comprised of Air Force personnel, many may be surprised the Army also has COMCAM capability and personnel. We should not only view F2F engagement and COMCAM as valuable parts of a strategy to integrate key public information elements, but as tools to achieve cognitive effects.

The final capability that plays a significant role in IW IO is the Civil Affairs-coordinated Civil Military Operations (CMO). CA is an IO-related capability with a valuable role in achieving tactical cognitive effects. Information Operations' role is more than just the synchronization of PSYOP activities with CMO. CMO can affect social-political change in communities and regions through infrastructure work and social services, which has an important effect on the populations' cognitive disposition. Though some may state "CMO is not IO," such a declaration fails to duly recognize a commander's important influence tool for achieving information and cognitive objectives. While CA may view itself as altruistic, its function is to assist the commander in affecting operational and informational environments. Philanthropy is for non-governmental organizations (NGO).

It is a fact PA, CA, and PSYOP personnel are effective in executing their respective functions in support of commander's guidance—in spite of an IO officer's presence. Centrally coordinated IO in IW does not necessarily subjugate or invalidate those fields, or erode their status with the commander: a PA officer can always say "no" to any IO officer's recommendation. Centrally coordinated IO in IW offers a method to eradicate seams between these respective areas, and other capabilities. Ideally, the IO officer is in a position to have full visibility of timing and effects within the area of operations, making him best-suited to coordinate and synchronize capabilities such as PA, CA, PSYOP, F2F, and COMCAM. Examples might suggest the timing or development of a PSYOP or PA product, recommend CMO in support of non-lethal objectives to persuade non-military (tribal, religious, government) leaders, recommend COMCAM document certain operations, or suggest conducting F2F engagements prior to an operation. Such suggestions or recommendations, provided to a commander or chief of staff, would help diminish the seams between these contributing functions, and achieve a greater effect. Without a doubt, one of the IO officer's greatest IW contributions can be in eliminating those seams, and maximizing overall effectiveness.

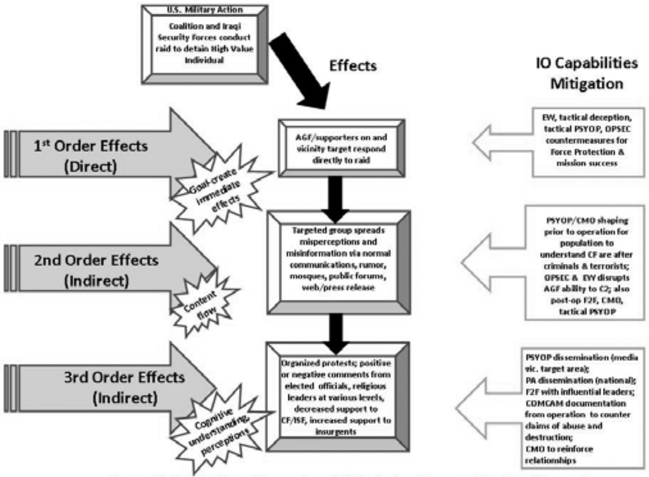

U.S. Military Action
Coalition and Iraqi Security Forces conduct raid to detain High Value Individual
Effects
IO Capabilities Mitigation
1st Order Effects (Direct)
Goal-create immediate effects
AGF/supporters on and vicinity target respond directly to raid
EW, tactical deception, tactical PSYOP, OPSEC countermeasures for Force Protection & mission success
2nd Order Effects (Indirect)
Content flow
Targeted group spreads misperceptions and misinformation via normal communications, rumor, mosques, public forums, web/press release
PSYOP/CMO shaping prior to operation for population to understand CF are after criminals & terrorists; OPSEC & EW disrupts AGF ability to C2; also post-op F2F, CMO, tactical PSYOP
3rd Order Effects (Indirect)
Cognitive understanding perceptions
Organized protests; positive or negative comments from elected officials, religious leaders at various levels, decreased support to CF/ISF, increased support to insurgents
PSYOP dissemination (media vic. target area); PA dissemination (national); F2F with influential leaders; COMCAM documentation from operation to counter claims of abuse and destruction; CMO to reinforce relationships

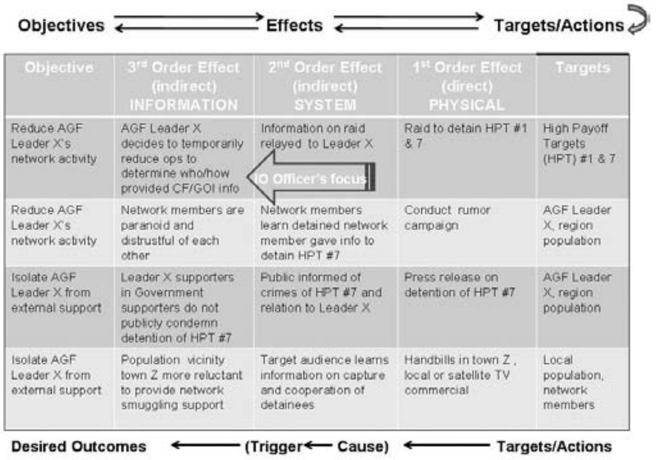
Figure 3. Evaluating Hierarchy of Effects for Planned Tactical Operation

Understanding Effects in IW

Measures of Effectiveness (MOE) are difficult to design and judge in a COIN campaign, because insurgencies are political and asymmetric. This is also applicable to Irregular Warfare due to population diversity, "invisible" enemies, added dimensions of time and space, and difficulty in observing, measuring—or even knowing—if our actions are successful. In IW, this is not a simple cause-effect observation with immediate or timely feedback; we require subjective and abstract metrics. Applying empirical data to measure subjective effects has a role, but is often awkwardly applied, with the resulting information of little significance or value if we do not properly define 'success.' Proposed solutions must recognize the differences between measuring effectiveness and measuring success, which do not always equate. Empirical data is best used to measuring success of tasks over time, or for trend analysis.

The Hierarchy of Effects

It is paramount that IO planners understand 1st, 2nd, and 3rd order effects, and apply this information to tactical IW planning. IO officers can expertly advise the commander, assessing IE risk to daily combat operations by addressing each order of effect, then the resulting collateral effects—those resulting positive or negative outcomes other than what we intended. There are three commonly measured effects: 1st order effects are associated with the physical dimension of the Information Environment, while 2nd and 3rd order effects are associated with the information and cognitive dimensions. There are few clear lines of demarcation beyond 3rd order effects. A 1st order effect is a direct effect, a result of actions with no intervening effect or mechanism between act and outcome, and can trigger additional outcomes (indirect, 2nd


Objectives
Effects
Targets/Actions
IO Officer's focus
Desired Outcomes
(Trigger
Cause)
Targets/Actions

Objective	3rd Order Effect (indirect) INFORMATION	2nd Order Effect (indirect) SYSTEM	1st Order Effect (direct) PHYSICAL	Targets
Reduce AGF Leader X's network activity	AGF Leader X decides to temporarily reduce ops to determine who/how provided CF/GOI info	Information on raid relayed to Leader X	Raid to detain HPT #1 & 7	High Payoff Targets (HPT) #1 & 7
Reduce AGF Leader X's network activity	Network members are paranoid and distrustful of each other	Network members learn detained network member gave info to detain HPT #7	Conduct rumor campaign	AGF Leader X, region population
Isolate AGF Leader X from external support	Leader X supporters in Government supporters do not publicly condemn detention of HPT #7	Public informed of crimes of HPT #7 and relation to Leader X	Press release on detention of HPT #7	AGF Leader X, region population
Isolate AGF Leader X from external support	Population vicinity town Z more reluctant to provide network smuggling support	Target audience learns information on capture and cooperation of detainees	Handbills in town Z , local or satellite TV commercial	Local population, network members

Figure 4. EBO Model for IO Effects Planning in IW
(Relationship of objectives, effects, and targets)

and 3rd order effects). Given the complex IW environment, the IO officer must not only take into account the likely resulting adversary reactions to friendly operations and events, but also the impact on the population and its resulting actions and reactions. Following are examples of how IO supports or mitigates each level of effects:

- 1st order effect: an immediate physical action or reaction; the IO goal is enable force protection/unit success in executing the mission, and limit adversary response. Could entail EW and tactical PSYOP actions, supported by tactical deception and stringent OPSEC countermeasures.

- 2nd order effect: the quality and integrity of information and information flow; EW, tactical PSYOP actions to limit disinformation resonating with population. Could include an F2F meeting with an influential municipal/religious leader and coordinated CMO to shape perceptions.

- 3rd order effect: decision making and perceptions; this is where the IO officer can bring coordinated capabilities and other actions to support gaining the desired effect/mitigating the preempt or counter effect. Use PA, PSYOP, and F2F to disseminate information.

By applying these suggested actions to a tactical IW scenario, say a raid to capture a suspected terrorist or violent criminal (Figure 3), IO officers can assess an operation's risk and effects.

Understanding 1st, 2nd, and 3rd order effects are also necessary for planning to achieve desired IO objectives. An IO objective should be effects-based, describing an information environment condition or state that IO elements attempt to achieve. The IW challenge is that we cannot always detect the populations' response through intelligence methods, or quantify responses with empirical data. Measuring responses requires 'atmospherics' and information not always personally gathered or observed by US forces—and sometimes not easily or best expressed with numbers. Limitations can be permissiveness of the environment, availability and access to people, and their level of cooperation for polling.

Applying the EBO Model

Just as important as evaluating the hierarchy of effects for planned tactical operations, is determining desired hierarchy of effects and supporting actions to achieve information objectives. There is a difference in "planning operations with effects," and "planning effects-based operations." This is an important distinction in IW. Effects are linked to desired objectives, exerting influence, causing a result, or triggering additional outcomes. IO planners can use an Effects-Based Operation (EBO) model (similar to an Effects Synchronization Matrix) to validate effect objectives, and the military operations supporting them. The model helps verify if we are truly gauging and calculating effects, rather than performance. EBOs address perceptions and cognitive dimensions of an adversary's reality, regardless of physical or military inferiority or superiority. Effects-based methodology is very much relevant in IW because it is centered on the conditions of that reality necessary to achieve success, but may not focus exclusively on an adversary. This is essential in warfare where political and social factors are inseparable from military operations to achieve campaign objectives. It requires IO officers to think well beyond the initial operation or IO action, and ensure we prepare to address collateral, or unintended, effects.

Figure 3 illustrates the hierarchy of effects applied to a tactical operation focused on the adversary. Figure 4 applies an EBO model to an IW objective of identifying information effects related actions. In this scenario the commander's intent is to reduce IED network activity, in order to decrease lethal attacks against the population and US forces. Objectives are: "AGF Leader X network activity reduced" and "Isolate AGF Leader X from external support." This identifies initial targets and actions, both lethal and non-lethal, and resulting direct and indirect effects. From the target, one selects likely 1st, 2nd, then 3rd order effects, ending with the stated objective. This is to ensure the target/action will likely produce the desired outcome. The IO officer evaluates if these likely effects (it is not possible to precisely predict or measure outcomes) are acceptable, and make necessary recommendations to the staff. The IO officer is focused on getting the 3rd order effect to occur.

Information operations planners should have a full breadth of understanding of operational risk and potential order of effects. So must the staff, as these are not exclusively IO functions to develop or gauge.

Conclusion

In the last six years, the prolonged US engagements in Iraq and Afghanistan have had a major impact on how the US conducts military operations, as well as the role general forces play. The methods and processes proposed in this discourse are not definitive, but serve to expand IO team knowledge and thought processes to better succeed in Irregular Warfare campaigns. The purpose is to share ideas and concepts with my peers, IO proponents, and others responsible for the training, educating, and preparing of IO officers for OIF and OEF.

Despite 10 years of Army and Joint IO experience at tactical, operational, and theater levels, I continue to experience hard and sharp learning curves with each successive deployment. Examination of warfare and information operations doctrine is required not just of senior leaders, but all those responsible for executing and coordinating IW operations, especially the military education and training system responsible for preparing those individuals and forces. In IW, the IO role is significantly greater than during major combat operations. People, populations, and the roles they play in society, government, the military, and insurgency, must be our foremost focus.

If all one has is a hammer, then the entire world begins to look like nails. Such limited thinking often extends to what commanders and staffs think IO offers. IO is more than just PA and PSYOP releases following a mission. Although the population's role in IW requires emphasis on the public engagement aspect of IO, an enemy we once underestimated is demonstrating more effective use of cyberspace as an internal and external communication tool. This certainly requires special "technical" IO attention and efforts. Additionally, at the tactical and the theater levels in Afghanistan and Iraq, it is time for PA and PSYOP officers to define how they will cooperate in support of the commander's information objectives, rather than itemizing reasons to stay at arms length. Continued friction only serves the adversary. We cannot prevent our various adversaries from disseminating their messages, but we can impact how that message resonates with intended target audiences. A misguided expectation is that words alone will have a tipping point effect. IO is not a golden arrow or a silver bullet to immediately counter and destroy enemy propaganda, nor cause whole populations to quickly change disposition. IO requires coordinated military operations. We should be capable of advising their commanders of the risks and potential direct, indirect, and collateral effects that physical domain operations will have on the Information Environment. And when evaluating effects, let's not make the process to measure them too hard.

Although force levels may decrease over the next few years, the commitment to victory will not. *People*, their populations and roles they play in society, government, the military—and the insurgency—are a foremost focus of IO methods in support of Irregular Warfare. Our forces in Iraq and Afghanistan must understand and be prepared for the changing threat environment. They must understand social-political situations and their impact on the IW environment, because various adversaries adapt. Other opportunists will surface when current rivals are defeated. COIN successes beget conditions that ultimately result in new problem sets, reflecting the inseparable political, military and social elements in Irregular Warfare. Such a world requires the indirect and non-lethal effects offered by coordinated IO.

A rule to heed: don't underestimate these challenges just because you understood the information and threat environment during your last deployment.

Author's Note: Special thanks to Marc Romanych and Rachel Kitson. I owe a debt of gratitude for their countless hours of editing and comments that significantly shaped the resulting work.

Bibliography/references for this article are on the IO Sphere Home Page at: https://www/jiowc.osis.gov/Publications/IOSphere/index.cfm Click on the "updates" link under the Spring 2008 issue.

LTC Norman E. Emery, US Army, is an Information Operations Officer assigned to 1st Information Operations Command (Land), Fort Belvoir, VA. A veteran of several Afghanistan and Iraq tours, he has performed Army and Joint IO duties since 1997 for the 101st Airborne Division (AASLT), Multi-National Forces-Iraq, and in support of various Special Operations organizations. He has published five articles on the topics of IO/terrorism/insurgency in *IO Sphere, Military Review*, and the *Journal of Information Warfare*. He holds an MS in Defense Analysis from the Naval Postgraduate School, and is pursuing a doctorate in Public Policy, completing a joint thesis (with LTC Robert Earl) on Terrorist Use of Information Operations, under the advisement of Dr. Dorothy Denning. LTC Emery welcomes all comments, questions, and thoughts at norman.emery@us.army.mil, or norm.emery@gmail.com

Information Operations Europe 2008

"Delivering Effect through Influence Activities"

Conference: 25th and 26th June 2008

Pre-Conference Workshops: 24th June 2008

Venue: Le Meridien Piccadilly, London, UK

Now in its 7th Year

Information Operations Europe **is the global annual meeting for the Psychological Operations, Influence and Strategic Communications communities. The key discussion topics and conference highlights include:**

- **Lessons Learned from the Theatre**: Case study briefings detailing proven Influence strategies and tools from Iraq, Afghanistan, Lebanon and Chad

- **Measurement of Effect**: Creative solutions to polling in hostile environments, the work of NATO Research and Technology Organisation's MOE Task Group and the German Armed Force's efforts to measure the success of influence activities in Regional Command North, Afghanistan

- **Coordination of Information Strategies across Departments**: Exclusive briefings detailing US and UK efforts to coordinate cohesive messages and harness all assets for Influence

- **International Military Briefings**: From the US DOD, UK MOD, French MOD, German MOD, Royal Danish Army, European Union Military Service, ISAF, Israeli Defence Forces and NATO

Guest Speakers Include:

- Major General David Morris, Commanding General, US Army Civil Affairs and Psychological Affairs Command (USACAPOC), US Army

- Air Commodore Graham Wright, Director of Targeting and Information Operations, UK MOD

- Rosemary Wenchel, Director of Information Operations and Strategic Studies, Office of the Under Secretary of Defence for Intelligence, US DOD

- Colonel Francois Chauvancy, Chief Information Operations, Joint Centre of Concepts, Doctrine and Experimentation (CICDE), French MOD

- Colonel Huub Vullinghs, Colonel of the Military Psychological and Sociological Branch, Royal Netherlands Army and Chief Information Operations, ISAF until April '08
- Captain Mark Deardurff (USN), Deputy Commander, Joint Information Operations Warfare Command, US Strategic Command

- Lieutenant Colonel Saar Raveh, Staff Officer, Israeli Defence Forces

Priority Registration for* IO Sphere *readers

Please quote the priority booking code (**IGB_11591.002_IOSPHERE_AD**) to ensure a **15% *IO Sphere* discount** on your registration fee. Please note there are only a limited number of ***IO Sphere*** Priority Registrations and they will be allocated to the first registrations made. All Priority Registrations must be completed by 9th May 2008.

FOR MORE INFORMATION:
International Quality & Productivity Center (IQPC)
Web: http://www.iqpc.com/UK/io2008/iosphere
Telephone: +44 (0) 207 368 9300
Email: enquire@defenceiq.com

The Marine Corps Information Operations Center

By the MCIOC Corner Stone Staff

In the information age, the 21st century warfighter cannot ignore the global proliferation of information, such as the twenty-four hour news cycle, internet blogs, the pervasiveness of wireless communication devices and other mediums traveling throughout the world nearly instantly.

Combatant Commanders have prioritized the integration of information operations into joint warfighting missions. The Marine Corps responded to this call in April of 2005 when then Commandant, General M.W. Hagee stated the Marine Corps will "...fully integrate Information Operations into all aspects of MAGTF Operations. Focus on abilities to influence key target audiences and personnel across the spectrum of conflict."

In order to meet this intent, down to the tactical level, the Corps is establishing the Marine Corps Information Operation Center (MCIOC). Set to stand-up in 2009 on Marine Corps Base Quantico, the MCIOC mission will be to provide the MAGTF a full spectrum and readily accessible Marine Corps IO resources.

Major Barry Craft, who serves at Headquarters Marine Corps as the Joint Information Operations Action Officer explained, “Anyone can view the nightly news and see that IO is becoming an essential part of routine military operations world-wide. In fact you can see occasional video messages from extremists on TV news, a form of enemy IO, in order to sensitize the local populace to their cause."

Operations Iraqi and Enduring Freedom after action reports have highlighted IO has helped stifle or prevent many conflicts. Information operations are another tool in the commander’s kit to complete his mission by mitigating an enemy's ability to disseminate hostile propaganda or disinformation that can influence populations, regimes, militaries and their leadership.

"It is not uncommon for Marines to witness a prevalence of effective enemy propaganda on local radio or TV stations in theater. They are facing a modern, sophisticated enemy force. And that enemy is becoming more adept in exploiting information technology to their advantage," said LtCol Mitch Rios, who serves as the Information Operations Chief at Headquarters Marine Corps.

Along with advancing technology, commanders at the "tip-of-the-spear" find information, if used effectively, is a cogent means to secure, shape and condition the battle space similar to direct and indirect fire weapon systems organic to the Marine Air Ground Task Force (MAGTF).

“... our deployed MAGTFs need an IO ‘reach-back’ capability. The MCIOC will be that support, ensuring IO resources and subject matter experts proficient in the capabilities of IO are readily available.”

A critical MCIOC capability will be providing a MAGTF a regionally specific IO support team during contingency operations and exercises. They will assist MAGTF staffs with the development and execution of their IO plan by providing subject matter experts and personnel culturally trained in whatever region the MAGTF is operating in. This will provide the MAGTF commander the capability to influence adversary information and decision-making systems while protecting his own.

In addition to operational support, the MCIOC will provide the ability for the MAGTF Commander to leverage the other service, joint and federal agency IO capabilities and IO centric intelligence expertise through reach back facilitated by relationships developed by the MCIOC.

Major David Clapp, the IO Capabilities, Integration Officer at Marine Corps Combat Development Command said, "our deployed MAGTFs need an IO ‘reach-back’ capability. The MCIOC will be that support, ensuring IO resources and subject matter experts proficient in the capabilities of IO are readily available.”

The MCIOC will also provide the MAGTFs a “reach-across” capability, working closely with other service branch IO organizations. “Since the MAGTF fights in a joint or ‘purple’ environment today, the MCIOC will work with Joint IO teams to best support our missions during joint operations," said Clapp.

The MCIOC implementation team has a long road ahead, but they reached some important development milestones. “Our small cornerstone staff has worked hard to determine our facilities, force structure, training and other requirements across the DOTMLPF (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities) spectrum. Now we need to get the word out there that we are looking for interested Marines with a background in Information Operations, intelligence, and other support functions, to join our team," said Rios.

Once fully operations capable in FY 2010, the MCIOC will staff more than 160 Marines and civilians, specializing in IO related fields. "The MCIOC will do great things for the Corps. Marines need to know joining this team will be a unique and fulfilling opportunity. They will make an impact on the Corps' future warfighting success," said Craft.

For more information on the MCIOC contact Maj. Barry Craft at barry.craft@usmc.mil