Success will be less a matter of imposing one’s will and more a function of shaping behavior.
—Secretary of Defense Robert M. Gates

O is dead! Long live IO! After 13-plus years of infighting, programmatic protectionism, general angst over who owns what, and turf battles with its new sibling the cyber community, a new draft doctrinal definition of information operations (IO) is now working its way through the Pentagon. Unlike previous definitions that centered on what things IO owns (the “pillars” and later the “core capabilities” of electronic warfare, computer network operations, psychological operations, military deception, and operations security), the new definition omits such lists, focusing instead on what IO does.

Information operations are “the planning and integrated employment of capabilities in the information environment across the phases of joint military operations.” This new definition avoids the major pitfall of its predecessors—a rice-bowl approach that actually discouraged integration of efforts. But this article is not about whether that new definition is right, or even good. It is about how the door is now open for a fresh look at an even more significant issue.

The world of IO has always had a weakness: the endless doctrinal debate about “who owns what” has distracted from useful discussion on how to orchestrate those pieces to actually accomplish something—in other words, strategy. Just what are the ends, ways, and means of IO, and how do we align them to defeat an enemy? The Department of Defense (DOD)—in fact, the U.S. Government as a whole—desperately needs a construct for designing interagency offensive information strategy that will enable leaders to employ the information element of national power in military operations. To build one, we first look at where current thought on “information power is lacking. Then we use a new construct for binning the means: hard and soft tools. Finally, we bridge the gap between those two with the ways—using the soft tools to influence, and the hard tools to disrupt, enemy action. We start with some basics.

Information Power

While information power is well accepted as one of the four elements of national power, neither the term nor the concept appeared in the 2006 National Security Strategy. It is strangely absent from the “full array of political, economic, diplomatic, and other tools at our disposal” that is the basis of the document. Nor does information power appear in the 2008 National Defense Strategy. Moreover, although there is no vetted definition of information power, the concept is understood and the link to how the military should exercise it is obvious: information operations. Considerable attention has
4. TITLE AND SUBTITLE
Information Strategy: The Missing Link

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Defense University Press, Joint Force Quarterly, 260 Fifth Ave., Bldg. 64, Fort McNair, Washington, DC, 20319-5066

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

16. SECURITY CLASSIFICATION OF:
a. REPORT unclassified
b. ABSTRACT unclassified
c. THIS PAGE unclassified

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES 3

19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)
Prepared by ANSI Std Z39-18
The target of offensive IO is the mind of the adversary. During conflict, especially during phases two (deter) and three (seize initiative) of a campaign, the primary target is the mind of the enemy commander at every level, from the national dictator down to the infantry company commander. Other targets may include the minds of lesser officials, the local populace, and outside actors. During other phases, the relative importance of each of those targets will vary. For instance, during phase four (dominate), the minds of the populace may be more important than the minds of any remaining militant commanders. Given that target—the adversary mind—we can now devise strategy.

Offensive Information Strategy

Contrary to standard assumptions about how complicated IO is, there are just two basic ends for any offensive information strategy: the adversary’s behavior has changed, or further coordinated resistance by that adversary is impossible. All interagency plans and actions in the information domain must be aligned to accomplish one of those ends. In the first case, the desired end is for adversary decisionmakers, commanders, and populations to voluntarily capitulate to or implement our demands. Defining precisely what specific adversary behavior must change (often “cessation of aggression” or “surrender”) will vary from conflict to conflict, but in all cases it is the crucial first step.

When approached in this way, it becomes clear that this end of information operations is actually the supported, not a supporting, operation, around which the other diplomatic, informational, military, and economic elements must be aligned. In the second case, the desired end is that the adversary’s ability to command and control forces and effectively resist will have collapsed. Seeking this end normally implies that the first end has not been achieved, making it a supporting, rather than supported, operation. The situation and phase of operations will dictate which of those two ends has primacy. But before we look at how, let us first look at the available means.

Means, Ways, and Ends

The means of IO are comprised of two sets of tools: the hard tools that (probably) constitute acts of war, and the soft tools that (probably) do not. The hard tools include computer network attack (CNA), electronic attack (EA), and kinetic attack. The soft tools include not only the traditional military capabilities of PSYOP and military deception, but also strategic communication, PA, and PD. While some may feel uncomfortable about putting these all together into one strategy, not doing so is precisely what has been getting in the way. Until we put all the tools on the table and force interagency collaboration, IO will remain forever fragmented.

This brings us to the ways: how to link the means to the ends. The existing doctrinal diagrams, with their “pillars” and “capabilities,” do nothing to show how to align them toward desired ends. That requires a new framework integrating the means across interagency boundaries. If the ends of IO strategy are “changed behavior” and “inability to resist,” then the ways also become clear. The means—the tools of IO—must be used either to influence or to disrupt the adversary. For influence, the soft tools are most applicable here, and the IO strategist must orchestrate the interagency owners and actors to align them (see figure 1). PD and PSYOP must complement each other in their efforts to change adversary behavior, and military deception must reinforce them both. Most importantly, we must align our IO
efforts with our actions—the “diplomacy of the deed.”

As far as disruption, we find a model readily available in John Boyd’s oft-trivialized “OODA Loop” (observe, orient, decide, act). In fact, Boyd’s entire concept—of late, usually misunderstood to mean that we simply need to speed up our own decision processes to guarantee victory—argued that by disrupting the enemy’s ability to make decisions, we would cause complete collapse of effective command. By applying the hard tools of CNA, EA, and kinetic attack, supplemented by the soft tools, to disrupt the adversary’s OODA loops and command and control systems at appropriate points (see figure 2), we can quickly render organized resistance impossible.

Overcoming more than a decade of IO inability to deliver will take some new thought and direction. The proposed new definition of IO is a helpful start, but it does not fill the need for an offensive information strategy model. For that we must reorganize strategy along the lines of ends, ways, and means. The ends are simple: adversary behavior has changed, or further adversary resistance is impossible. The means bin nicely into two groups, the hard and soft tools. Finally, the ways tie them all together using the soft tools to influence and the hard tools to disrupt the adversary. Using this model, we will finally be able to effectively apply the information element of power in offensive operations.

Notes


3 “Information Operations” (Washington, DC: Staff action package, Office of the Under Secretary of Defense [Intelligence], 2009), 1. The six phases of joint military operations are one—shape; two—deter; three—seize the initiative; four—dominate; five—stabilize; six—enable civil authority.


7 Sharp, x.


10 When applied to an actual operation, clear goals and objectives of influence must be specified early on: who must be influenced to do or think what?

11 John R. Boyd, A Discourse on Winning and Losing (Maxwell Air Force Base, AL: Air University, 1987).