Small Wars / 21st Century

APPENDIX B

INFORMATION OPERATIONS

IO involves actions taken to affect an enemy's information and information systems while defending one's own information and information systems in order to achieve specific objectives.[1] The focus of IO is on the individual decision makers and the decision making process. IO is the ability to adversely influence enemy decision making processes while enhancing and protecting our own. Therefore, for IO to be successful, it demands an ability to understand people, cultures, and motivations. In the context of maneuver warfare, IO attempts to disrupt the observe, orient, decision, action (OODA) loop of the enemy, affecting his ability to act by causing the enemy to receive information that is inaccurate, incomplete, or received at an inopportune time.[2]

IO covers the entire spectrum of warfare and is a key capability in small wars. Peacetime IO can be used to influence our adversaries through regional engagement and influence operations to help shape the strategic environment. Additionally, it can be used to impart a clearer understanding and perception of our mission and its purpose. In the pre-crisis stage, IO can help deter adversaries from initiating actions detrimental to the interests of the United States or its allies. Carefully conceived, coordinated, and executed, IO can make an important contribution to defusing crises; reducing the period of confrontation; and enhancing diplomatic, economic, military, and social activities, thereby forestalling and possibly eliminating the need to employ physical force. In the crisis stage, IO can be a force multiplier. During combat operations, IO can help shape the battlespace and prepare the way for future combat actions to accomplish the MAGTF's objectives. Once the crisis is contained, IO may help to restore peace and order, and allow the successful termination of military operations.

---

[1] Joint Publication *Information Operations, A Strategy for Peace-The Decisive Edge in War*, Washington, DC: The Joint Chiefs of Staff, March 1999, p. 3.

[2] The Marine Corps applies the basic concept laid out by John Boyd in U.S. Marine Corps, "Information Operations Concept," in *Marine Corps Warfighting Concepts*, for the 21st Century, 1998, pp. IX3-IX18.

Information Operations Principles

- ***IO is an integral function of the MAGTF.*** Planning for IO is inherent to MAGTF planning and is not conducted by unique IO forces, although some non-organic capabilities such as PSYOP units may assist in planning and executing IO activities.
- ***MAGTF IO is focused on the objective,*** not just enemy forces.
- ***The MAGTF commander's intent and concept of operations determine IO targets, objectives and priorities.***
- ***MAGTF IO must be synchronized and integrated with those of higher and adjacent commands. This integration occurs in two directions.*** Horizontally, MAGTF IO must be coordinated and integrated with strategic and theater-level IO activities. Vertically, MAGTF IO activities have to be integrated with everything else the MAGTF is doing since military operations and actions will also send a message. Rhetoric and action must be integrated to send a consistent message.[3]

Target Audiences.

There may be numerous target audiences for Information Operations as depicted in Figure 1.[4] The MAGTF may target hostile forces and their supporters in a given area with one message. It may be necessary to influence the neutral component of the population to influence them in a positive way to support our allies and coalition partners. Obviously, as previously covered, the impact of each message is dependent upon a very nuanced understanding of current perceptions and attitudes of the target audience, and the underlying culture. Without an in depth grasp of the basic cultural values, rituals, heroes or symbols of a given culture, it is extremely difficult to tap into and shift the basic attitudes and ultimately the behaviors of the audience.

---

[3] MCWP 3-0.4, *Marine Air-Ground Task Force Information Operations*, Washington, DC: Headquarters, U.S. Marine Corps, 2002, pp. 1-3 to 1-4.

[4] Colonel Richard Iron, British Army, used this graph and construct during a presentation on Irregular Warfare at Quantico, VA, 6 Oct. 2004.

By operationalizing IO, we can gain the initiative and achieve an informational advantage over our opponents that expertly employs offensive and defensive tactics, techniques, and procedures in order to achieve success. To comprehend the employment of IO, it will be necessary to describe each of the elements of IO as key enabling functions.

IO is the cumulative effect of distinct functions integrated in order to create synergistic effects and act as a force multiplier. These functions, when combined with accurate and timely intelligence, form the basis of IO. The following paragraphs outline the essential components of IO most relevant to the planning and conduct of Small Wars:

Electronic Warfare (EW). Electronic warfare represents the military use of the electromagnetic spectrum and directed energy to manipulate the same in order to defeat enemy systems. EW is a force multiplier and is not limited to just radio frequencies (RF spectrum) but includes optical, acoustical, and infrared emissions as well. Control of the electromagnetic spectrum is gained by protecting friendly systems while exploiting and countering enemy systems. When all EW assets (air, ground, sea, space) are fully integrated into the scheme of maneuver, synergy is achieved, attrition minimized, electronic fratricide avoided, and decisiveness enhanced. In a small wars context, EW can be used to paralyze an enemy's C2 network. Given the growing sophistication of adaptive networks and their use of modern information technology, this will remain a relevant pillar of IO.

Computer Network Operations (CNO). Computer network operations are activities designed to control or deny the adversary's use of telecommunications and/or computer networks. Network attacks are used to render inoperable or temporarily disable systems or functions without physical evidence of destruction or manipulation. Computer and/or telecommunications attacks aim to influence decisions and perceptions; for example, affecting user confidence, denying data/information exchange, or confusing images or other

information. Considering the increasing use of computers by potential enemies and transnational actors, an increasing need to attack these systems in Small Wars, in order to deny their use to the enemy is anticipated.

Psychological Operations. Psychological Operations (PSYOP) is the art of influencing the attitudes, feelings, emotions, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[5] It involves operations planned to convey selected information and indicators to foreign audiences, and can serve as both a combat multiplier and a combat reducer. It can help magnify the impact of combat operations, for example, by convincing enemy forces that defeat is inevitable. It can also help reduce the incidence of combat and save lives. It can be used to convince enemy soldiers to put down their weapons. As Major General Wilhelm, the commander of US Marine Forces during Operation Restore Hope in Somalia, explained, "the PSYOP loudspeaker teams were a combat subtractor…they reduced the amount of unnecessary bloodshed by convincing Somali gunmen to surrender rather than fight."[6] PSYOP gives military commanders the capability to communicate directly with the civilian population, providing the people with needed information and articulating the United States' side of the story to gain indigenous support.

In Small Wars, PSYOP can be used to:

1. Create dissension, low morale, and subversion within *insurgent forces,* which may shift the loyalty of adversary units or individuals.
2. Attack the legitimacy or credibility of the adversary to the general population.
3. Counter or negate the effectiveness of *the adversary's* propaganda to external audiences and local population.
4. Gain *civilian support* for the host nation (HN) government.
5. Generate a favorable image of the US. among selected *foreign target audiences*, and support for U.S. operations.

---

[5] Joint Publication 3-53, *Doctrine for Joint Psychological Operations*, Joint Staff, 5 Sept. 2003.

[6] *Psychological Operations in Support of Operation Restore Hope*, United Task Force Somalia, May 4, 1993, p. 6.

6. Reduce support and resources of the adversary's operations among the HN's *civilian population*.
7. Build and maintain the morale of HN *military forces* and sustain their perception that success is assured.
8. Gaining support of *neutral elements* (uncommitted groups) to our side.[7]

The delivery of messages through PSYOP can take numerous forms: face to face communications, loudspeaker broadcasts, radio and television broadcasts, printed materials such as leaflets, posters, booklets, comic books, and newspapers, and modern technology such as cell-phones and e-mails via internet.

In planning PSYOP, several basic elements must be present: a clearly defined mission; analysis of all targets; the evaluation of actions for psychological implications; a reliable medium or media for transmission; rapid exploitation of PSYOP themes; and continued assessment of the results of PSYOP for their relevance to the mission. When integrated into the joint force commander's overall campaign plan, PSYOP can help accomplish the mission by magnifying the impact of the many different things the command is saying and doing. Designed and tailored for a specific target audience, psychological operations must relate to the situation at hand, be used in a timely manner; be projected through the most appropriate media forms, and use the appropriate language.

Related IO Activities

Public affairs and civil military operations, while being military functions, are not elements of IO but are related activities that support IO and require close coordination and integration with the core capabilities. However, the primary purpose and rules under which they operate

[7] Adapted from Joint Pub. 3-53, p. I-12.

must not be compromised in the planning process. This will require additional consideration in the planning and execution of IO.