CENTER for STRATEGIC LEADERSHIP

Issue Paper

Center for Strategic Leadership,
U.S. Army War College

May 2009
Volume 4-09

Talking the Talk: Why Warfighters Don't Understand Information Operations

Dennis M. Murphy

(This article originally appeared in the April, 2009 issue of "IO Journal" and is reprinted here with the permission of the editor.)

Back in 2006 Army Colonel Rob Baker published an article in *Military Review* entitled "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations."[1] Any information practitioner who reads this excellent piece will immediately latch on to the fact that Baker's brigade was not really conducting information operations (IO), but in fact was using strategic communication as its primary enabler. But wait…can you conduct strategic communication at the tactical level? And if, from the lofty ivory tower of academia or the hallowed halls of service doctrine organizations you told Baker that he was not conducting IO would he really care about your nuanced interpretation? In other words, does it really matter?

The value of information as a military enabler has always been a factor in warfare. But the rapid evolution of the information environment has caused information to rise in importance to where it is effectively used by adversaries as an asymmetric weapon of choice. The improvised explosive device may be a tactical kinetic weapon, but it is, more importantly, a strategic information weapon when the detonator is paired with a videographer. In an attempt to both counter this information-savvy enemy, as well as exploit that same environment to achieve military objectives, the United States military has struggled to establish definitions and doctrine concurrent with applying those nascent concepts in combat. The result is a developmental process that has muddied the waters outside the very narrow subset of military service members and academicians who claim some form of "information" as their primary specialty; ironic, given the communications and marketing expertise espoused by some of those very same practitioners.

A review of current military and U.S. government information-related lexicon and definitions points out a very obvious flaw: this stuff is confusing…and in some cases, self-defeating. It's time for a doctrinal pause to allow a clean slate review of information operations, strategic communication and, yes, cyberspace operations. Such a review may find that simpler is better.

Words (and Definitions) Matter

Information Operations

Any detailed review of current information-related terminology and definitions used by the United States government should be considered from the perspective of a warfighting commander. Remember, if information is an enabler that

1. Baker makes a compelling case for the importance of information effects as a main effort while a brigade commander in Iraq. He refers to his actions as "information operations" but a close read reveals that his unit was primarily conducting strategic communication. See "The Decisive Effort: A Brigade Combat Team Commander's Perspective on Information Operations" in the May-June 2006 issue of *Military Review*.

Professor Dennis M. Murphy is the Director of the Information in Warfare Group, part of the Science and Technology Divison of the Center for Strategic Leadership, United States Army War College.

supports the achievement of a military objective, then the warfighter needs to know where it fits in his plan and how to exploit it. In other words, the warfighter needs to "own" the information capabilities…and in order to own it, he must understand it. Consider information operations.

The first question one may ask is whether information *operations* (emphasis added) are separate operations in and of themselves, or part of the greater military operation. To some, this may seem trivial and perhaps inconsequential, but to the uninitiated, the lexicon itself defines the concept. Consequently, the commander, who probably hasn't read IO doctrine, and who may have received, at most, a three hour block of instruction three years ago in a senior service college, is left to his own devices. And so anecdotal evidence exists of commanders and operations officers directing IO staffs to "sprinkle some of that IO stuff" on the already completed military plan. Understandable perhaps, since if information operations are separate operations, then it's pretty easy to push the IO staff out of the core planning group to the side trailer or tent. By the way, the U.S. military's Joint Publication 3-13 clearly states that IO is in support of the overarching joint operation and should be fully integrated into the planning process.[2]

If the term "information operations" is an issue in and of itself, perhaps the definition can provide clarification…so here goes. Information operations is:

> *The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations (PSYOP), military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own.*[3]

Unfortunately, the reader's focus tends to move directly to the listed core capabilities within the definition at the expense of the rest of the verbiage. Consequently, IO becomes PSYOP or IO is computer network operations in the mind of the warfighter.[4] This focus on capabilities further obfuscates the definition when civilians, often in the mainstream media, take the next logical leap that PSYOP equals propaganda which in turn equals lies.[5] And since IO is perceived to be PSYOP, and the definition of IO includes deception…well, you get the obvious (albeit incorrect) conclusion.

Not only is the listing of the capabilities an issue, but the mere number of them detracts from an understanding of the concept. Since there are five core capabilities and eight additional supporting and related capabilities, to include physical attack, the perception is that IO is either everything you do (more on this later) or simply so complex that it must be left to the expert staff section to handle. But remove the reference to capabilities from the definition and the clarification is telling. Information operations is:

> *The integrated employment of …capabilities…to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own.*

Now it should become obvious that IO is an integrating function, first and foremost, and not a separate operation or a separate single capability. In other words IO can't be PSYOP alone, but it can be PSYOP and electronic warfare if those capabilities are synergistically integrated to achieve the appropriate effect against the appropriate target audience. That desired effect is to influence disrupt, corrupt or usurp. Its target audience is adversarial human and automated decision-making. Given this target audience it's evident that IO can impact the cognitive, informational and/or physical dimensions of the information environment. By explicitly excluding a laundry list of capabilities, the definition is no longer self-limiting since the tools available are now constrained only by the imagination of the commander and his staff. While it may not be about everything you do, it certainly can be about anything you can do to achieve the desired information effects in support of the military operation, to include physical attack, i.e. actions.

---

2. Chairman of the Joint Chiefs of Staff, "Joint Publication 3-13, Information Operations," 13 February 2006, pp. ix, xii.
3. Ibid, p. I-1.
4. It's worth noting that the definition of IO includes core capabilities for programmatic reasons, i.e. the listed capabilities have funding streams. Unfortunately, there are numerous examples of senior military leaders using the term "IO" when referring to a single, specific capability thus reinforcing the confusion.
5. The long history that, at least in perception, equates psychological operations to propaganda is outlined in "Propaganda: Can a Word Decide a War" by the author and James F. White, in the autumn, 2007 issue of *Parameters*.

Strategic Communication

If you think IO is confusing outside of a small circle of information experts, consider strategic communication. Strategic communication is an emergent concept with several definitions floating about, no doctrinal base and a lexicon that fails completely to convey the desired understanding. No small wonder that U.S. Southern Command's Admiral James Stavridis recently paraphrased World War II's great naval commander and strategist Ernest King, stating "I don't know what the hell this [strategic communication] is that Marshall is always talking about, but I want some of it."[6] In this case it may be more beneficial to first look at the definition and then analyze the term itself. The 2006 Quadrennial Defense Review roadmap on strategic communication defines it as:

> *focused USG (United States Government) processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs and actions synchronized with other elements of national power.*[7]

The roadmap goes on to list the primary supporting capabilities of strategic communication as public affairs, aspects of information operations (principally psychological operations), military diplomacy, defense support to public diplomacy, and visual information.[8] Once again, the listing of capabilities within the roadmap muddies the waters for the warfighting commander and in fact limits the perceived means available to *communications* (emphasis added) based activities and so reinforces the lexicon of the term itself. However, parsing the definition to its essential parts again provides clarity:

> *Focused USG processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives….*

So, strategic communication is a process of understanding and engaging. This implies a two way conversation. The desired effect is to create, strengthen and preserve conditions favorable to national interests and objectives. The target audience is intentionally large and vague, i.e. simply "key audiences." Strategic communication focuses on the cognitive dimension of the information environment. Removing the capabilities listing once again removes some of the mystery from the term.[9]

Simplifying definitions also allows one to easily compare strategic communication to IO. Strategic communication is the more broadly overarching concept targeting key audiences and focusing on the cognitive dimension of the information environment. IO as an integrating function, on the other hand, more specifically targets an adversary's decision making capability which may be in the cognitive, informational and/or physical dimensions of the information environment. Considering the targets and effects described above, it should be clear that both strategic communication and IO can be employed at all levels of warfare (tactical, operational, theater strategic and national strategic). Tactical commanders routinely employ strategic communication in Iraq and Afghanistan today based on their interactions with key audiences in their area of responsibility to a potential strategic end. On the other end of the scale, IO could certainly be employed strategically as part of a Phase 0 shaping operation or a Phase 1 deterrent operation against a potential adversary's decision-making capability.

Just Plain "Information": Recommendations and Conclusion

The Joint Staff recently published the definition of cyberspace operations stating that it "should encompass computer network operations and activities to operate and defend the Global Information Grid."[10]

6. James G. Stavridis, "Strategic Communication and National Security," *Joint Force Quarterly*, 3rd Quarter, 2007, p. 4.
7. U.S. Department of Defense, "QDR Execution Roadmap for Strategic Communication," September 2006, p. 3. The Deputy Assistant Secretary of Defense for Joint Communication states that this is the only Department of Defense definition of strategic communication that should be in use.
8. Ibid, p 2.
9. The office of the Assistant Secretary of Defense for Public Affairs recently published "Principles of Strategic Communication." Interestingly, and apropos to the complexity of the roadmap definition, this product simply refers to strategic communication as the orchestration and/or synchronization of words, images and actions to achieve a desired effect.
10. Vice Chairman of the Joint Chiefs of Staff, "Definition of Cyberspace Operations," memorandum for the Deputy Secretary of Defense, September 29, 2008.

Eschewing further analysis, you can see where this is going. With the rapid evolution of the information environment, "cyberspace operations" is the latest example of inventing terminology and definitions on the fly, often overlapping with current doctrine and lexicon. (You'll note that "computer network operations" is a core capability in the definition of IO.) Additionally, as the terms IO, strategic communication and cyberspace operations gain greater usage, confusion increases while codification proceeds, often as separate doctrine development for each concept. For instance, U.S. Joint Forces Command recently published a "pre-doctrinal" publication on strategic communication.[11] No doubt, someone, somewhere on the Joint Staff is working on the embryonic beginnings of cyberspace operations doctrine.

Given the above analysis, the U.S. military would be much better off pausing to review current publications and then consolidate and simplify what is currently confusing, overlapping and disparate guidance. The result should be an overarching joint doctrinal effort that both considers existing concepts and focuses on an understanding of information as a warfighting enabler. Entitle it (again, simply) "Information." The review may find that it is totally appropriate to include information operations, strategic communication and cyberspace operations *concepts* (emphasis added). But in doing so the reviewers should specifically consider changing the lexicon of the terms where appropriate and parsing the existing definitions to their simplest essentials. Capabilities can be addressed within this proposed publication, but not within the definitions themselves. In fact, the definitions should focus on the desired effects and the targeted audiences. Given the rapid acceptance of strategic communication and the nascent emergence of cyberspace operations as warfighting constructs, no doubt a new concept is just around the corner. A doctrinal approach to information writ large will allow the overarching focus and understanding that warfighters need in order to "own" the enablers, while providing the flexibility to incorporate whatever new concept may appear on the horizon.

There are glimmers of hope in this regard. The Army, in its overarching field manual "Operations" (FM 3-0) makes little reference to IO but instead adopts the term "Information." Additionally, joint doctrine writers are in the process of revising Joint Publication 3-13 ("Information Operations"). The final coordination program directive proposes a chapter on information operations' relationships to other concepts to include strategic communication and cyberspace operations, perhaps in an attempt to gain clarification. But that same directive warns against a change in terminology stating that "new or modified…terms should only be used when such terms are essential to the development and understanding of proposed doctrine."[12] The Joint Staff would be well served to consider the revision of Joint Publication 3-13 as an opportunity for a doctrinal pause. The time is ripe for a clean slate review of the current terminology and definitions and to provide an overarching doctrinal manual that strikes a balance between providing an understandable baseline as well as a practical implementing blueprint. In the rapidly changing information environment sometimes simpler is better.

****

This and other CSL publications may be found on the USAWC/CSL web site at: http://www.csl.army.mil.

****

11. United States Joint Forces Command, "Commander's Handbook for Strategic Communication," September 1, 2008, p. i.
12. The Joint Staff, "Final Coordination (FC) Program Directive for Joint Publication 3-13, *Information Operations,"* received December 2008.