THE FUTURE OF INFORMATION OPERATIONS

Major Walter E. Richter, U.S. Army

I N JOINT PUBLICATION (JP) 3-13, *Information Operations,* published 13 February 2006, the Department of Defense (DOD) states that all informational efforts must be part of a robust strategic communication capability supporting governmental activities to understand, inform, and influence relevant foreign audiences.[1]

The visibility and significance of information operations (IO) and strategic communications within national policy has increased in recent years, receiving emphasis in both national defense and national security strategies. Within the combatant commands, IO supports the strategic communication plan to ensure a unity of themes and messages, emphasize success, accurately confirm or refute civilian reporting of U.S. operations, and reinforce the legitimacy of U.S. goals in the international community.[2]

In response to this, the U.S. Army is revising Field Manual (FM) 3-13, *Information Operations*, further refining the November 2003 edition. Even so, its proposed doctrinal changes are evolutionary rather than revolutionary and frequently do not reflect commanders' operational experiences, appearing at times to address Cold War-era threat models.

Will the Army's new doctrinal definition and core capabilities of IO be adequate to support a national strategic communication plan? Will it be able to counter emergent and future threats?

Unfortunately, the current definition and core capabilities of information operations appear inadequate to support a national strategic communications plan, counter emerging threats, or meet National Defense objectives over the next 15 years.

Throughout U.S. agencies, including the military community, the concept of information operations in general and psychological operations in particular as a weapon of deception has gradually diminished. Instead, IO now seeks to influence attitudes and actions within an area of interest, providing a target audience with truthful information. Ideally, this process has the possibility of replacing violence.[3]

The Army has taken a more pragmatic view of IO, choosing to focus on how information best supports leaders in both "kinetic and non-kinetic" operations. This article evaluates the current core capabilities of information operations:

- Psychological operations (PSYOP).
- Electronic warfare (EW).

Major Walter Richter, U.S. Army, is currently the lead planner for the III Corps Strategic Initiatives Group, having recently completed a deployment as a lead planner for Multi-National Corps-Iraq (III Corps). He holds a Masters of Strategy from the U.S. Army Command and General Staff College and a Masters of Operational Studies from Marine Corps University. As a Foreign Area Officer, he is also a graduate of the Slovak National Defense Academy's Senior Commanders' Staff Course.

_____

PHOTO: Light-enhanced, night vision photography showing U.S. Army Soldiers assigned to the 82d Airborne Division, Multi-National Force-West, interviewing Iraqi citizens to gain information on insurgents in northern Al Anbar Province Iraq, 5 May 2008. (U.S. Marine Corps, LCPL Grant T. Walker)

- Computer network operations (CNO).
- Military deception (MILDEC).
- Operational security (OPSEC).
- Public and civil affairs (PA and CA).

For the purposes of this article, the adjective "kinetic" means "relating to the motion of material bodies and the forces and energy associated therewith."[4] Kinetic operations involve application of force to achieve a direct effect, such as artillery, infantry, aviation, and armored offensive and defensive operations. Non-kinetic operations are those operations that seek to influence a target audience through electronic or print media, computer network operations, electronic warfare, or the targeted administration of humanitarian assistance. It is important to note that many operations do not fall neatly into one category or another. For example, a security patrol may have the power to apply force (a kinetic operation), but over time, if its consistently professional conduct earns it the respect of local populace, its presence can become a non-kinetic effect—if not a complete operation in itself.

Both JP 3-13 and FM 3-13 define IO as "the integrated employment of the core capabilities… in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting [friendly] core capabilities."[5] Here, the difference between kinetic and non-kinetic operations becomes ambiguous. The benefit of this ambiguity is that it allows commanders the option of focusing IO on both kinetic and non-kinetic operations, possibly using indirect fire assets to strike at information nodes, destroying command and control through computer network attack, using deceptive tactics incorporating electronics, or employing active and passive measures to safeguard friendly command and control. Conversely, commanders may also direct IO planning efforts toward non-kinetic operations: learning enemy combatant objectives through a comprehensive cultural-anthropological understanding of local leaders and their ideological underpinnings, or bolstering public perceptions of friendly forces.

While commanders must always retain the initiative to incorporate both kinetic and non-kinetic assets to establish information superiority, is it an effective allocation of assets for the IO cell to coordinate such divergent capabilities, while G3 operations already focus their actions on many of the same areas? In order to ensure that future commanders do not lose information superiority against enemies unbound by ethics or the truth, it is necessary for IO officers to become resident experts with skills in public information, marketing, and cultural anthropology.

Consequences of Recent Military Operations

Current Army information operations doctrine emerged from the 1996 FM 100-6, *Information Operations*, which divided IO into five core capabilities that supported the physical destruction of an enemy: PSYOP, CNO, MILDEC, EW, and OPSEC.[6] Information operations included the ability to ensure the security of friendly information systems and to synchronize the application of force throughout hierarchical and nonhierarchical systems—linking sensors, shooters, and commanders—while degrading, disrupting, or exploiting the enemy's command and control. Acknowledging the criticality of adapting to the changing information environment, doctrine remained focused almost solely on defeating a conventional military enemy through support of kinetic operations.

To be fair, the 1996 FM 100-6 did acknowledge the need to conduct IO across the full spectrum of military operations. Nonetheless, the previous decades' focus on Soviet threat capabilities and the subsequent 1991 Gulf War against a conventional, Soviet-modeled force likely constrained American military thought. Despite the December 1995 Dayton Peace Accords, a response to the ethnic conflict in the former Yugoslavia, FM 100-6 failed to consider the rise of non-state actors or the emergence of military operations no longer wholly focused on the physical destruction of an enemy. Now, rather than only denying, defeating, or destroying an enemy, American military leaders must work to create stable and secure environments, thereby promoting the rule of law and respect for human rights.

The Balkans

Information operations, as an institutionalized art, showed its potential during NATO-led operations in the former Yugoslavia as U.S. military leaders

> *…American military leaders must work to create stable and secure environments, thereby promoting the rule of law and respect for human rights.*

responded to manipulation of the media by Bosnian, Serb, and Croatian political leaders who were igniting latent ethnic hatreds.[7] Originally, the Serbs used government-controlled media to target only Serb citizens with its distorted messages (rather than the international community). Government leaders sowed fear and paranoia in Bosnian-Serbs, who in turn developed a violent hatred of Bosnian and Croat ethnics within Yugoslavia, further convincing the Serbs that they were indeed struggling for their survival as a people. While these messages were highly effective among the Serbs, they found little resonance elsewhere.[8]

Bosnian Muslim (Bosniac) leaders initially had little in the way of media assets. However, since nearly all of the international press correspondents in the former Yugoslavia were in Sarajevo, a city besieged by Serbs, the perception of Bosniacs as hapless victims rapidly spread worldwide. Since journalists and the predominantly Bosniac Sarajevans shared the same hardships, many reporters may have developed a biased perspective, focusing solely on Muslim suffering at the hands of the Serbs.[9]

After the U.S. deployment as part of the Dayton Accord Implementation Force (IFOR) in December 1995, and after the publication of FM 100-6 in 1996, U.S. commanders soon found that IO doctrine failed to recognize the effect that public information (PI) had on local populations. In the form of local and international news media, as well as the growing online community, public information held tremendous influence over the population that IFOR was attempting to stabilize. Given IFOR's mission to enforce the Dayton Peace Accords and public information's predominance on the populace, it became virtually impossible to separate public affairs completely from IO.[10] With the assistance of the Land Information Warfare Agency, leaders from the 1st Armored Division

and later the 1st Infantry Division established an IO council designed to bring together key players for information dissemination from PI, PA, G3, PSYOP, and Civil Affairs.[11]

By obtaining input from the IO council and presenting truthful information to the populace, the multinational division countered the enemy propaganda disseminated by local media. Active throughout the planning process, IO identified target pressure points of local leaders, objectives for each target, and used a division synchronization matrix to mesh IO core capabilities. In order to convey the division's message to Bosnian public, the IO council coordinated PSYOP radio messages with Army division press releases to prevent conflicting messages or "information fratricide." While fratricide of this nature commonly involves casualties due to conflicts between friendly communication systems, information fratricide can also be public information that compromises OPSEC or the local credibility of a unit's leaders and Soldiers.

The ethicality of PA and IO integration has remained a contentious debate with military officials firmly ensconced on both sides of the issue. One U.S. Army public affairs officer stated in a recent article that "the practical military value of public affairs to the operator is neither tactical nor operational, nor is it easily quantifiable. It is strategic, a concept that is difficult to perceive or stomach when one is locked into personal and savage combat at trench-knife level."[12] In short, PA service to the Army is an institution with its own legitimizing code of conduct that supersedes any one command or mission.

Conversely, a U.S. Air Force spokesperson stated that while credibility is an unambiguous and inflexible standard of professional conduct, it is neither a center of gravity nor an objective in and of itself.[13] Rather, PA must support the command and its mission through accurate and timely reporting, detailed media analysis, media training, and talking points for Soldiers throughout all levels of the command.

This integration of public information with IO was employed and refined during the war against Serbia and subsequent stability and support operations in Kosovo. Command reluctance to confront the press furthered media speculation after U.S. Air Force F16s mistakenly hit a refugee convoy during the bombing campaign against the Serbian

> *…while credibility is an unambiguous and inflexible standard of professional conduct, it is neither a center of gravity nor an objective in and of itself.*

capital. The lack of a common PA theme among commanders led to conflicting statements by NATO leaders that Serbs were responsible for the attack. The commanders later admitted that NATO had indeed fired on the convoy, but said they only targeted military vehicles. After a week without a clear military message, NATO belatedly addressed the issue openly through a PA assessment of issues that did much to quell the speculation about the incident.[14] Unfortunately, the initial lack of a coherent response had already undermined the credibility of peacekeeping forces in Kosovo.

Throughout operations in the Balkans, Combat Camera also emerged as a powerful information tool, documenting activities and events for exploitation by PA or PSYOP. Additionally, Combat Camera supported commanders during contentious opera-

tions such as cordons and searches as a means to counter enemy propaganda rapidly.

Published experiences of commanders in the Balkans repeatedly emphasize the criticality of information dominance. While one cannot ignore the role of technology, these lessons emphasize the human dimension and the need to develop an understanding of social and cultural structures through communication, both formal and informal. However, the Army has yet to adjust its doctrinal IO core capabilities, especially the incorporation of PA and CA within IO.

Afghanistan

Experiences in Afghanistan further demonstrate the need to integrate public affairs and civil affairs into information operations. In response to the terrorist attacks of 11 September 2001 against the World Trade Center and the Pentagon, the United States initiated military actions in Afghanistan by means of Operation Enduring Freedom (OEF). Early operations used land-based B-1, B-2, and B-52 bombers; carrier-based F-14 and F/A-18 fighters, and Tomahawk cruise missiles launched into Afghanistan from both U.S. and British ships and submarines; and special operations forces providing ground coordination and working closely with local Afghan militias opposed to the Taliban regime.[15] Initial military objectives were the destruction of terrorist training camps and infrastructure within Afghanistan, the capture of Al-Qaeda leaders, and the cessation of terrorist activities in Afghanistan.[16]

Electronic warfare predominated these early IO efforts, targeting enemy communication and air defense artillery assets. Psychological or influence operations focused on convincing enemy combatants to surrender. Only later did commanders work to convince Afghans that attacks on Taliban fighters were not attacks on the Afghan populace, thus laying the groundwork for a democratic Afghan government opposed to terror and respectful of human rights. Influence operations sought to convince world audiences that despite the violence

A U.S. Air Force F-16C Fighting Falcon aircraft of the 31st Fighter Wing takes off for a mission in support of NATO airstrikes against the Bosnian Serbs, September 1995.

DOD, SSGT Dixie Trawick

of its attacks on the Taliban and Al-Qaeda, the coalition was doing everything possible to minimize the loss of life and property of Afghan civilians.[17]

While the coalition's overwhelming military strength ensured that these initial kinetic operations were successful, they did not fully address cultural issues critical to establishing democracy in Afghanistan. The tendency of commanders to focus IO solely on supporting kinetic operations is understandable, because gauging the success of influence operations is inherently more complex than tallying a battle damage assessment of an air strike. Not surprisingly, IO lacked the doctrinal structure to address these issues. It had remained focused on physical

U.S. Air Force, TSGT Cecilio Ricardo

A C-130 Hercules loadmaster drops a box of 10,000 warning leaflets over Afghanistan. Early psychological or influence operations in Afghanistan focused on convincing enemy combatants to surrender.

systems and not Afghan culture, thus limiting the coalition's ability to influence the people. In short, the exclusive use of IO to support short-range kinetic objectives is redundant and ultimately fails to support a commander's long-range objectives.

The skills necessary for IO planners to implement successful influence operations are markedly different from those needed to destroy a combatant's information capabilities. Creating conditions conducive for a stable government is a far greater IO challenge. Furthermore, IO planners must ensure that support is long-lasting and that desired conditions will persist long after coalition forces have left. In preparation for OEF, military planners either overlooked long-term informational consequences or, subsumed by the immediacy of their kinetic operations, paid insufficient attention to the mission's message and effect on long-term objectives.

In order for an IO theme to be successful, it must fulfill three criteria:

● It must first recast the perception of the enemy, both locally and internationally, from that of freedom fighters or even rebels, to that of an illegitimate militant force or something else unacceptable to the local culture.

● Second, it must recast the nature of conflict, or (more important) the perception of the conflict, both nationally and internationally, so that the coalition forces are seen as liberators and not a conquering army.

● Third, it must have the ability to recast the ultimate goals of the operation as conditions on the ground meet or fail to meet planning expectations.[18]

In all this, it is critical when confronting numerous threats across vastly different cultures that planners recognize that one solution will not fit every situation. In other words, a particular projected image of coalition forces may be acceptable to one society and wholly unacceptable to another.

The recent resurgence in militant and criminal activity by the Taliban may very well be due to IO planning oversights, such as eradicating poppy production without providing poppy farmers with profitable alternatives. Nevertheless, prior to this resurgence, IO had undergone refinements in the planning and execution of IO and in the areas of CA and PSYOP, along with increased interagency integration. PSYOP provided support to the interim Afghan administration as well as humanitarian de-mining operations. Civil affairs Soldiers also coordinated with non-governmental organizations as part of the State Department's Overseas Humanitarian Disaster and Civic Aid program. The experience demonstrated the need for a fully equipped

civil military operations center, capable of entering the theater with little logistical support from theater-level special operations forces.[19] These experiences highlight the integral role CA has already played in successful IO as a means to influence the populace. The potential of proper CA integration is not the ability to "win hearts and minds." Rather, it is the ability to establish relationships of mutual respect and trust that foster popular support as all sides recognize the long-term benefits of cooperating with coalition forces.[20]

Iraq

In early 2003, the United States prepared to lead an international coalition to oust the regime of Saddam Hussein. It appeared that information operations received consideration limited to kinetic operations as the coalition invaded Iraq and the Ba'athist leadership fled. Information operations again focused largely on supporting the defeat of Saddam's regime, not establishing a stable environment or a lasting peace. Worse yet, the coalition's practice of occupying former Ba'athist party palaces and infrequently mingling with the local populace may have prevented many Iraqis from coming to see coalition forces as something more than a follow-on regime to the Ba'athists.[21] Frequently, inexperienced Soldiers found themselves in a dangerous situation where enemies were hard to identify, and they sometimes would "humiliate the men, offend the women, and alienate the very people who are supposed to be providing intelligence about terrorists and Ba'athists."[22]

Technologically focused IO planners concentrated efforts on tracking computer networks and integrating EW and CNO into division operations. They soon found themselves struggling to understand social structures, ethnic and tribal divisions, and historical factors that fed into the emerging intra-Iraqi conflict.[23] Fortunately, information operations have received increasing consideration as the conflict has progressed. Commanders who originally saw IO as a distraction to fighting and winning soon sought to understand the ethnically diverse sectors they controlled. As they developed their understanding of IO, they created organizations at brigade, division, and corps levels to address the human dimension of the conflict.

Like others did in the Balkans and Afghanistan, Colonel Ralph O. Baker, a brigade commander in Iraq, discovered the operational significance of public information and the subsequent need for PA and IO integration. He realized that press releases, whether Iraqi or international, have immediate effects on popular attitudes and can counter enemy propaganda. To assist Baker's IO planning, PA provided him with media analysis on popular perceptions in sector.[24] Coordinated through CA units, organic engineer and medical assets, and maneuver units, humanitarian assistance helped establish relationships of "trust and respect" among community leaders and service members.

Despite the contentiousness of the IO-PA issue, most senior military leaders acknowledge the need for effective PA-IO integration. Joseph Collins, former Deputy Assistant Secretary of Defense for Stability Operations, stated that if strategic communications in Iraq

DOD

The coalition practice of occupying former Ba'athist party palaces may have created an impression that coalition forces were a successor to the Ba'athist regime, rather than a liberating force.
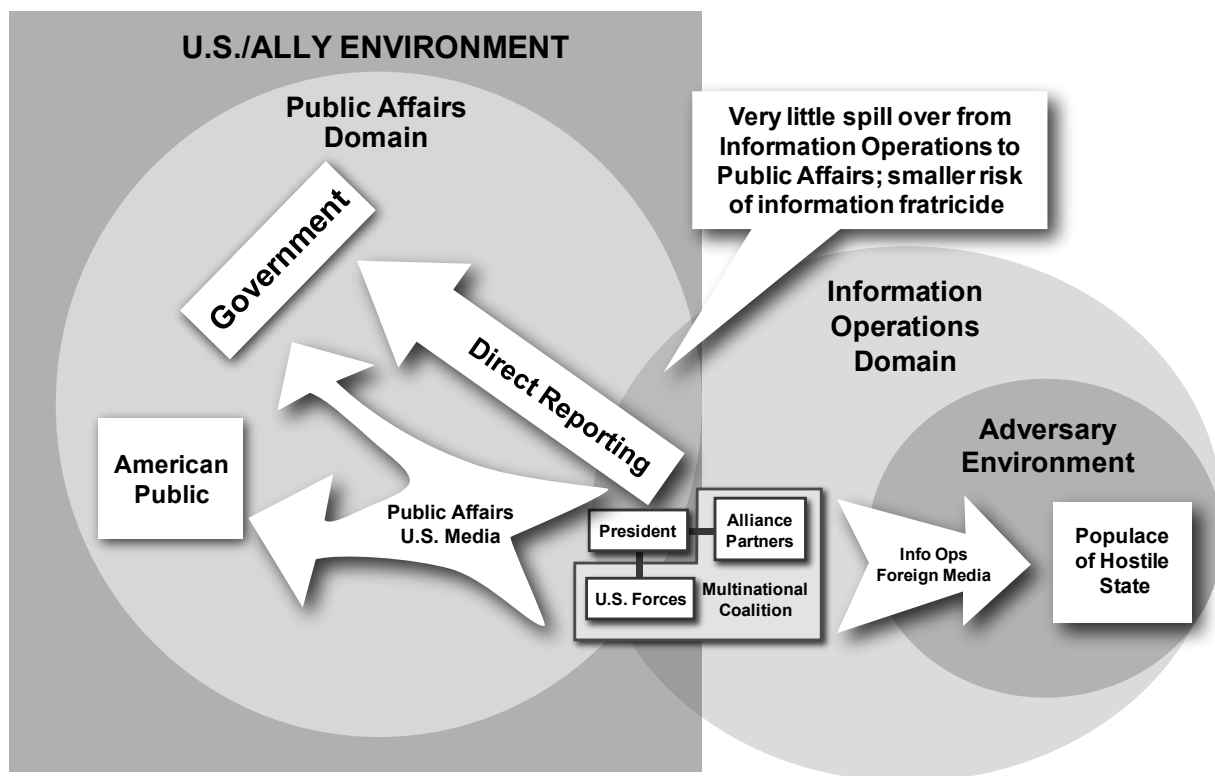
Figure 1. Old information environments.

do not improve, we will fail. He went on to add, "We are not achieving synergy and mass in our strategic communications." After a tour as III Corps commander in Iraq, Lieutenant General Thomas Metz declared that the Army needed a "broader and more aggressive, comprehensive, and holistic approach to IO—an approach that recognizes the challenges of the global information environment and seamlessly integrates the functions of traditional IO and PA—to succeed on the information-age battlefield."[25]

The need for leaders to understand complex social networks, not just computer or electronic networks, is a constant theme in Operation Iraqi Freedom after-action reviews. While media such as radio, television, and the Internet are invaluable in delivering messages, the greater need is for messages that will create cultural and social resonance in the local population.

Proposed Changes

In discussing information flow, it is helpful to consider how it has evolved and changed. Figure 1 demonstrates how the United States traditionally viewed the flow of information in and out of theater and to and from the military to the U.S. government,

the American public, and a foreign audience. Note that while information flow has become more complex and erratic, it was never simplistic or entirely precise in nature.
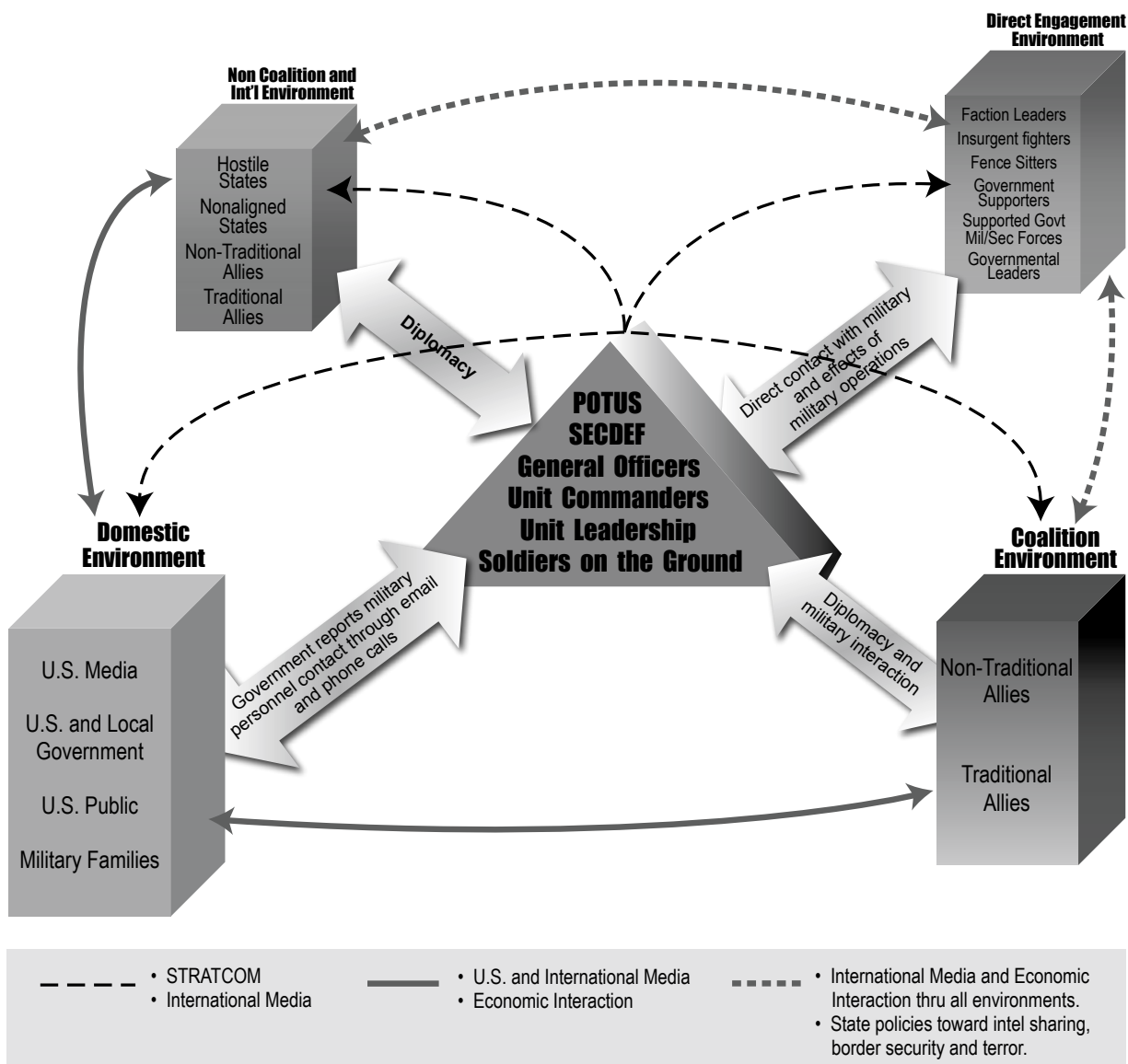
As information environment models have become three-dimensional, information flows more rapidly across all boundaries. IO was previously relegated to an "adversary environment," with PA in a "U.S./ally environment." Now, information flows easily across four different environments:

● The direct engagement environment.
● The domestic environment.
● The allied coalition environment.
● The non-coalition/international environment.

While each environment has its own characteristics, IO can no longer consider these environments simply as friend or foe. Within each environment, there are varying degrees of trust and commonality with respect to U.S. goals and objectives. The most significant difference between these environments is how the same information will have vastly different effects from one to the next.

In analyzing the emergent effects of the new information environments (Figure 2), it may be tempting to focus exclusively on the technology transmitting

Direct Engagement Environment

Faction Leaders
Insurgent fighters
Fence Sitters
Government Supporters
Supported Govt Mil/Sec Forces
Governmental Leaders

Non Coalition and Int'l Environment

Hostile States

Nonaligned States

Non-Traditional Allies

Traditional Allies

Diplomacy

Direct contact with military and effects of military operations

POTUS
SECDEF
General Officers
Unit Commanders
Unit Leadership
Soldiers on the Ground

Domestic Environment

U.S. Media

U.S. and Local Government

U.S. Public

Military Families

Government reports military personnel contact through email and phone calls

Diplomacy and military interaction

Coalition Environment

Non-Traditional Allies

Traditional Allies

- - - - -   • STRATCOM
• International Media

————   • U.S. and International Media
• Economic Interaction

· · · · ·   • International Media and Economic Interaction thru all environments.
• State policies toward intel sharing, border security and terror.

Figure 2. New information environments.

the data. However, based on commanders' observations, controlling or stopping information flow is virtually impossible. The value of IO resides not in the technology of information transmission, but in understanding how that information affects the environment. Moreover, in response to concerns that IO must provide support to technical capabilities, resident experts in the Army's Network and Space Operations and Forces Development Signal Corps can provide far more comprehensive support than IO. The incorporation of these assets back into G2 (for collection) and G3 (for offensive electronic measures) would better allow IO to concentrate on influence operations.

Public Affairs versus Information Operations

The integration of PA and IO is a continual theme throughout numerous after-action reviews. Incidents involving the Lincoln Group's placement of positive stories in Iraqi newspapers demonstrate how readily information now crosses environments and raised concerns over the prospect of IO controlling PA.[26] The issue here is that the stories, while factual, were deceitful in concealing their source by appearing to reflect the interests of the editorial staff of an Iraqi newspaper.[27]

Stories such as these undermine the credibility of any positive coverage the military receives. Proper

coordination of PA with IO must never deceive the populace as to the origin of information. Rather, coordination ensures that press releases counter enemy propaganda, do not violate OPSEC, and minimize information fratricide. If commanders are consistent in their press releases and avoid information fratricide, in time they may have greater success establishing trust and respect with the populace. Additionally, PA should provide units media analysis and media training, better enabling them to engage the media effectively, thereby further establishing and maintaining credibility.

New Information Operations Concepts

Beyond PA integration, how can IO further enhance influence capabilities of a supported command? Persistence of current conditions in future operations could provide the Army with the incentive to provide extensive training and education to IO officers in the studies of both marketing and cultural anthropology.

IO as marketing. Marketing tools and concepts could generate support for coalition military operations just as an advertiser promotes a commercial product. Similar to commercial products, local support for coalition operations has benefits and costs. Benefits for citizens supporting coalition operations may be humanitarian assistance projects in their towns, as well as stability and security in their neighborhoods. Costs for that cooperation may be the loss of black-market wealth and the appearance of collaboration, placing the lives of coalition supporters and their families in peril. While applying commercial concepts to military operations may appear unorthodox, this construct could help IO planners present commanders with a clear cost benefit analysis of the conditions that commanders need the local populace to accept.[28]

While it is difficult to predict future areas of operation for the U.S. military, the use of marketing tools to leverage humanitarian assistance and public affairs within an information operations plan to target a global audience has tremendous possibilities for future operations.

Cultural anthropology. In conjunction with marketing, cultural anthropology seeks to understand the motivations and desires of actors within the context of a culture and society. Cultural anthropology is the "scientific study of human culture based on archaeological, ethnological, ethnographic, linguistic, social, and psychological data and methods of analysis."[29] It is a social science discipline whose traditional focus has been non-Western tribal societies, some of which we now confront in current operations. Anthropological methodologies include participant observation, fieldwork, historical research, and endeavors to understand societies from their perspectives, rather than through the researchers' personal experiences, beliefs, and values.[30]

Within the military, a primary task of cultural anthropology would be translating knowledge gained from field experience into doctrine, an obvious benefit for military leaders seeking to understand and even predict behavior in non-Western societies. Despite such benefits, there has been little movement to incorporate anthropology into military leader training.[31] In military terms, understanding cultural anthropology is an important step toward enabling better human intelligence. Understanding cultures through training, increased interaction with local populations during operations, and ideally living among them may help local civilians understand a unit's values and its mission. While there is an inherent security risk in this, increased public access may create commonality between military units and a local populace.

For future operations, Soldiers will require a greater appreciation of the culture in which they operate. Knowledge about customs and courtesies is valuable, but only a beginning. Leaders, planners, and Soldiers must understand how a culture will affect operations. Forcing IO officers to focus on human rather than technical aspects of information environments will better enable IO to leverage influence and will provide combat leaders, planners, and Soldiers the necessary tools for future deployments.

> *For future operations, Soldiers will require a greater appreciation of the culture in which they operate.*

Change in Definition

The current definition of IO listed in the November 2003 FM 3-13 is:

> The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision making.

The U.S. Army recently approved an updated definition that replaces the previous purpose, "to affect," with an expanded one that reads:

> . . . to influence, disrupt, corrupt or usurp adversarial human and automated decision making, while protecting our own. It includes the use of these capabilities to influence the perceptions of foreign friendly and neutral audiences.

Reassessment of Core Capabilities

While the revised purpose acknowledges the ramifications of incorporating IO into planning, it does nothing to reassess core IO capabilities, and may give commanders who previously focused IO on kinetic operations the misleading impression that technology remains the key to information superiority. On the contrary, capabilities historically associated with successful IO are PA, PSYOP, Combat Camera, and civil affairs/civil-military operations.

If current trends persist, operations focused solely on destroying an enemy, objective, or capability will occur with decreasing frequency, while missions to enable a foreign security force or empower a local civil administration will become more frequent. Beyond just accomplishing increasingly complex missions, the ability to project these successful accomplishments, either locally, internationally, or both, may well determine overall mission success.

The IO core capabilities that can effectively address future operations—PA, PSYOP, Combat Camera, and CA—should be reassessed.

The current IO core capabilities of OPSEC and MILDEC could fall under G3 operations, while EW and CNO could fall under the G6 for support, under the G2 for collection of intelligence, and under the G3 for offensive electronic measures. While this may seem a radical departure for some, it would represent an institutional acknowledgement of what is already a reality on the ground.
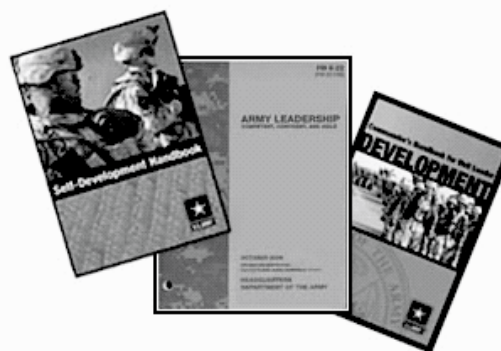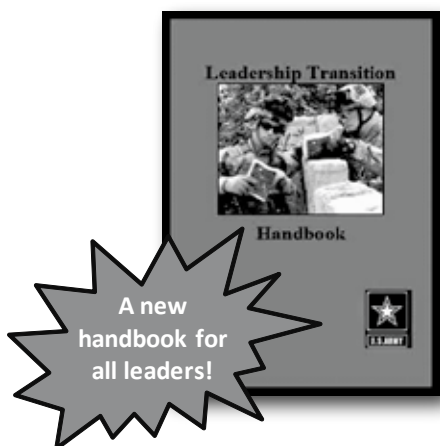
Implications for Future Operations

U.S. National Security Strategy calls for a "future force that will provide tailored deterrence of both state and non-state threats (including WMD employment, terrorist attacks in the physical and information domains, and opportunistic aggression) while assuring allies and dissuading potential competitors."[32] As a consequence, the lines between informational environments will continue to blur.

The lessons in this subject have repeatedly presented themselves during operations in the Balkans, Afghanistan, and Iraq, but caused little change in doctrine. In light of the Army's ongoing self-assessment and published reports, commanders in Afghanistan and Iraq must have been aware of the challenges faced in the Balkan operations. The reluctance to modify doctrine may have been the result of an unwillingness to accept the risk of diverting limited assets and personnel from the mission of destroying the enemy. However, a more likely explanation was that planners viewed lessons learned after a peacekeeping mission as invalid for high intensity conflict.

For information operations to address these threats adequately and support a national strategic communications plan, the Army must ensure its IO officers have the skills and assets necessary to provide commanders with an in-depth understanding of cultural and societal factors within any given environment. IO officers must further assess how those factors will affect operations, further enabling commanders to influence local populaces, establish relationships of trust and respect, and ultimately create legacies of stability and security. *MR*

NOTES

1. JP 3-13, *Information Operations* (U.S. Joint Publication: 13 February 2006), I-10.

2. GEN Richard Myers, *National Military Strategy: A Strategy for Today, A Vision for Tomorrow* (Washington, DC: Joint Chiefs of Staff, 2004), 12.

3. Robert David Steele, "Information Operations: Putting the 'I' back into DIME" (Carlisle Barracks, PA: Strategic Studies Institute of the U.S. Army War College, February 2006).

4. *Merriam-Webster Online* (2007) [database on-line]; available from <www.m-w.com/dictionary/kinetic>; Internet, accessed 4 February 2007.

5. JP 3-13.

6. FM 100-16, *Information Operations* (Washington, DC: U.S. Government Printing Office, 1996).

7. Steven Collins, "Army PSYOP in Bosnia: Capabilities and Constraints," *Parameters* (Carlisle, PA: U.S. Army War College, Summer 1999): 57-73.

8. Ibid.

9. Ibid.

10. MAJ Todd Sholtis, "Planning for Legitimacy: A Joint Operational Approach to Public Affairs," *Air & Space Power Journal* (8 June 2005), on-line, available from <www.airpower.maxwell.af.mil/airchronicles/cc/sholtis.html>, accessed 20 February 2007.

11. Pascalle Combelles Siegel, "Information Activities," *Lesson from Bosnia: The IFOR Experience* (1997) [ASAF Air War College database on-line], available from <www.au.af.mil/au/awc/awcgate/ccrp/wentz_bosnia.pdf>, accessed 20 February 2007.

12. COL William M. Darley, "Why Public Affairs is not Information Operations," *Army Magazine*. 55, no. 1 (January 2005), <www.ausa.org/webpub/DeptArmyMagazine.nsf/byid/CCRN-6CCSFV, accessed 20 February 2007.

13. Sholtis.

14. MAJ Gary Pounder, "Opportunity Lost: Public Affairs information operations, and the Air War against Serbia," *Aerospace Power Journal* (Maxwell Air Force Base, AL: Air Force University, Summer 2000): 1-2.

15. "Operation Enduring Freedom—Afghanistan," *Global Security Website,* <http://www.globalsecurity.org/military/ops/enduring-freedom.htm>, accessed 19 February 2007.

16. George W. Bush, "September 20th Address to a Joint Session of Congress" and "October 7th Address to the Country," *Global Security*, <www.globalsecurity.org/military/ops/enduring-freedom.htm>, accessed on 19 February 2007.

17. MAJ Joseph Cox, "Information Operations in Operations Enduring Freedom and Iraqi Freedom—What Went Wrong?" (Fort Leavenworth, KS: School of Advanced Military Studies, 2006): 57.

18. Peter W. Singer, "Winning the War of Words: Information Warfare in Afghanistan, America's response to Terrorism Analysis Paper #5, (23 October 2001). [Brookings Institute database on-line]; available from <http://www.brookings.edu/views/papers/psinger/20011023.htm>: Internet; accessed 30 November 2006.

19. BG Pat Maney, Deputy Commander, USACAPOC (A). "Lessons Learned in Afghanistan Slideshow" *National Defense Industrial Association-SO/LIC Symposium* (11 February 2003), U.S. Air Force Air War College database on-line, <http://www.au.af.mil/au/awc/awcgate/ndia/maney.pdf>, accessed 19 February 2007.

20. LTC Charles Eassa, Deputy Director, U.S. Army Information Operations, source, Michael Schrage, "Use Every Article in the Arsenal," *Washington Post* (15 January 2006).

21. MAJ Norman Emery, "Information Operations in Iraq," *Military Review* (May-June 2004): 11-14.

22. Evan Thomas, "Groping in the Dark," *Newsweek* (1 September 2003): 30.

23. Personal interview with LTC Charles Eassa, U.S. Army, Deputy Director, U.S. Army Information Operations Proponent (Alexandria, VA: 2 November 2006).

24. COL Ralph O. Baker, "The Decisive Weapon," *Military Review* (May-June 2006): 13-32.

25. LTG Thomas F. Metz, "Massing Effects in the Information Domain," *Military Review* (May-June 2006): 2-12.

26. Josh White, "Military Planting Articles in Iraq Papers," *Washington Post,* 1 December 2005, A18.

27. Ibid.

28. CPT Stoney Trent, "Marketing: An Overlooked Aspect of Information Operations," *Military Review* (July-August 2006): 70-74.

29. Anne H. Soukhanov, *Webster's II, New Riverside University Dictionary* (Boston, MA: The Riverside Publishing Company, 1994), 335.

30. Montgomery McFate, "Anthropology and Counterinsurgency: The Strange Story of their Curious Relationship," *Military Review* (March-April 2005), <www.army.mil/professionalwriting/volumes/volume3/august_2005/7_05_2.html>, accessed 20 February 2007.

31. Ibid.

32. George W. Bush, *National Security Strategy 2006.*