CHAPTER 15

Tactical Influence Operations

Stuart H. Starr

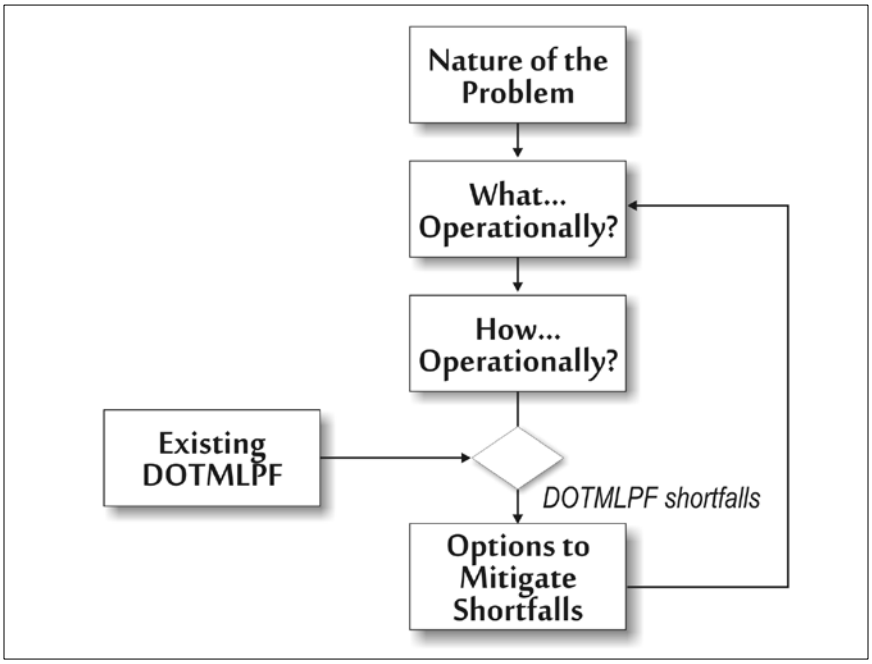
THIS CHAPTER explores the challenges associated with influence operations at the tactical level. It begins with a framework that identifies five key interrelated areas for the analysis of tactical influence operations options. To illustrate the framework, the creative actions taken by Colonel Ralph Baker, USA, in the early days of Operation *Iraqi Freedom* are examined.[1] The framework then looks forward to identify and explore options for enhancing tactical influence operations by exploiting the opportunities offered by advances in cyberspace.[2] The chapter concludes with a brief summary to guide policymakers and identify residual policy issues that warrant further attention.

Framework: A Mission-Oriented Approach to Tactical Influence Operations

A useful framework for assessing influence operations is based on the mission- oriented approach to command and control (C^2) assessment,[3] which addresses five interrelated questions (shown in figure 15–1):

- What is the nature of the problem?
- What are you trying to do operationally?
- How are you trying to do it operationally?
- What gaps in the areas of doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) impede this operation?[4]
- What steps should we take to ameliorate key DOTMLPF gaps?

Figure 15-1. Mission-Oriented Approach



The mission-oriented approach has been applied to a variety of C^2 issues. From 1980 to 2000, these included the development of a North Atlantic Treaty Organization C^2 plan[5] and the derivation of an advanced battlespace information system to support transformation of the force.[6] The focus of those activities was to formulate and link alternative operational objectives to associated materiel needs and plans, including science and technology initiatives. Here, we extend the mission-oriented approach to address the full spectrum of DOTMLPF factors.

Lessons learned from prior applications of the mission-oriented approach are applied to the analyses of tactical influence operations. First, the nature of the problem demands a mix of skills to implement the approach. Thus, we need to tap the insights of high-level decisionmakers, operational personnel at the tactical level, and experts in DOTMLPF. Second, problems of this nature are generally characterized by the "curse of dimensionality," which requires structured techniques for keeping the problem tractable by deconstructing it, for example, by factors such as geography and range of military operations. Third, it has proven useful to apply the framework iteratively in order to identify and address critical issues systematically. Thus, we employ a broad, shallow cut to analyze tactical influence operations in this chapter. Subsequent iterations would consider narrower, deeper cuts organized around the major policy issues. Fourth, it has proven useful to formulate measures of merit (MOMs) to support analyses of these issues. In this chapter, we identify and discuss key input and out-put MOMs.

Nature of the Problem

To set the stage for the analysis, we identify and describe the key stakeholders and characterize the environment in which they are interacting. We illustrate the application of the framework with the experiences of Colonel Ralph Baker, USA, in Baghdad.

From 2003 to 2004, COL Baker commanded roughly 5,000 members of the 2^{d} Brigade Combat Team, part of the 1st Armored Division. The unit was deployed in two of Baghdad's nine major districts, Karkh and Karada, covering an area of 400 square kilometers. This area of responsibility (AOR) is highly varied in sectarian composition, with a mix of Sunni, Shia, and Christian populations, and in the distribution of wealth, with neighborhoods ranging from affluent to poor. Baker found it vital, therefore, to tailor his influence operations to deal with this mix.

Baker divided the indigenous population into three categories. First, he identified those who "would never accept the Coalition's presence," such as insurgents and terrorists. Baker engaged in an "influence operations duel" with that segment of the population. He observed that they were extremely agile at exploiting adverse events for influence purposes. For example, kinetic events such as improvised explosive device (IED) incidents and sniper attacks were deliberately used in order to acquire dramatic video shots for future influence operations activities.[7] Relatively unsophisticated in its employment of influence operations tools in 2003–2004, this segment of the population has since improved its production capabilities considerably to include use of the Internet and mass media. This category has, over the last several years, also become much more complex in its makeup due to a confusing combination of insurgent activity, terrorist actions, civil war, and organized crime.

A second category Baker identified comprised those who "readily accept the Coalition's presence (for example, secular, Western-educated pragmatists)." He viewed them as natural allies who could serve as surrogates to communicate his influence operations message.

The deteriorating situation in Iraq, however, subsequently caused many in this category to flee to Jordan, Syria, and other countries.

Baker characterized the third category as undecided: "the vast majority." It is this group that constitutes the "terrain" for tactical influence operations. Baker identified two major issues with the influence operations campaign that he inherited, from top-down and bottom-up perspectives. First, he noted that higher echelon activities were slow to respond to changes on the ground and were not tailored adequately to selected audiences. This slow, one-size-fits-all approach never fit anyone. From a bottom-up perspective, activities at battalion level and below manifested creativity but were marred by inconsistent and contradictory messages, a problem Baker called "IO [information operations] fratricide."

The nature of the overall problem can also be characterized by employing a simple societal model. In this model, the inputs are the individual levers of national power, including mixes of diplomatic, informational, military, and economic (DIME) actions. The societal outputs can be classified as political, military, economic, social, informational, and infrastructure (PMESII) elements.[8] The following discussion briefly summarizes the PMESII situation that Baker encountered in 2003–2004.

Politically, while COL Baker was in Iraq, the Coalitional Provisional Authority (CPA) was in its early stages, and a national Iraqi government was just emerging. Militarily, security was marginal and on the verge of substantial degradation; at that point, there was a debate as to whether an insurgency was under way. Economically, there was extremely high unemployment; the Iraqi army had been disbanded, and former Ba'athists had been discharged from their jobs. Socially, sectarian schisms were appearing, which subsequently deepened considerably following major acts of violence such as the destruction of the Shi'ite mosque in Samarra. Informationally, a strident tone was emerging from the clergy and segments of the Arab press such as al Jazeera. Perhaps most importantly, the infrastructure was dysfunctional: Coalition commanders had identified the urgent need to improve Iraqi sewage, water, electricity, academic institutions, and trash collection systems.[9] The information communications technology structure was also in disrepair; thus, options to exploit cyberspace to support influence operations were not readily available (an issue further discussed below).

Operational Goals

An operational goal often quoted during the Vietnam War was "to win the hearts and minds" of the population. In Iraq, however, COL Baker concluded that it would not be feasible to realize that ambitious goal, which transcended the tactical, amounting to an operational or strategic goal. More practically, realizing a goal of that magnitude would require developing legitimate friendships, but to do so would take more effort and time than he could afford.

Therefore, Baker adopted an alternative goal: "earn the trust, confidence, and respect of the Iraqis." To achieve that goal, he pursued two themes: "discredit insurgents and terrorists," and "highlight economic, political, social, and security reforms."

For the purposes of this chapter, COL Baker's operational goal is a point of departure for use of the mission-oriented approach to explore the consequences of pursuing each theme. Thus, having answered the first two questions—the nature of the problem, and the operational goals—we seek answers to the third question: how best to pursue this goal?

Accomplishing Operational Goals

This segment considers two answers to the question of how to pursue the chosen operational themes. Looking backward, we examine the choices that COL Baker made to implement an operational plan of attack. Looking forward, we identify how cyberspace might be leveraged for future tactical influence operations.

Looking Backward: Empirical Lessons for Tactical Influence Operations

Baker elected to try to reach the "undecided" population by focusing on five specific audiences: media (the Arab press), clerics (such as imams), sheiks and tribal leaders, local government officials, and university and school leadership. Choice of target audiences is the key to best utilizing limited resources at brigade level for influence operations.

These choices raise several key issues. First, the editorial policies of the Arab press transcend the AOR of a brigade combat team.[10] It might be argued that this is a strategic issue that should be addressed at a higher echelon. A second issue is that there might be other target audiences who could play important roles, such as nongovernmental organizations (NGOs) or the business community. These entities might provide additional avenues for reaching the "undecided" population.

Having chosen his target audiences, Baker employed the following tools: psychological operations; civil affairs; Public Affairs; Combat Camera; Commander's Emergency Response Program; and unit leaders.[11]

COL Baker also relied on many traditional mechanisms of influence operations; for example, he developed leaflets that could be used routinely or modified rapidly to respond to a specific exigency.[12]

Notably, COL Baker elected not to employ military deception, one of the traditional pillars of information operations, as part of his influence operation campaign. In support of this decision, he argued that "being honest in the execution of information operations is highly important. This goes back to developing trust and confidence, especially with target audiences. If you lose your credibility, you cannot conduct effective IO. *Therefore, you should never try to implement any sort of IO 'deception operations'.*"[13]

To implement his influence operation campaign, Baker created an IO Working Group (IOWG) that drew on his diverse personnel resources. He adapted individuals to roles for which their prior career training and experience had not specifically prepared them. Thus, for example, he placed the brigade fire support officer in charge of the IOWG, because of his experience in "targeting," although the challenges associated with nonkinetic targeting differ markedly from those of kinetic targeting. He also augmented his team with some indigenous personnel who could support monitoring of the information environment, such as sermons or local news media, and Iraqi "press agents" to assist in working with the Arab press.

Table 15-1. Output Measures of Merit

Category	Measures
Political	Political reforms (participation in elections, compromises among sects)
Military	Number and severity of insurgent, terrorist attacks (emphasize Iraqi casualties, damage, impact, in order to discredit)
Economic	Improvements in economic reforms (reconstruction projects completed)
Social	Ability of diverse social groups to live in harmony; acceptance of presence of blue forces (measure willingness of Iraqis to work with blue forces; count who is "waving" where)
Informational	Increase/decrease of anti-U.S./Coalition graffiti; lack of negative press; number of accurate, positive stories published or aired; clerics' tone in mosque sermons; reaction of undecideds to red force information operations
Infrastructure	Improvements in sewer, water, electricity, academic institutions, trash collection, and information and communications technology

To use these personnel and tools, first, he modified his staff processes. He codified almost all influence operations activities in an IO annex, which was developed and issued as a fragmentary order. He mandated weekly or biweekly meetings with the civilian leaders of the targeted audiences, directed the collection of data to support weekly talking points, and required weekly reports and monthly backbriefs from his IOWG.

Second, COL Baker scheduled periodic meetings with others. This included weekly/ biweekly meetings with the targeted audiences to listen and communicate. He particularly emphasized eliciting thoughts on what was not going well and sought to respond rapidly. He conducted weekly roundtables with key members of the Arab press, supported by public affairs office activities and his Iraqi press agents.

Baker also implemented a sequence of feedback efforts. Two native Iraqis monitored the Arab satellite news 24 hours a day, and they also monitored the rhetoric of the local imams, graffiti on walls, and the "wave" factor: they noted who among the Iraqi populace was waving to Coalition soldiers on the streets.

To support these operational analyses, Baker kept track of specific metrics including the number of accurate or positive stories published or aired, quantifying a lack of negative press; the number of walk-in or noninformant tips; the "wave" factor; whether there was an increase or decrease of anti-U.S./Coalition graffiti; the tenor of mosque sermons; and the willingness of Iraqis to work with U.S. forces.

Such measures of merit could usefully be augmented and structured into two classes: input measures and output measures. The input measures would be those that characterized influence operations performance, such as the number of meetings held with targeted groups, or the amount of time spent in creating, validating, and disseminating messages to the targeted groups. Such measures would be largely under the control of blue forces.

Even more important would be output measures to characterize the progress toward specific goals such as those that Baker adopted. Such measures could usefully track the dimensions of PMESII, as illustrated in table 15–1.[14]

Looking Forward: Using Cyberspace in Tactical Influence Operations

Cyberspace is likely to play an increasing role in future tactical influence operations. It has the potential to support the rapid dissemination of precision guided messages and to extend the reach of influence operations far beyond the immediate range of the traditional methods of loudspeakers and leaflets.[15]

Examples of the kinds of cyberspace tools that could be used in support of future tactical influence operations campaigns include creative use of the Internet; "E-flets"; the "silent loudspeaker"; inserting messages into existing mass media; social networks; virtual reality; "Megaphone"; ring tones; and video games. Each of these tools is discussed briefly below.

Terrorist groups have exploited the Internet extensively to support a broad variety of functions such as influencing target audiences and facilitating training.[16] General John Abizaid, USA, former Commander, U.S. Central Command, has pointed out that al Qaeda is a master of "recruiting, training, equipping, advertising, manipulating, propagandizing [and] proselytizing" in cyberspace.[17] The United States is currently constrained in its use of the Internet for fear of "blowback" effects on U.S. audiences—that is, U.S. audiences might be influenced by propaganda aimed at our adversaries.[18] Restrictions on U.S. use of the Internet in support of influence operations have meant, however, that we have effectively ceded the use of this mechanism to our adversaries.

"E-flets" are a type of message sent on the Internet, usually through uniform resource locator links to a Web site with a message for the target audience. Attackers can use them anonymously. A "silent loudspeaker" sends text messages tailored to a specific population, generally through their cellular phones or personal digital assistants. The message may contain partially true (or "grey") information or what is called "rumor intelligence."

The United States has developed several mechanisms for inserting messages into existing mass media. For example, it has developed systems to support the broadcast of a live or recorded message on a nation's television or radio airwaves. However, current airborne systems (for example, the EC–130 Commando Solo) are limited in their speed, range, vulnerability to adversary air defense systems, and time on station.[19] In addition, written articles are sometimes generated to be disseminated in the local press or in U.S. media outlets. However, it can prove embarrassing to blue forces when it is revealed that the media have been paid to run those articles.[20] Many of these techniques overlap significantly with operational and strategic influence operations.

Over the last several years, there has been explosive growth in participation in social networks such as MySpace and FaceBook. Information from such sites can provide vital information to support tactical influence operations. Use of social networking techniques could enhance the effectiveness of technical applications of cyberspace.[21] However, there is concern that an adversary could access these social network sites to gain insights that would undermine operations security. Participation in virtual reality sites such as Second Life has surged. Recently, these sites have witnessed increased political agitation as participants have used them to express dissent. It has also been reported that "home-grown jihadis are rehearsing for terror attacks in virtual worlds such as Second Life."[22] Furthermore, in recent clashes, such as the war between Hizballah and Israel, YouTube was employed rapidly by civilians to post still and video imagery to depict alternative perspectives of the conflict.[23]

Israeli sources have developed "Megaphone" software that can send an alert when specified subjects come up in chat rooms or Internet polls. Such a tool could send alerts to an

IOWG, which could use the information to help shape discourse and frame key questions.[24] Sometimes, embarrassing pronouncements by important public figures have been surreptitiously recorded and made into cellphone ringtones so that repetition of the message would undermine the reputation of those individuals.[25] New video games glorify jihadi goals and values to indoctrinate young people with the ethos of terrorism. Blue forces need analogous games to counter this trend.

These cyber influence tools raise a set of issues and observations. First, many of these tools are characterized by some level of deception. However, recall that COL Baker instructed his working group that deception should be avoided because it would breed mistrust in the target audience. Second, the use of these techniques requires in-depth understanding of the architecture of cyberspace. For example, the kinetic attack team would have to avoid destroying cellular towers needed to transmit messages to the target audience.

Third, since cyberspace technology features bidirectionality, it offers the opportunity to elicit useful feedback from the target audience. This can be achieved by monitoring key blogs or conducting Internet interviews.[26]

DOTMLPF Gaps

Shortcomings in the areas specified by DOTMLPF factors have been observed and must be addressed. *Doctrinally*, there has been a failure of the organization to be responsive and synchronized for influence operations, top-down and bottom-up. Relationships among strategic, operational, and tactical influence operations must be harmonized to ensure that messages are properly tailored and timely. This is a particular problem with increasing numbers of stakeholders in influence operations (for example, multinational actors, interagency organizations, NGOs). However, this must not constrain our ability to communicate directly and in a timely fashion with the local population.

Organizationally, IOWGs tend to have too few members and an insufficient mix of skills. This suggests that such organizations should be expanded and augmented with well-trained staff members with adequate skills and experience. Existing IOWGs have very limited *training* in counterinsurgency (COIN) operations and media relations. However, there is a countervailing concern that emphasis in COIN training may lead to the erosion of traditional major combat skills.[27] In addition, there is a serious lack of training in various languages that blue forces are likely to need over the next decades.

From a *materiel* perspective, IOWGs do not have systems to cope with shortfalls. In particular, they lack automated tools to support the timely translation of voluminous written and oral information and decision aids to support formulation and analysis of influence operations courses of action (COAs).

From a *leadership and education* perspective, IOWGs lack adequate education on cultural awareness. Given the diverse areas where these working groups are likely to operate, it is important that reachback capability be established to gain access to experts in cultural subjects. In addition, access should be established to human terrain teams in theater to take full advantage of their social science skills and cultural expertise.[28]

From a *personnel* perspective, the leaders of IOWGs have inadequate capacity to reward individuals with vital skills, such as cultural experts, and thus lack the tools needed to encourage the evolution of needed capabilities.

Finally, IOWGs lack appropriate *facilities* to support information-sharing with the

targeted audiences and key stakeholders. Creative use of cyberspace could facilitate this exchange of information without compromising the security of key groups.

Options to Mitigate DOTMLPF Gaps

There are a wide range of options to redress specified DOTMLPF gaps. The following list builds upon and restructures selected recommendations suggested by COL Baker.

Doctrine. First, we should reassess policies and regulations that inhibit tactical units' ability to compete in an influence operations environment. Second, we should explore the potential utility of additional elements of the influence operations toolbox, such as tactical military deception, computer network operations, public affairs, civil affairs, and humanitarian assistance and disaster relief. Third, we should expand and restructure the MOMs to facilitate the formal implementation and analysis of influence operations.

Organization. We should rethink the composition and size of the IOWG to avoid ad hoc assignments. Thus, we should consider expanding the number of people and the seniority of the staff assigned to the IOWG. In addition, we should employ properly educated and trained personnel in the areas of nonkinetic targeting and public affairs, recognizing that the ideal personnel might not always be available.

Training. Two of Baker's recommendations are being partially implemented. First, COIN instruction should be required at all levels in the institutional training base. However, a balance must be struck so that we do not erode the ability to support major combat operations. In addition, we must increase the quality and quantity of media training provided to soldiers.

Materiel. If the United States is to be an effective participant in the "IO duel," constraints on its use of the Internet for influence operations should be reevaluated, particularly for transmissions in languages that have an extremely small linguistic base in the United States (such as Pashtun and Dari). In particular, it would be appropriate to reassess the continued utility of the 60-year-old Smith-Mundt Act.[29]

Second, the need to understand vast amounts of oral information, such as sermons at mosques and radio or television transmissions, and written information, such as newspapers, requires expedited development, transition, and use of automated translation devices (spoken and written). We should also encourage the creation and use of reachback centers of excellence. We should more rapidly develop and field decision aids to support influence operations COA analysis.[30]

Leadership and Education. An urgently needed step is to integrate cultural awareness education as a standard component in our institutional curriculum and to increase the quality and quantity of media training provided to service leaders.

Personnel. We should seek more mature, experienced soldiers to support IOWGs. We should consider vastly increasing the number of authorized culture experts for potential AORs.

Facilities. Currently, there are many facilities to enhance information-sharing in the AOR. We should standardize and populate civil-military operations centers to facilitate information-sharing with nonmilitary participants.[31] These facilities should enable sharing information in cyberspace, to augment the face-to-face physical interactions by which trust can be built most effectively.

This chapter has put forth a number of interlocking frameworks for conceptualizing and analyzing tactical influence operations issues. The proposed mission-oriented approach provides a logical way of organizing and addressing these issues. It incorporates the DIME-PMESII paradigm to provide a systematic means of characterizing the nature of the problem and formulating useful MOMs. The DOTMLPF paradigm provides a systematic means of identifying gaps and formulating integrated packages of actions to redress those gaps. Overall, if the United States is to be effective in future influence operations, "the warfighter must be able to 'pre-empt, react, and be adaptive.'"[32]

Several key policy issues should be addressed as we consider more aggressive use of cyberspace to support tactical influence operations. These include blue force use of the Internet, the value of employing deception operations, and the development of doctrine so that a coalition of multinational and interagency forces can undertake a coherent, effective influence operations campaign.

---

[1] Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006), 13–32.

[2] The discussion of cyberspace opportunities for enhancing tactical influence operations draws extensively on the ideas advanced by Timothy L. Thomas, "Hezballah, Israel, and Cyber PSYOP," *IOsphere* (Winter 2007), 36–44.

[3] David T. Signori and Stuart H. Starr, "The Mission-oriented Approach to NATO C^2 Planning," *SIGNAL* (September 1987), 119–127. This article discusses the development of the approach and applies it to NATO command and control planning.

[4] The acronym *DOTMLPF* was introduced in *Joint Vision 2020*, which was issued by the Chairman of the Joint Chiefs of Staff on May 30, 2000. The framework is used extensively by the Services and the joint community as a problem-solving construct for assessing current capabilities and managing change.

[5] See Brigadier K.T. Hoegberg, "Toward a NATO C^3 Master Plan," *SIGNAL* (October 1985).

[6] Joint Staff, Director of Command, Control, Communications, and Computers, and Director, Defense Research and Engineering, *Advanced Battlespace Information System (ABIS) Task Force Report*, vol. 2, *Major Results*, report no. A859313, May 1996, available at <http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA313958&Location=U2&doc=GetTRDoc.pdf>.

[7] Chuck de Caro, "Killing Al Qaeda: The Destruction of Radical Islam Using SOFTWAR and AMOEBA," paper no. 031, 12th International Command and Control Research and Technology Symposium, Newport, RI, June 19–21, 2007.

[8] Societal models of this type are discussed and analyzed in Greg L. Zacharias et al., *Behavioral Modeling and Simulation: From Individuals to Societies* (Washington, DC: National Academies Press, 2008), issued by the Board on Behavior, Cognitive, and Sensory Sciences and Education.

[9] Thom Shanker, "Success in Iraq Depends on Services and Jobs, General Says," *The New York Times*, August 22, 2005.

[10] Steven P. Carney, "This is Al Jazeera," *IOsphere* (Winter 2007), 22–29.

[11] It is notable that only one of these tools, psychological operations, is considered a "pillar" of information operations. The other four "pillars" of information operations include computer network operations, electronic warfare, military deception, and operations security. The remaining tools (civil affairs, public affairs, Combat Camera, and the Commander's Emergency Response Program) are generally regarded as supporting or related capabilities (see DOD Directive 3600.1, "Information Operations," August 14, 2006).

[12] For example, standard leaflets were used to disseminate information about repetitive events such as improvised explosive device incidents or house raids. Conversely, tailored leaflets were used to respond to specific incidents (for example, a specific insurgent incident that killed or wounded Iraqi citizens in a selected neighborhood).

[13] Baker, emphasis added.

[14] From a visualization perspective, it might be useful to senior leadership if these measures are depicted in "stoplight charts" (red, amber, green). In addition, it would be useful to depict aggregate values and trends.

[15] Thomas.

[16] See chapter 19 in this volume, "Cyber Terrorism: Menace or Myth?"

[17] Fawzia Sheikh, "Abizaid: U.S. Military Has Failed to Embrace Cyberspace in Terror War," *Inside the Army*, July 2, 2007.
[18] Note that the Smith-Mundt Act of 1948 has been invoked to limit U.S. use of the Internet. However, that law was focused on the Department of State. Policies in the Department of Defense (DOD) have been ambiguous about the use of the Internet. For example, "Policy for DOD Interactive Internet Activities" (June 8, 2007) enables use of a system accessible via the Internet that allows two-way communications. However, the Joint Task Force–Global Network Operations announced on May 14, 2007, that DOD access will be blocked to 13 "entertainment sites" on the Internet (for example, YouTube, MySpace). Consequently, workarounds are needed to implement waivers and independent arrangements to access the Internet.
[19] For example, slow-moving EC–130 aircraft broadcast for up to 10 hours a day in Afghanistan. Douglas Waller, "Using PsyWar against the Taliban," *Time*, December 10, 2001.
[20] Lynne Duke, "The Word at War," *The Washington Post*, March 26, 2006, D1.
[21] M. Craig Geron, "Editorial: IO in an Unpredictable World," *IOsphere* (Winter 2007), 3–4.
[22] Natalie O'Brien, "Terrorists Practice on Cyber Game," *The Australian*, July 31, 2007.
[23] Dennis M. Murphy, "New Media and the Warfighter," Center for Strategic Leadership Issue Paper, Volume 3–08, March 2008, available at <www.carlisle.army.mil/usacsl/ publications/IP3-08NewMediaandtheWarfighter.pdf>.
[24] "[Israel's] Foreign Ministry has ordered trainee diplomats to track websites and chatrooms so that networks of U.S. and European groups with hundreds of thousands of Jewish activists can place supportive messages. . . . [S]pecial 'megaphone' software . . . alerts [subscribers] to anti-Israeli chatrooms or internet polls to enable them to post contrary viewpoints . . . [and] influence an opinion survey or the course of a debate." Jonit Farago, "Israel backed by army of cyber-soldiers," *Times* (London), July 28, 2006, available at <www.timesonline.co.uk/tol/news/world/middle_east/article693911.ece>.
[25] At a November 2007 summit in Chile, King Juan Carlos of Spain asked Venezuelan president Hugo Chavez to "shut up" after Chavez said Spain's ex-Prime Minister Jose Maria Aznar was a "fascist." An estimated 500,000 people have downloaded the insult for their ringtones. As a 21-year-old student in Caracas told the *Miami Herald*, "It's a form of protest. It's something that a lot of people would like to tell the president." BBC News, accessed at <http://news.bbc.co.uk/go/pr/fr/-/2/hi/Europe/7101.386.stm>, November 19, 2007.
[26] Thomas.
[27] Marina Malenic, "Army Concerned that COIN is Displacing Conventional Training," *Inside the Army*, July 2, 2007.
[28] Monte Morin, "Cultural Advisers Give U.S. Teams an Edge," *Stars and Stripes, Mideast Edition*, June 28, 2007.
[29] The Smith-Mundt Act of 1948, amended in 1972 and 1998, prohibits the U.S. Government from propagandizing the American public with information and psychological operations directed at foreign audiences.
[30] A new generation of useful tools to support course of action analysis is emerging. For example, the Defense Advanced Research Projects Agency has been developing a family of "plug and play" models that can be assembled to model a society through the Conflict Modeling, Planning and Outcomes Experimentation program (Alexander Kott and Peter Corpac, "Technology to Assist Leaders in Planning and Executing Campaigns in Complex Operational Environments," paper no. 232, 12th International Command and Control Research and Technology Symposium, Newport, RI, June 19–21, 2007). However, additional work is required to verify, validate, and accredit these models for their intended use (Robert Clemence et al., "Verification, Validation, and Accreditation of Complex Societal Models," paper no. 165, 13th International Command and Control Research and Technology Symposium, Bellevue, WA, June 17–19, 2008).
[31] See also chapter 17 in this volume, "Facilitating Stability Operations with Cyberpower."
[32] Murphy.